Advanced Keylogger with Keystroke Dynamics

Jyothis Sabu
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham
Amritapuri, India
letter2jyothis@gmail.com

Ananthanarayanan S
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham
Amritapuri, India
ananthandevan093@gmail.com

Aravind Gopan
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham
Amritapuri, India
aravindgs1401@gmail.com

Gowtham S
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham
Amritapuri, India
gowthamsmitha51@gmail.com

Shalu Murali
Department of Computer Science and EngineeringAmrita Vishwa Vidyapeetham
Amritapuri, India
shalum@am.amrita.edu

2023 International Conference on Inventive Computation Technologies (ICICT) | 979-8-3503-9849-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICICT57646.2023.10134044

***Abstract* — Keyloggers are software programs that are used to record and monitor keystrokes made on a computer keyboard. They are often used by hackers to illegally access personal details, including passwords, debit and credit card details, and other sensitive information. Keystroke dynamics is a biometric technique that uses the unique patterns and rhythms of a person's keystrokes to identify them. By combining keyloggers with keystroke dynamics, it is possible to create a more secure and accurate form of user authentication. Traditional keyloggers capture only the keystrokes, but not the entire activity of the user like system and application details. The goal is to create a software that is similar to a keylogger yet is far more sophisticated. The keystrokes entered into a keyboard-based system will be saved by the software. The software also provides information on the system's current application that the user is on. Additionally, the program logs data, like public and private IP address, MAC Address, and User information. Together with these characteristics, the program will also examine the users' typing patterns and be able to recognize anyone using the system based on their typing pattern. The keyboard input is intercepted by the keylogger software, which records all keystrokes and stores them in a log file. The data is typically encrypted and stored securely to prevent unauthorized access. The keylogger can then transmit the log file to a remote server, where the data can be analyzed and used for various purposes.**

Keywords* — *Keyloggers, Keystroke Dynamics, Typing pattern

I. INTRODUCTION

In the modern world, people use the internet as their main method of communication and information sharing. Because of the tremendous amount of knowledge available online, the internet era is booming and more and more people are moving online [11] . Malware is short for malicious software, which infects a system, carry out malicious operations, and steal confidential financial and personal information without the user's knowledge. Malware comes in a variety of forms, including viruses, Trojan horses, worms, keyloggers, and spyware [12].

A keylogger is a type of software program that is installed on a computer system to record and monitor all of the keystrokes made on the keyboard. It can be used to capture passwords, credit card numbers, and other sensitive information. In recent years, keystroke logging software has gained interest on a global scale. Keyloggers can be installed on a computer system in a variety of ways, including through email attachments, infected websites, or malicious software downloads[6].

A keylogger works by intercepting the signals sent from the keyboard to the computer's operating system. It then records these signals and stores them in a log file. This log file can be accessed by the person who installed the keylogger, allowing them to view all of the keystrokes made on the keyboard. Some keyloggers can capture screenshots, record microphone input, and monitor internet activity. Keyloggers can be used for a variety of productive purposes, but with the explosive growth in Internet usage, their destructive use far outweighs any potential benefits. The execution of key-loggers has advanced to the point that they are now a severe threat to the security and privacy of a user. Key-loggers are invisible to antivirus and spyware software makes them more dangerous[7].

In recent years, keystroke logging software has gained interest on a global scale. A keystroke logger is a sort of computer programme that is covertly placed on a user's computer to record keystrokes without the user's knowledge or consent. The theft of the user's personal information, particularly financial data like credit card numbers through analysis of the user's typing patterns, is a common goal for the attacker. [8] Keystroke dynamics is a biometric technique that uses the unique patterns and rhythms of a person's keystrokes to identify them. It is based on the fact that each person has a distinct way of typing, with variations in timing, pressure, and speed. By analyzing these patterns, it is possible to create a unique biometric signature for each user. It works by recording the timing and rhythm of a person's keystrokes as they type. This information is then analyzed to create a biometric signature that can be used for user authentication. The process typically involves recording a user's keystrokes over a while and then using machine learning algorithms to analyze the data and create a unique signature for each user. By combining keyloggers with keystroke dynamics, it is possible to create a more secure and accurate form of user authentication. Instead of relying on passwords or other forms of authentication that can be easily hacked, keystroke dynamics provides a unique and highly

orized licensed use limited to: AMRITA VISHWA VIDYAPEETHAM AMRITA SCHOOL OF ENGINEERING. Downloaded on January 09,2024 at 13:36:57 UTC from IEEE Xplore. Restrictions ap

personalized way of identifying users. This can be especially useful in high security environments such as government agencies, financial institutions, and health care organizations. A keylogger commonly referred to as keystroke logging software or hardware can capture various inputs supplied by the user and user behaviour. It coordinated the user's keystrokes, website visits, computer programme access, instant messages, and several other computer-related activities while they were using a computer. A user may easily identify a keylogger that is based on hardware by looking at the connections between the keyboard and the computer's hardware, while keyloggers that are based on software are more challenging to discover because they take the shape of software that is installed on a computer[9].

Keyloggers and keystroke dynamics are powerful tools that can be used to monitor computer activity and identify users. While they can be used for malicious purposes, they also have many legitimate uses in areas such as user authentication and security. By understanding how they work and how they can be used together, sensitive information can be protected and overall security posture can be improved[10].

Most people prefer to just see the negative aspects of this particular programme, but it also has useful applications. In addition to being used for vengeful purposes like gathering account information, Visa numbers, client names, passwords, and other private information, it can also be used to monitor children's activities at home, in the office, and by law enforcement to look into and follow incidents involving the use of PCs.The project will be entirely written in Python, using the pynput module, which isn't a built-in part of Python and needs to be installed. The software keeps track of the keyboard strokes and records the results in a file. It also includes a function that will send the logs directly to the email in order to advance the project.

In addition to accessing keystrokes typed into the system like a typical software keylogger, Advanced Keylogger with keystroke Dynamics also gathers data on which specific application is now running on the system. This will make the information more useful by enabling us to identify the application in which the user had entered the keystrokes. Additionally, this application enables the system to examine the user's typing speed so that it can accurately identify the user of the system while numerous users are simultaneously using it. Also, all of these details will be kept in log files and can be shared in the same way with the administrator.

The unethical use of the application can also be avoided ,as the user will be able to understand that the application will be running in the background . So ,the information are extracted with their complete concern and hence it is completely ethical. Also if anyone closes the application in between for doing some malicious activities, the administrator will be able to know that immediately. Hence , this application is serving as an effective activity monitoring system which is many times better than the already existing keylogger system.

II. Related Works

Keyloggers are software or hardware tools that record every keystroke made on a computer keyboard or mobile device. They can be used for both legitimate purposes, such as monitoring employee productivity or parental control, and malicious purposes, such as stealing passwords and sensitive information.

There is a significant body of literature on keyloggers, including their development, detection, and prevention. Here is a brief literature review on keyloggers:

A. Development of Keyloggers:

Researchers have developed different types of keyloggers over the years, including software-based keyloggers, hardware-based keyloggers, and kernel-based keyloggers. Software-based keyloggers are the most common type and can be installed on a computer without the user's knowledge. Hardware-based keyloggers, on the other hand, are installed between the keyboard and computer and record every keystroke made. Kernel-based keyloggers operate at the operating system level and can be difficult to detect[4].

B. Detection of Keyloggers:

Detection of keyloggers can be challenging, as they are designed to be stealthy and avoid detection. Researchers have proposed various methods for detecting keyloggers, such as using anti-virus software, scanning the registry for suspicious entries, and monitoring system resources[5]. However, keyloggers can also evade detection by using encryption or by disguising themselves as legitimate files.

C. Prevention of Keyloggers:

According to the CIA triad, information security means the preservation of confidentiality, integrity and availability of data [16]. Prevention of keyloggers is crucial to protect sensitive information from being stolen. Researchers have proposed several prevention methods, such as using antivirus software, keeping software updated, using two-factor authentication, and using a virtual keyboard. However, these methods may not be foolproof, and it is important to remain vigilant and aware of potential threats.

Paper [1] is completely based on setting up a software based keylogger using python. The software should monitor the keyboard movement and store the output in a file. It utilizes the pynput module from the python library. To elevate the project a new feature is also added in which these logs will be directly sent to the email.

In paper[2] using a screen-recorded video of a person typing on his system, this research provides a novel exploitation technique that extracts and learns a user's typing pattern. Computer vision is used in the method. Instead of injecting a keylogger into the victim's PC, an attacker may use a screen-recorded video to make the attack more concealable and simpler to execute. This research also shows, from a screen-recorded video, how to construct an astonishing statistical resemblance in keyboard timing patterns.

The Keystroke Dynamics authentication service could then be supported using the patterns. Exact time when a key is typed should be known and when the next character is entered after to detect typing patterns from a screen-

orized licensed use limited to: AMRITA VISHWA VIDYAPEETHAM AMRITA SCHOOL OF ENGINEERING. Downloaded on January 09,2024 at 13:36:57 UTC from IEEE Xplore. Restrictions ap

recorded video. Two problems require solutions namely, text cursor tracking and detection separating characters and extracting timing.

As noted in Algorithm 1, the first proposed method aims to identify and follow the emergence of a text cursor on a screen-recorded video. Using Open CV, the proposed algorithm was created. First, frame f from the screen recording is read. Then, the Canny method finds the edges of each object (which includes buttons, text cursor, characters and others) that appear on the frame and extracts its structural information. The retrieved frame f is then combined with the previous frame on the video, f 1, using a bit-wise XOR technique. Using this method, extract each object (in this case, a hypothetical moving text cursor) whose position has changed since the previous frame f 1. The next step is to extract the moving objects by obtaining their outlines, which include the text cursor. Lastly, the contour's shape is compared to the previously defined average shape of a text cursor to identify and extract the text cursor object. Then, the text cursor object's size and location are determined by calculating and generating a bounding box region around the item. The coordinates for the text cursor location are xMin, yMin, xMax, and yMax. In this study, the bounding box that the text cursor object is in is referred to as the Cursor Bounding Box (CBB)[2].

The second algorithm executes to extract the most recently entered key from each frame based on the calculated CBB coordinates and once the coordinates and the CBB region of the text cursor are retrieved. This method is predicated on the notion that the character to the left of the text pointer object must be the most recently input character by the user.

Paper [3] proposes an AI-powered child safety system that helps shield kids from modern cyber attacks while giving parents additional supervision over their kids. The system comprises Keyloggers, keystroke and mouse movement loggers which record user behavior and identify patterns in data collection. Through these records, it detects children's improper behavior and reveals children's emotional states. The main components include Behavioral Data Extractor, a Behavior-based authentication system, Smart Resource Restrictor, Automated outside threat protector.

Paper [4] proposes a keylogger that captures the key chain. Keylogger is designed to identify and record each key the victim types. It is also legitimately used by businesses to fix issues, improve customer service, and monitor employee behaviour. The Key Logger application functions as a Trojan horse and is presented as an executable(.exe) file. The software may initially appear to have been used for utility purposes, however, it is actually designed as a Key Logger. The Names Running Applications are stored in a file by the key logger, which also records information about what the user is doing. Keylog and Process Log Files both include encrypted data. The White Space Encryption Algorithm is the encryption technique used in this work, and it is a substitution cypher.

III. Methodology and Architecture

A. Overview

The proposed system is designed to perform the functions of a software keylogger and in addition to that certain innovations are also added to it which makes it a more advanced system than a normal keylogger. As a whole, the application performs a set of functions. Just like a keylogger, the application accesses the keystrokes typed on the keyboard of the targeted system so that the one who is monitoring the target system can identify all the things typed in the target system. Another feature of the application is that it accesses what all items selected using the mouse cursor of the target device. This is done because, in an ordinary keylogger, one will not be able to understand whether the person using the target system has selected any pop-up messages or has selected anything using a mouse cursor. This issue will be solved by using the application. Also, it will provide information about which application is currently running in the target system, thus making it possible to know in which application the person using the target system is typing. Also, in case a single system is being used by multiple users, the application will be able to know which person among them is currently using the system. This is done by analyzing their typing pattern. The application will check how much time is taken by the user to press the next key after pressing a key on the keyboard. This identifies the typing speed of the person and thereby their typing pattern and successfully identifies the person using the system. Finally, all these data will be stored as data logs and sent to the admin mail ID as log files. These features of the proposed application make it many times better than a normal software keylogger and hence it could be more useful.

B. Design and Working

The code is implemented in python utilizing the operating system-dependent functionality. Modules used include OS, socket, time, keyboard, numpy, pywinauto, pynput, smtplib, SSL etc. The code is also developed as an application in parallel with a python source code executed using a compiler. The application can be modified to run on system startup as well.

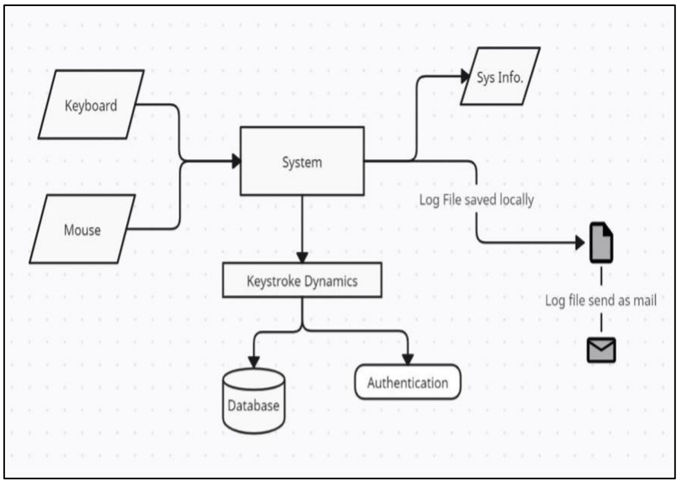
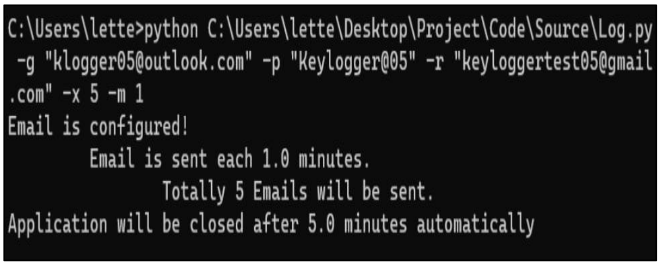


Fig. 1. Proposed block diagram

As shown in Figure 1 the inputs to the keylogger system are coming from the keyboard and the mouse. It captures and

orized licensed use limited to: AMRITA VISHWA VIDYAPEETHAM AMRITA SCHOOL OF ENGINEERING. Downloaded on January 09,2024 at 13:36:57 UTC from IEEE Xplore. Restrictions ap

interprets the inputs and stores the keystrokes as a log file which will be created for each day. The log file will be saved on the local system as well as can be transferred to the administrator through the mail. For configuring the mail the user has to input the credentials for an outlook mail. The keylogger module logins to the account to send the log files to the admin mail. The duration in which the emails are sent and the time interval between them also can be adjusted here.



```
C:\Users\lette>python C:\Users\lette\Desktop\Project\Code\Source\Log.py
 -g "klogger05@outlook.com" -p "Keylogger@05" -r "keyloggertest05@gmail
.com" -x 5 -m 1
Email is configured!
        Email is sent each 1.0 minutes.
               Totally 5 Emails will be sent.
Application will be closed after 5.0 minutes automatically
```

Fig. 2. Configuring email address

In figure 3 the outlook mail is used for sending the log file. The login credentials are to be provided in the prompt as well as the receiver email address. The ‘x’ notes the total number of emails which will be transferred and the ‘m’ notes the time interval between mail in minutes. Here x = 5 and m = 1, so the total duration of the application run will be 5*1 = 5 minutes.

The configuration using time has various applications of its own. In the case of an employee monitoring system, the system can be configured to work and send the log files according to the scheduled working time of an organization. For each day, a log file will be created in the local system on the file path provided by the admin. The log file contains information like the time, duration, the particular window and the open tabs as well as the keystrokes entered. Function keys like backspace, enter, tab and shift are also captured. For the typing pattern, information like Time duration, No of Keys pressed, Typing Speed(characters per second) and Latency/Elapsed Seconds are used. The keystroke dynamics can be used as bio-metrics for authentication services [15].

Along with the log file, a system information file is also created which includes details such as host name, username, machine details, operating system and type, processor details, screen resolution, private and public IP address and the time the user logged in. It also includes the RAM details such as the total memory, used and available memory and percentage of RAM currently being utilized. It shows the top five processes based on memory usage. This can be used by the admin to check whether the employees are using any other applications besides those for work. It gives the non-working automatic services as well as how long an application has been open. The running process list is also shown.

The system also identifies the different keyboard layouts and carries out the required mapping. It uses Languages codes, taken from lcid_dict to detect various languages. Functions for detecting user inactivity and termination are also declared.

C. Workflow

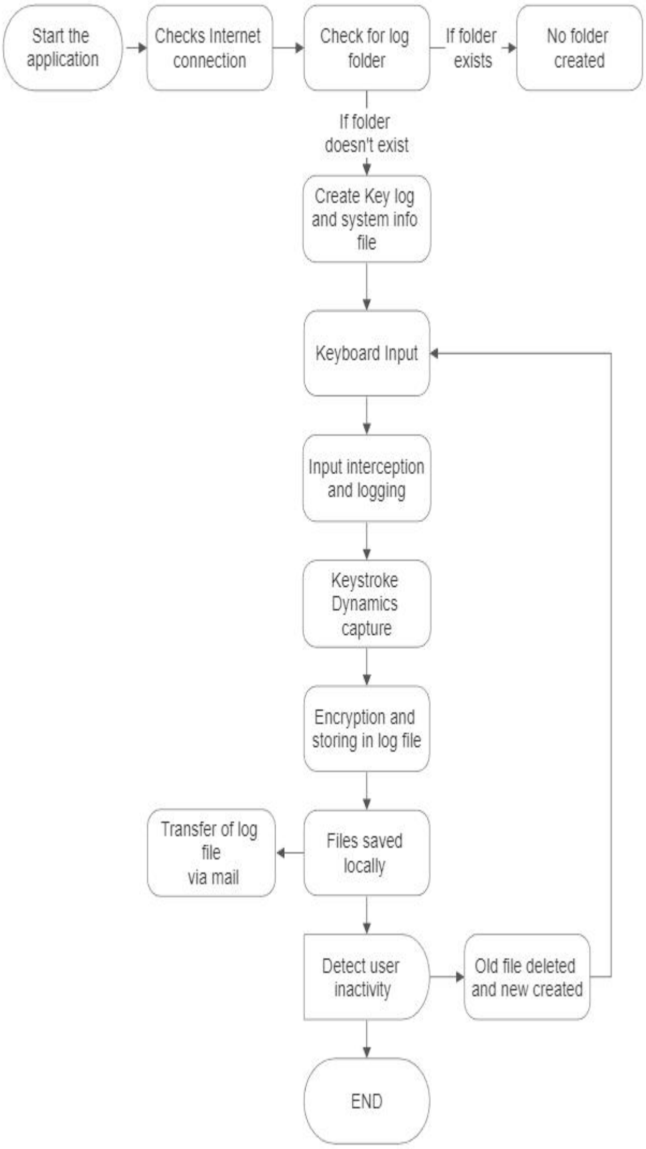

Start the application
Checks Internet connection
Check for log folder
If folder exists
No folder created
If folder doesn't exist
Create Key log and system info file
Keyboard Input
Input interception and logging
Keystroke Dynamics capture
Encryption and storing in log file
Transfer of log file via mail
Files saved locally
Detect user inactivity
Old file deleted and new created
END

Fig. 3. Flowdiagram

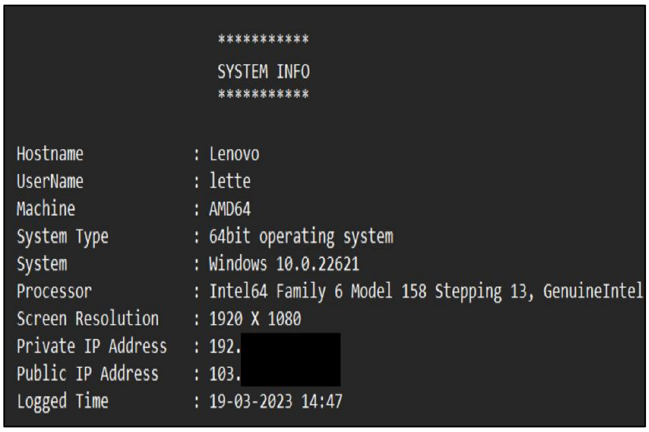
The application can be made to run on startup or manually by the user. The module checks for internet connections to send the log files. The log folder for each day will be created. The keyboard input is intercepted by the keylogger software, which records all keystrokes and stores them in a log file. It includes an additional step for keystroke dynamics. After the keystrokes are logged, they are analyzed for unique patterns and rhythms that can be used to create a biometric signature for each user. This signature can be stored alongside the log file in a secure and encrypted manner. The data is encrypted and stored securely to prevent unauthorized access. The keylogger can then transmit the log file to a remote server through email, where the data can be analyzed and used for various purposes like analysis and authentication. The program detects user inactivity by detecting screen change, mouse movement and key press. If all three are inactive for straight three minutes then the program stops and new files for log details are created.

orized licensed use limited to: AMRITA VISHWA VIDYAPEETHAM AMRITA SCHOOL OF ENGINEERING. Downloaded on January 09,2024 at 13:36:57 UTC from IEEE Xplore. Restrictions ap

IV. EXPERIMENTAL RESULTS

The keylogger program is executed using a command prompt (a program in which you type commands instead of using a mouse) [13]. The user can run the application from the .exefile as well as from the source code using the python compiler. The sample output obtained is shown in the figures below. The output is in the form of a system info file and a log file.

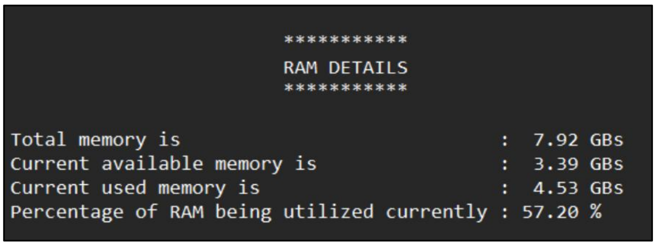
A. System Information file



```
                     ***********
                     SYSTEM INFO
                     ***********

Hostname            : Lenovo
UserName            : lette
Machine             : AMD64
System Type         : 64bit operating system
System              : Windows 10.0.22621
Processor           : Intel64 Family 6 Model 158 Stepping 13, GenuineIntel
Screen Resolution   : 1920 X 1080
Private IP Address  : 192.[redacted]
Public IP Address   : 103.
Logged Time         : 19-03-2023 14:47
```

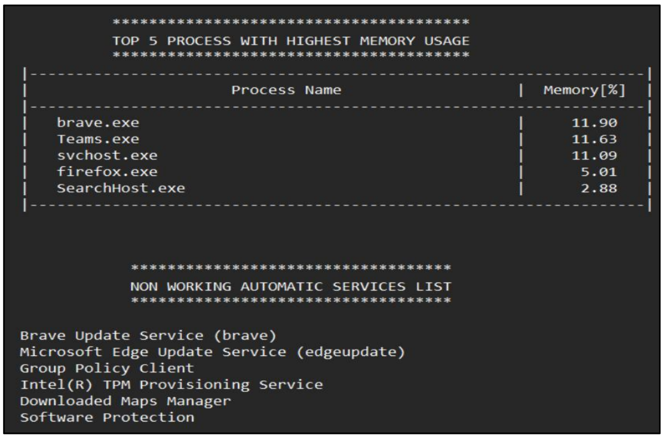
Fig. 4. Basic system information

The system information file (Fig 4) contains many details like host name, username, machine details, operating system and type, processor details, screen resolution, private and public IP address and the time the user logged in. It also shows the RAM details, the top five processes with the highest memory usage, the non-working automatic services list, the time the applications have been running, the currently running processes etc.



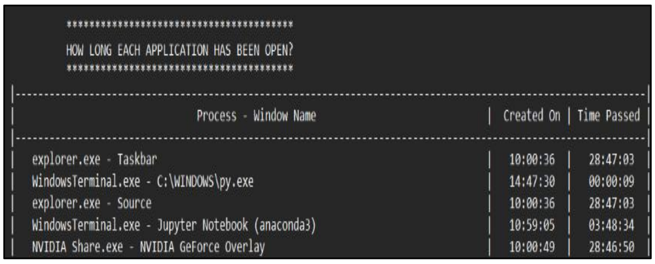
```
                             ***********
                             RAM DETAILS
                             ***********

Total memory is                           :  7.92 GBs
Current available memory is               :  3.39 GBs
Current used memory is                    :  4.53 GBs
Percentage of RAM being utilized currently : 57.20 %
```

Fig. 5. RAM details



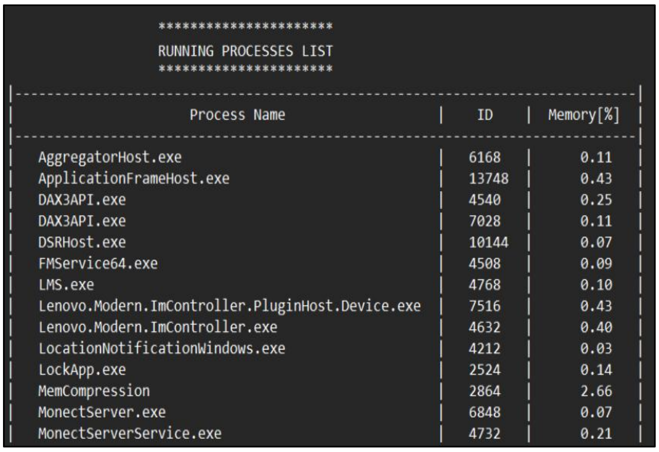
```
          ***************************************
          TOP 5 PROCESS WITH HIGHEST MEMORY USAGE
          ***************************************
|------------------------------------------------------------------|
|                    Process Name                    |  Memory[%]  |
|------------------------------------------------------------------|
|   brave.exe                                        |     11.90   |
|   Teams.exe                                        |     11.63   |
|   svchost.exe                                      |     11.09   |
|   firefox.exe                                      |      5.01   |
|   SearchHost.exe                                   |      2.88   |
|------------------------------------------------------------------|



           ***********************************
           NON WORKING AUTOMATIC SERVICES LIST
           ***********************************

Brave Update Service (brave)
Microsoft Edge Update Service (edgeupdate)
Group Policy Client
Intel(R) TPM Provisioning Service
Downloaded Maps Manager
Software Protection
```

Fig. 6. Top 5 Processes and Non-working automatic services list



```
      ***************************************
      HOW LONG EACH APPLICATION HAS BEEN OPEN?
      ***************************************

|----------------------------------------------------------------------------------|
|                       Process - Window Name                | Created On | Time Passed |
|----------------------------------------------------------------------------------|
|  explorer.exe - Taskbar                                    |  10:00:36  |  28:47:03  |
|  WindowsTerminal.exe - C:\WINDOWS\py.exe                   |  14:47:30  |  00:00:09  |
|  explorer.exe - Source                                     |  10:00:36  |  28:47:03  |
|  WindowsTerminal.exe - Jupyter Notebook (anaconda3)        |  10:59:05  |  03:48:34  |
|  NVIDIA Share.exe - NVIDIA GeForce Overlay                 |  10:00:49  |  28:46:50  |
```

Fig. 7. Application running duration

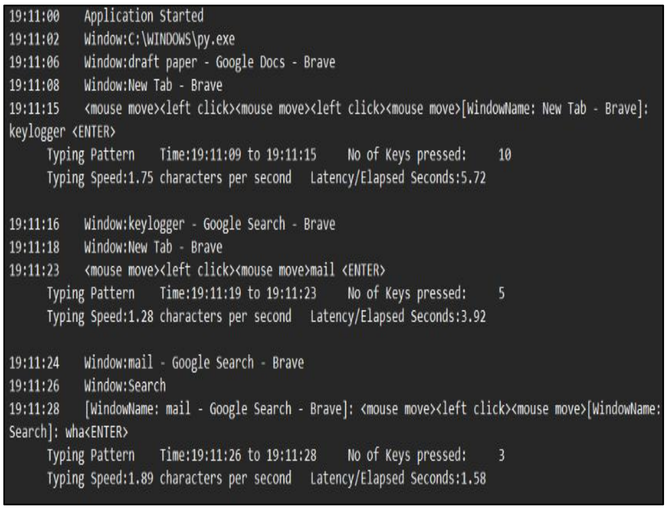


```
                  *********************
                  RUNNING PROCESSES LIST
                  *********************
|----------------------------------------------------------------------|
|                    Process Name                  |   ID   | Memory[%] |
|----------------------------------------------------------------------|
|  AggregatorHost.exe                              |  6168  |    0.11   |
|  ApplicationFrameHost.exe                        |  13748 |    0.43   |
|  DAX3API.exe                                     |  4540  |    0.25   |
|  DAX3API.exe                                     |  7028  |    0.11   |
|  DSRHost.exe                                     |  10144 |    0.07   |
|  FMService64.exe                                 |  4508  |    0.09   |
|  LMS.exe                                         |  4768  |    0.10   |
|  Lenovo.Modern.ImController.PluginHost.Device.exe |  7516  |    0.43   |
|  Lenovo.Modern.ImController.exe                  |  4632  |    0.40   |
|  LocationNotificationWindows.exe                 |  4212  |    0.03   |
|  LockApp.exe                                     |  2524  |    0.14   |
|  MemCompression                                  |  2864  |    2.66   |
|  MonectServer.exe                                |  6848  |    0.07   |
|  MonectServerService.exe                         |  4732  |    0.21   |
```

Fig. 8. Running Processes List

B. Log file

The second output is the log file which is also in a text format. It shows the time details, applications running and their details, the windows and tabs opened, data entered on the windows, and queries searched both online as well as in the system. Function keys like backspace, enter, tab and shift are also captured. For the typing pattern, information like Time duration, number of keys pressed, typing speed(characters per second) and Latency/Elapsed Seconds are used. When compared to physiological bio-metrics, this behavioral biometric is less accurate. In this, two parameters, the time between pressing and releasing a key and the time between two more key presses are taken into account[14].



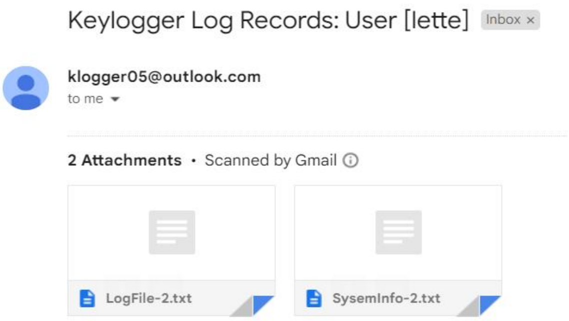
```
19:11:00    Application Started
19:11:02    Window:C:\WINDOWS\py.exe
19:11:06    Window:draft paper - Google Docs - Brave
19:11:08    Window:New Tab - Brave
19:11:15    <mouse move><left click><mouse move><left click><mouse move>[WindowName: New Tab - Brave]:
keylogger <ENTER>
     Typing Pattern    Time:19:11:09 to 19:11:15     No of Keys pressed:     10
     Typing Speed:1.75 characters per second   Latency/Elapsed Seconds:5.72

19:11:16    Window:keylogger - Google Search - Brave
19:11:18    Window:New Tab - Brave
19:11:23    <mouse move><left click><mouse move>mail <ENTER>
     Typing Pattern    Time:19:11:19 to 19:11:23     No of Keys pressed:     5
     Typing Speed:1.28 characters per second   Latency/Elapsed Seconds:3.92

19:11:24    Window:mail - Google Search - Brave
19:11:26    Window:Search
19:11:28    [WindowName: mail - Google Search - Brave]: <mouse move><left click><mouse move>[WindowName:
Search]: wha<ENTER>
     Typing Pattern    Time:19:11:26 to 19:11:28     No of Keys pressed:     3
     Typing Speed:1.89 characters per second   Latency/Elapsed Seconds:1.58
```

Fig. 9. Sample Log File

orized licensed use limited to: AMRITA VISHWA VIDYAPEETHAM AMRITA SCHOOL OF ENGINEERING. Downloaded on January 09,2024 at 13:36:57 UTC from IEEE Xplore. Restrictions ap

C. Mail Transfer

The emails containing the system info and the log file are sent to the configured mail address from the outlook mail id. It will be sent according to the configurations which determine the number of emails within an interval of time.



Keylogger Log Records: User [lette]

klogger05@outlook.com
to me

2 Attachments • Scanned by Gmail

LogFile-2.txt

SysemInfo-2.txt

Fig. 10. Successful email transfer

V. Conclusion and Future Work

The research suggests a novel keystroke logger with keystroke dynamics. By recording keystroke occurrences and mouse clicks without revealing the client, it can function like a basic keylogger to obtain all confidential data from system users. The software can track data, store it in a specific folder, or send it to the owner's email address. While it is running in the background, the software can conceal itself from the system's owner. The methodology significantly raises the bar for seeing the information and obtaining it for either legitimate or illegitimate purposes. For an upcoming study some points are, a method for accurately predicting latency from non-typed keys, or characters that don't show up on the video sequence. Moreover, work on enhancing text pointer tracking and character recognition models for more complex scenarios, such as those involving multiple fonts, scrolling displays, etc. Create a system to deduce and record KeyHolds from a video capture, in addition to KeyDelay timing. Measure the proposed attack's evasion rate and compare it to keystroke dynamics authentication (such as TypingDNA, Behaviosec, etc.). Hopefully, this study will also draw attention to Keystroke Dynamics' susceptibility to behaviour data leakage and the need for computer security researchers and the general public to pay closer attention to potential attacks against Keystroke Dynamic authentication in order to improve its safety down the road.

Acknowledgment

We express our deep gratitude to Amrita Vishwa Vidyapeetham for providing us with valuable advice. We gratefully acknowledge the kind of support, efforts and timely guidance provided by our mentor, Mr Shalu Murali, for completing the research work successfully.

References

[1] Santripti Bhujel, Mrs N. Priya ”Keylogger for Windows using Python” Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 — Issue-1, December2020, pp.566-568.

[2] Siahaan, C.R.P., Chowanda, A. Spoofing keystroke dynamics authentication through synthetic typing pattern extracted from screen recorded video. J Big Data 9, 111 (2022).

[3] M. Harfath, R. Amrith, N. Dulanaka, P. Perera, L. Rupersinga and C. Liyanapathirana, ”Intelligent Cyber Safe Framework for Children,” 2021 IEEE 12th Annual Ubiquitous Computing, Electronics and MobileCommunication Conference (UEMCON), New York, NY, USA, 2021, pp. 0023-0029.

[4] M. Srivastava, A. Kumari, K. K. Dwivedi, S. Jain and V. Saxena,”Analysis and Implementation of Novel Keylogger Technique,” 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2021, pp. 1-6.

[5] A. Singh, P. Choudhary, A. K. Singh and D. K. Tyagi, ”KeyloggerDetection and Prevention”, Journal of Physics: Conference Series, Volume 2007, 3rd International Conference on Computational and Experimental Methods in Mechanical Engineering (ICCEMME) (2021)11-13.

[6] A. P. Singh and V. Singh, ”Infringement of Prevention Technique against Keyloggers using Sift Attack,” 2018 International Conference on Advanced Computation and Telecommunication (ICACAT), Bhopal,India, 2018, pp. 1-4.

[7] 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, Cairns, QLD, Australia, 2007, pp. 314-318.

[8] K. Nasaka, T. Takami, T. Yamamoto and M. Nishigaki, ”A Keystroke Logger Detection Using Keyboard-Input-Related API Monitoring,” 2011 14th International Conference on Network-Based Information Systems, Tirana, Albania, 2011, pp. 651-656.

[9] A. P. Kuncoro and B. A. Kusuma, ”Keylogger Is A Hacking Technique That Allows Threatening Information On Mobile Banking User,” 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 2018, pp. 141-145

[10] A. Solairaj, S. C. Prabanand, J. Mathalairaj, C. Prathap and L. S. Vignesh, ”Keyloggers software detection techniques,” 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2016, pp. 1-6

[11] V. S. Mohan, V. R, S. KP and P. Poornachandran, ”S.P.O.O.F Net: Syntactic Patterns for identification of Ominous Online Factors,” 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA,2018, pp. 258-263

[12] S. Akarsh, S. Sriram, P. Poornachandran, V. K. Menon and K. P. Soman, ”Deep Learning Framework for Domain Generation Algorithms Prediction Using Long Short-term Memory,” 2019 5th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 666-671.

[13] Faaiz Anwar, S. Saravanan, ”Comparison of Artificial Intelligence Algorithms for IoT Botnet Detection on Apache Spark Platform”, Procedia Computer Science, Volume 215, 2022, Pages 499-508, ISSN 1877-0509.

[14] N. Lalithamani, D. R. Balaji and S. S. Dev, ”Survey on nonobstructive and continuous user authentication on mobile devices,” 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2017, pp. 1-6.

[15] N. S. Subramanian, S. Narayanan, M. D. Soumya, N. Jayakumar, K. Bijlani, ”Using Aadhaar for Continuous Test-Taker Presence Verification in Online Exams”, Information and Decision Sciences, 2018, Volume 701, ISBN: 978-981-10-7562-9.

[16] P. R and S. Sankaran, ”An Experimental Platform for Security of Cyber Physical Systems,” 2019 IEEE International Symposium on SmartElectronic Systems (iSES) (Formerly iNiS), Rourkela, India, 2019, pp. 123-128.

orized licensed use limited to: AMRITA VISHWA VIDYAPEETHAM AMRITA SCHOOL OF ENGINEERING. Downloaded on January 09,2024 at 13:36:57 UTC from IEEE Xplore. Restrictions ap