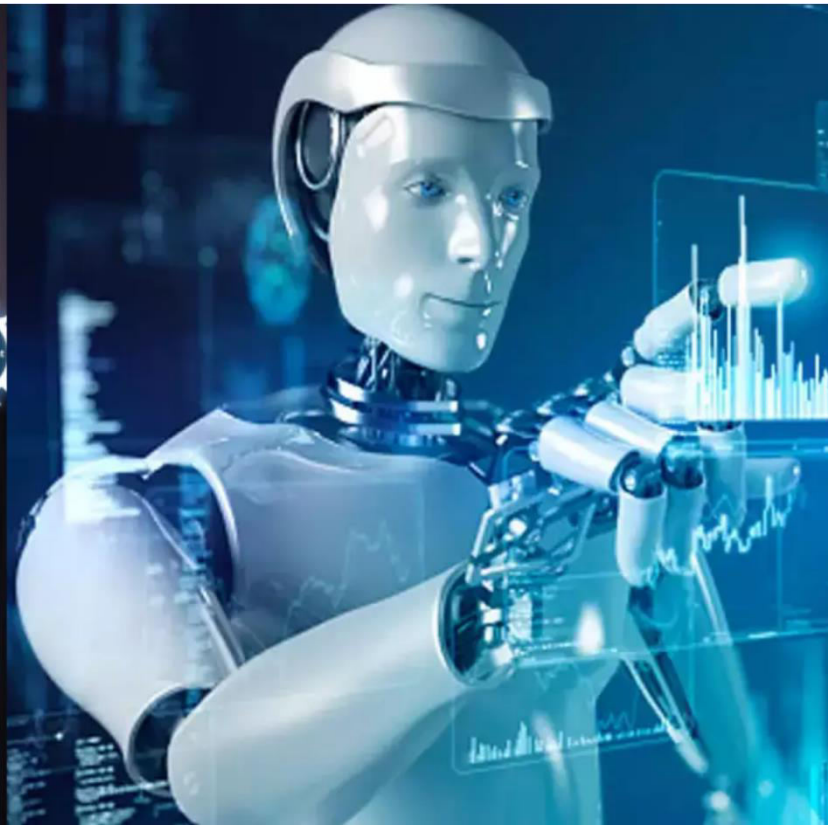
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404139|

Surveillance of System Activity using a Software Keylogger

Assistant Prof. S. Yoheswari[1], Priyadharshini O S[2], Puveia J P[3]

Professor and Faculty Mentor, Dept. of Computer Science and Engineering, K.L.N College of Engineering, Madurai, Tamil Nadu, India

B. E Student, Dept. of Computer Science and Engineering, K.L.N College of Engineering, Madurai, Tamil Nadu, India

ABSTRACT: In many companies, data security and recovery are now the most important factor. In many cases where data recovery is required. For these kinds of problems, a keylogger is one of the best solutions, which is often referred to as keylogging or keyboard capture. Key capping is the act of recording keystrokes on a keyboard, usually covertly so that the person using the keyboard does not know that their actions are being monitored. With the help of keylogger application, users can get the data when the working file is corrupted due to several reasons like power loss etc. This is a tracking application used to track the users which records the keystrokes; uses log files to retrieve information. Using this application, we can recall a forgotten email or URL. In this keylogger project, whenever the user types something on the keyboard, the keystrokes are captured and sent to the admin email address within a set time.

KEYWORDS: Surveillance, Keylogger, Keystrokes, System Monitoring

I. INTRODUCTION

In many IT infrastructure organizations now-a-days, data security and data recovery are the most important factors which is basically deployed in Computer Forensics. Computer forensics consists of the art of examining digital media to preserve, recover and analyse the data in an effective manner. There are many cases where data recovery is required essentially. So, by using keylogger application users can retrieve data in the time of disaster and damaging of working file due to loss of power etc. This is a surveillance application used to track the users which log keystrokes, uses log files to retrieve information, capture a record of all typed keys. The collected information is saved on the system as a hidden file or emailed to the admin or the forensic analyst.

II. LITERATURE SURVEY

In [1] Exploring the application of keystroke logging techniques to research in second language (L2) writing-Yu Tiana, Sarat. Cushing. This model Keystroke logging is a strong but subtle technique for investigating second-language (L2) writing processes by recording real-time keystroke, pause, and revision data. In contrast to more intrusive methods such as think-aloud protocols, keystroke logging yields fine-grained information about planning, fluency, and revision behaviour. Software like Input log and FlexKeyLogger facilitates the analysis of writing patterns, supporting cognitive models that treat writing as a recursive process. This technique has applications in writing assessment, automated evaluation, and instruction, providing data-driven feedback to enhance writing approaches. Some of the challenges include pauses, dealing with large databases, and ethical issues of privacy. In spite of all these limitations, keystroke logging, when combined with complementary techniques, provides a rich source of information on L2 writing development.

In [2] Real-Time Data Security: USB Keyboard Encryption for Preventing Keylogging Attacks - Blessy K, Anandharaj G, Anafa Rumana S, Blessy K, Sabreen S, Dr. R. Ravi. This model explores into the creation and use of hardware keyloggers for monitoring, data recovery, and security tracking by silently recording keystrokes and sending logs by email. Compared to software keyloggers, hardware keyloggers work at a lower level, and hence they are more difficult to identify and uninstall. Though they provide benefits in system monitoring and data recovery, the paper raises ethical and legal issues since unapproved monitoring will infringe on privacy legislation

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404139|

and erode organizational trust. Also, ongoing keylogging can reduce system performance and introduce cybersecurity threats if not appropriately secured. The research concludes that although keyloggers can prove to be useful tools, their use must reconcile security requirements with ethical and privacy issues.

In [3] HookTracer: Automatic Detection and Analysis of Keystroke Loggers Using Memory Forensics- Andrew Case, Ryan. DiMaggio, Md Firoz-Uli-Amin, Mohammad Bayatti M. Jalozai. This model explores Hook Tracer, a new memory forensics-based detector and analyser for keystroke loggers. Different from common filesystem-based forensic analysis, Hook Tracer specifically deals with memory-only malware, where no disk footprint is present. Hook Tracer extends the plugin of message hooks in Volatility to classify automatically hooks as malware or harmless without the necessity for reverse engineering by hand. One of its key features is that it can emulate keystrokes within an emulated environment, initiating keylogger action for automated detection. The tool accommodates both 32-bit and 64-bit executables and enhances forensic processes by allowing even inexperienced investigators to identify keyloggers.

In [4] Alpha logger: Detecting Motion Based Side Channel Attack Using Smart Phone Keylogger- Abdul Rehman Javed, Muhammad Asim, Ali Hilal Al Bayatti. Alpha Logger, an Android application, illustrates motion-based side-channel attacks using accelerometer, gyroscope, and magnetometer readings to predict keystrokes. Recording sensor data at 10Hz, it uses ML algorithms such as Decision Trees and SVM, with 90.2% accuracy using accelerometer and magnetometer. The research identifies security threats from uncontrolled sensor access, although its emphasis on Android and exclusion of special characters restrict practical use.

III. EXISTING SYSTEM

Keystroke logging records elaborate writing processes by recording all key presses on writing tasks. Keystroke measures such as typing pace, pauses, and corrections show cognitive processes of planning, editing, and revising and indicate how writers construct and refine ideas. Keystroke logging extends writing instruction and assessment through the examination of writer's cognitive activity and development. Input log and FlexKeyLogger are keystroke logging tools for controlled and online settings. The system illustrates how keystroke logging software monitors writing habits, providing windows into cognitive processes, strategies, and revisions.

IV. PROPOSED SYSTEM

Software keyloggers offer a convenient alternative to hardware keyloggers by being installable and controllable remotely without involving direct access to the target device. The suggested software installs itself onto an intended system if the user simply clicks on the link via an email or on social media. After it is installed, the software continuously monitors and logs all keystrokes input by the user on their system keyboard, intercepting information like user's messages. The keystrokes are then collated in text form and automatically emailed to a specified email address, providing real-time access to the logged information. The Keylogger sends logged keystrokes securely over SMTP to an admin email.

V. METHODOLOGY

5.1 Pynput Keylogging

The `pynput` library in Python is a powerful tool for monitoring and controlling input devices such as keyboards a mouse, offering modules like `pynput. Mouse` and `pynput. Keyboard` for handling various input events. It allows developers to listen for keystrokes and mouse movements, as well as simulate input, making it highly effective for automation tasks and system controls. But with its utility comes the possibility of being used for nefarious purposes, like illicit keylogging and monitoring of users without permission. Through the recording of keystrokes, an application can also trace out sensitive user information, which, if abused, may result in privacy invasions or security violations. Once keystrokes are logged through `pynput`, the information can be sent to an administrator's email securely for continued monitoring and analysis. Although this type of surveillance is capable of understanding user behaviour, evaluating potential threats to security or improving cybersecurity methodology, it causes ethical and lawful issues in regard to privacy as well as consent.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404139|

5.2 Threaded keylogger

Threading is important in allowing a keylogger to effectively record user keystrokes in real time while at the same time performing other critical functions without lag or delay. The main thread of the keylogger is tasked with continuously recording keystrokes, while a second thread effectively handles the storage of this information by saving it to a file or sending it to an administrator's email. This concurrent processing greatly improves the performance of the keylogger by insuring keystroke information is recorded smoothly while at the same time executing operations such as data storage and transmission without a bottleneck. The keystrokes are recorded into a specific data structure, which is then read by an email-sending thread to send periodic updates to an administrator in a timely manner. Moreover, efficient thread management ensures that all currently running threads shut down when the program terminates to avoid resource leak and maintain system stability.

5.3 SMTP Communication

Keyloggers utilize SMTP to send captured keystrokes undetected to a remote server or email, so data is always available even when the system crashes. Since they utilize regular email channels for operation, their presence can remain undetected, making them suitable for ethical and nefarious purposes alike. Companies use them for employee monitoring or data recovery to assist in the recovery of lost data in situations of file corruption due to accidental actions or power outage. Yet, keyloggers also present serious security threats when hacked by malicious individuals to steal sensitive information, which results in identity theft, monetary fraud, and privacy violations. Their capability of silently exfiltrating information over SMTP makes them especially dangerous because the victims will not be aware of the invasion. Although keyloggers are used for their legitimate purposes, their misuse has serious ethical and legal implications and emphasizes the implementation of strict security controls to deter unauthorized access and data theft.

5.4 Deploying Keylogger

A keylogger captures keystrokes, even prior to an event taking place, in order to avert data loss due to crashes or accidental termination. It saves sensitive data such as URLs and email addresses to a log file or database. For security purposes and remote accessibility, it sends data through email using SMTP. Aside from keystroke logging, it also saves metadata such as timestamps, application usage, and mouse clicks. This information assists in system diagnosis, security scanning, and behavioural inspection. With ongoing observation of user action, a keylogger facilitates the monitoring of interactions for ensured control and recall of lost data when necessary.

VI. SYSTEM ARCHITECTURE

A Software Architecture Diagram gives a top-down view of a system, showing its essential elements, relationships, and data flow. It features modules that process particular functionalities, interfaces that specify communication among components, and data flow paths that outline how information is processed. It can also reflect deployment information, indicating how components are spread over servers or cloud hosts. This diagram acts as a roadmap for developers and stakeholders, providing clarity, scalability, and streamlined system design while allowing collaboration and decision- making.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404139|

The Software keylogger through email architecture diagram is as shown in Fig 1.

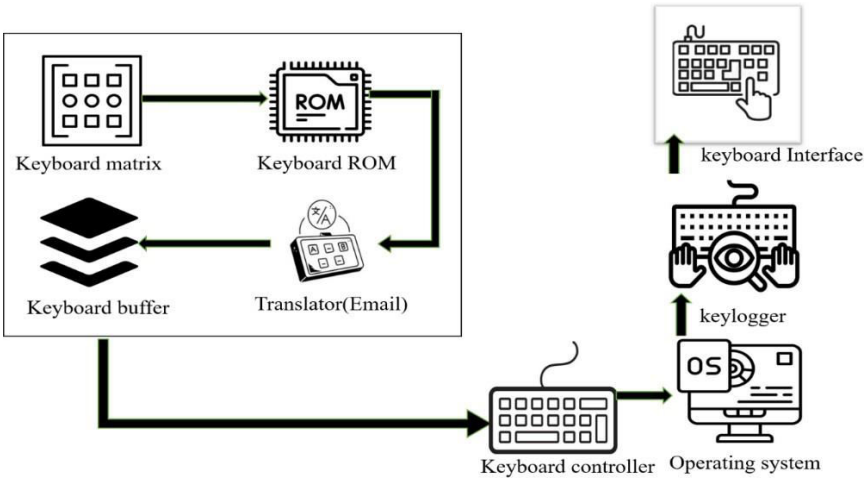


Fig.1 Architecture of the system

This system illustrating the operation of a keylogger in a keyboard input system. Upon pressing a key, the keyboard matrix registers it and transmits the signal to the keyboard ROM for processing. The data is then transferred to the keyboard buffer before it is transmitted to the keyboard controller and the operating system (OS) for use by the application. But a keylogger catches the keystrokes before they are sent to the OS, stealing sensitive information. The keylogger sends the captured data through a translator (Email) module. Lastly, the keystrokes are handled by the keyboard interface, enabling external monitoring of user inputs.

VII. EXPERIMENTAL RESULTS

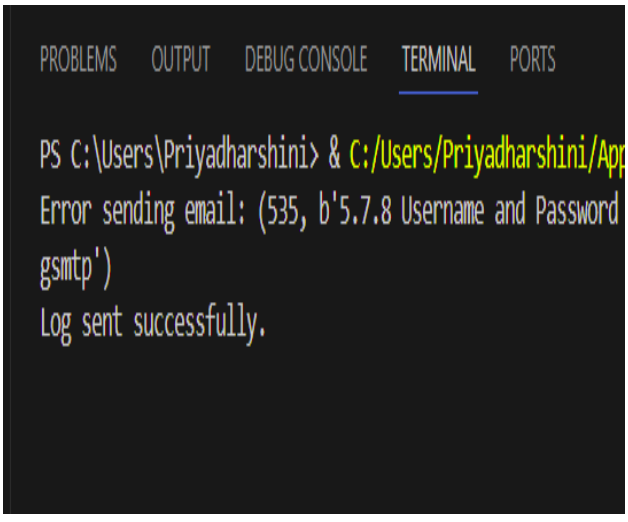


Fig 2. Logging confirmation

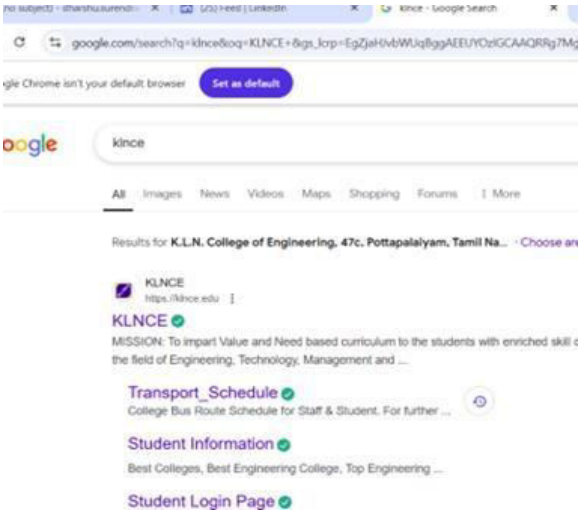


Fig 3. Keystroke Logging

In this Fig 2 Shows the confirms that the logging process, such as capturing user actions, system events, or security logs, has been successfully completed. Fig 3 shows the User types on keyboard in website and keystroke captured on every key pressed, its often used for monitoring user activity.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404139|

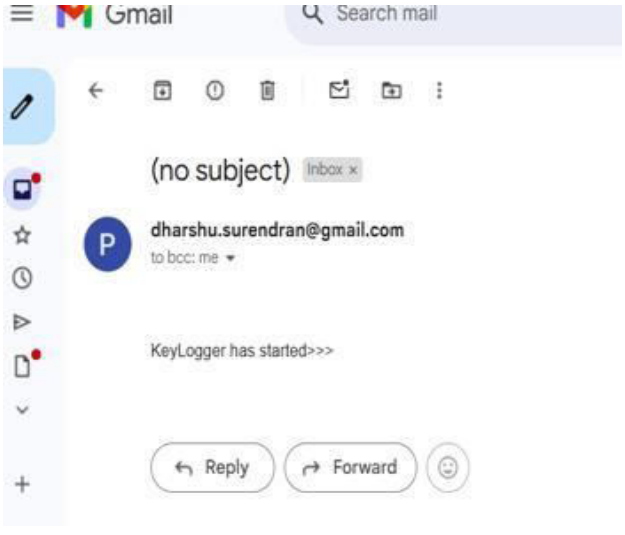


Fig 4. Keylogger Activation Alert

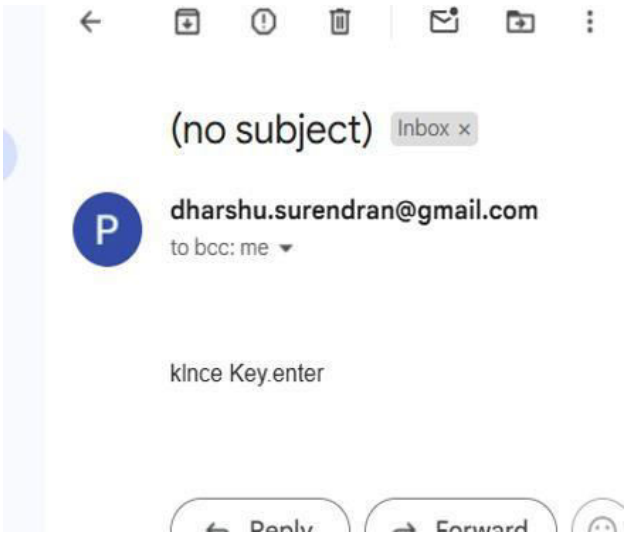


Fig 5. Captured Keystrokes sent to Admin through email

In this Fig 4 refers to a warning message indicating that a keylogger has been activated. Fig 5. From the screenshot, the keylogger has successfully captured the user's keystrokes. The user typed "klnce" and pressed the Enter key, which is recorded as "Key.enter". The keylogger is working perfectly and sending the captured keystrokes to the admin email for monitoring purposes.

VIII. CONCLUSION

A keylogger is a monitoring software that captures all keystrokes input on a keyboard, usually in secret. Alternatively, a keylogger also goes by the name of a keyboard capturer. Keyloggers can run secretly in the background, quietly capturing all typed content such as emails, messages, passwords, and other confidential information. Although the term has a generally negative connotation because of its link to malicious hacking and information theft, keyloggers do have legitimate uses. Employers can lawfully install keyloggers on devices owned by companies to maintain productivity and enforce adherence to company policies. Parents might use them to monitor their children's internet use. Ethical hackers in cybersecurity occasionally use keyloggers to scan system vulnerabilities. Yet, due to the abuse potential, the use of keyloggers has to be managed responsibly, with appropriate consent and legal supervision. Misuse can result in severe privacy invasions and legal repercussions, particularly when used to steal confidential or personal data.

REFERENCES

[1] Abdul Rehman Javed, Mirza Omer Beg, Muhammad Asim, Thar Baker, Ali Hilal Al-Bayatti 'Alpha logger: Detecting Motion Based Side Channel Attack Using Smart Phone Keylogger' on Springer Year:2020, Volume no:14, pp:4869–488

[2] Andrew Case, Ryan. DiMaggio, Md Firoz-Uli-Amin, Mohammad Bayatti M. Jalozai, "HookTracer: Automatic Detection and Analysis of Keystroke Loggers Using Memory Forensics" on Elsevier Year:2020 vol no:96, Issue 20

[3] Arjun Singh, Pushpa Choudhary, Akhilesh Kumar Singh, Dheerendra Kumar Tyagi "Keylogger Detection and Prevention" on IOP of Conferences Year:2021, Vol no :7, pp: 1742-6596.

[4] Atiya Kazi, Manthan Mungekar, Dnyanesh Sawant, Pankaj Mirashi, "Keylogger Detection", on ResearchGate Year: 2023, Vol no: 5, Issue no: 4.

[5] Blessy K, Anandharaj G, Anafa Rumana S, Blessy K, Sabreen S, Dr. R. Ravi, "Real-Time Data Security: USB Keyboard Encryption for Preventing Keylogging Attacks " on Elsevier Year: 2024, Vol no:11, Issue no: 9.

[6] Daniela Oliveira, Jesus Navarro, Enrique Naudon, "Bridging the Semantic Gap to Mitigate Kernel-level Keyloggers" on IEEE Year :2012, Vol no: 75.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404139|

[7] Robbi Rahim, Heri Nurdiyanto, Ansari Saleh A, Dahlan Abdullah, Dedy Hartman, and Darmawan Napitupulu,' Keylogger Application to Monitoring Users Activity with Exact String-Matching Algorithm' on Elsevier Year:2018, Vol no: 8, Issue 95.

[8] Yu Tiana, SaraT. Cushing,"Exploring the application of keystroke logging techniques to research in second language (L2) writing" on Elsevier Year: 2025,Volume no :4,pp:2772-7661.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details