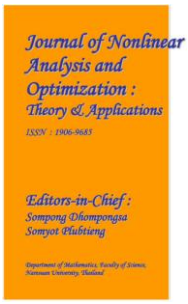
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 2, No.1 : 2024
ISSN : **1906-9685**



ENHANCING KEYBOARD AND MOUSE EVENT LOGGER WITH JSON STORAGE

Akshaya S Student, III Year (Digital Cyber Forensic Science) Rathinam College of Arts and Science, Coimbatore-21
Dr. Ramraj M., Ph.D. Assistant Professor Department of Digital Cyber Forensic Science Rathinam College of Arts and Science, Coimbatore-21

ABSTRACT

This system is designed to store data in JSON format and keep a record of keyboard keystrokes and mouse movements, clicks, and other interactions on a computer. The keylogger component monitors keyboard inputs discreetly, recording each keystroke along with relevant metadata such as timestamp and application context. This data is then organized into JSON format, which makes it easy to store and analyze. The mouse event logger captures a range of mouse activities, including cursor movements, button clicks, and scroll actions. This augments the keystroke data with a more complete picture of user interactions. JSON ensures flexibility and scalability in data representation, making it easy to integrate with various applications and platforms for further processing and analysis. Furthermore, JSON's lightweight and human-readable structure makes it ideal for efficiently storing and transmitting logged events while maintaining data integrity.

INTRODUCTION:

. Keyloggers, or keystroke loggers, are tools that record what a person types on a device. While there are legitimate and legal uses for keyloggers, many uses for keyloggers are malicious. In a keylogger attack, the keylogger software records every keystroke on the victim's device and sends it to the attacker. It can be either hardware- or software-based. The latter type is also known as system monitoring software or keyboard capture software. Either way, keylogging software allows an unauthorized threat actor to view the user's keystrokes, and then use this knowledge to access and compromise the device. Software Key loggers, also known as keystroke loggers, record the keys hit on a device and save them to a file, which is then accessed by the person who deployed the malware.
A keylogger and mouse event logger program does not require physical access to the user's computer for installation. It can be purposefully downloaded by someone who wants to monitor activity on a particular computer, or it can be malware downloaded unwittingly by the user of the keyboard and its device, and then executed as part of a rootkit or remote administration Trojan. Whenever the user clicks any keystroke or clicks the mouse will be monitored and the log will be stored in the json file which I have inserted with the project. So the user can also monitor the logs of the keystrokes and mouse events.

FEASIBILITY STUDY

A system is a feasible system only if it is feasible within limited recourse and time. In this system every process can be feasible for the user and also a developer. The different types of feasible systems that have to be analyzed are,

1. Technical Feasibility
2. Behavioral Feasibility
3. Economical Feasibility
4. Operational Feasibility

Technical Feasibility:

Technical Feasibility is the assessment of the technical view of the system. The technical feasibility of creating a keylogger depends on several factors:

• **Operating System Compatibility:** Keyloggers and mouse event loggers can be developed for various operating systems such as Windows, macOS, and Linux. Each operating system has its APIs and mechanisms for capturing keyboard and mouse events.

• **Permissions and Security:** Depending on the operating system and user permissions, capturing keyboard and mouse events may require elevated privileges

• **Anti-Malware Considerations:** Keyloggers and mouse event loggers are often flagged as potentially unwanted or malicious software by antivirus and anti-malware programs. Developers need to be aware of this and consider ethical implications when creating such software.

• **Data Storage and Privacy:** Captured keystrokes and mouse events contain sensitive user data. Developers must handle this data with care, ensuring it is stored securely and used responsibly. Unauthorized access to this data could lead to privacy breaches and legal consequences.

• **Monitoring and Logging Mechanisms:** The keylogger/mouse event logger needs to efficiently capture events without significantly impacting system performance. This involves designing efficient event monitoring and logging mechanisms.

Behavioural Feasibility:

The behavioral feasibility of a keylogger and mouse event logger refers to assessing whether such software aligns with users' behavior, needs, and expectations. Here are some considerations regarding the behavioral feasibility:

• **User Acceptance:** Keyloggers and mouse event loggers may not be readily accepted by users due to privacy concerns. Users may perceive such software as invasive and may be reluctant to install or use it unless they have a clear understanding of its purpose and implications.

• **Ethical Considerations:** Developers must consider the ethical implications of developing and deploying keyloggers and mouse event loggers. Respecting user privacy, ensuring data security, and using the software responsibly are essential for maintaining behavioral feasibility.

• **Legitimate Use Cases:** While keyloggers and mouse event loggers are often associated with malicious activities, there are legitimate use cases such as parental control, employee monitoring in organizations, and accessibility features for users with disabilities. Highlighting these use cases can improve the acceptance of such software.

Economical Feasibility:

The economic feasibility of keyloggers and mouse event loggers involves assessing the financial viability and potential costs and benefits associated with developing, deploying, and using such software. Here are some considerations regarding the economic feasibility:

• Developing keylogger and mouse event logger software involves costs associated with software development, including personnel, tools, and resources. The complexity of the software, the required features, and the expertise of the development team can impact development costs.

• After development, ongoing maintenance and support are necessary to ensure the software remains functional, secure, and compatible with evolving operating systems and hardware platforms. Maintenance costs may include bug fixes, updates, and customer support.

.Operational Feasibility:

Operational feasibility for keyloggers and mouse event loggers refers to assessing whether such software can be effectively integrated into existing systems and processes and whether it meets the operational needs and requirements of users. Here are some considerations regarding the operational feasibility:

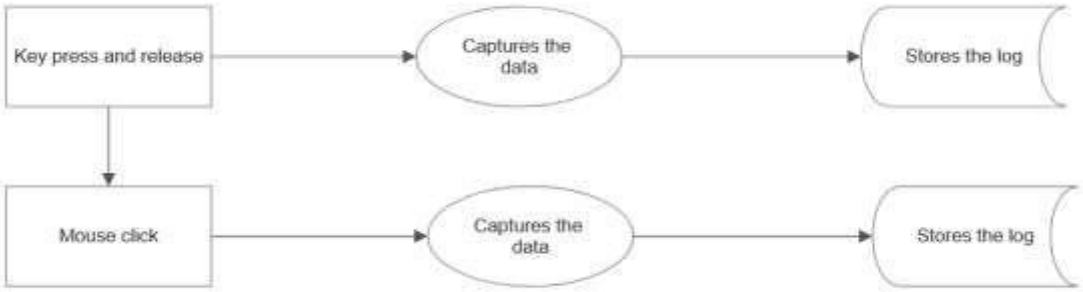
• **Ease of Installation and Configuration:** The software should be easy to install and configure, even for users with limited technical expertise. Clear documentation and user-friendly interfaces can facilitate the installation and setup process.

• **Performance and Reliability:** The software should perform reliably under normal operating conditions, without causing excessive system slowdowns or errors. It should accurately capture keystrokes and mouse events without significant delays or interruptions.

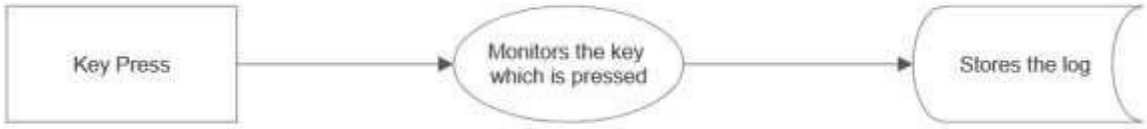
• **Security and Data Protection:** Keylogger and mouse event logger software should adhere to best practices for security and data protection. This includes implementing encryption, access controls and other security measures to prevent unauthorized access to captured data.

DATA FLOW DIAGRAM

Level 0:



The keylogger and mouse event logger are tools that capture keystrokes and mouse click coordinates. They record both key press and key release strokes and save them in a log. Similarly, the mouse click coordinates are also captured and stored in a log.**Level 1:**

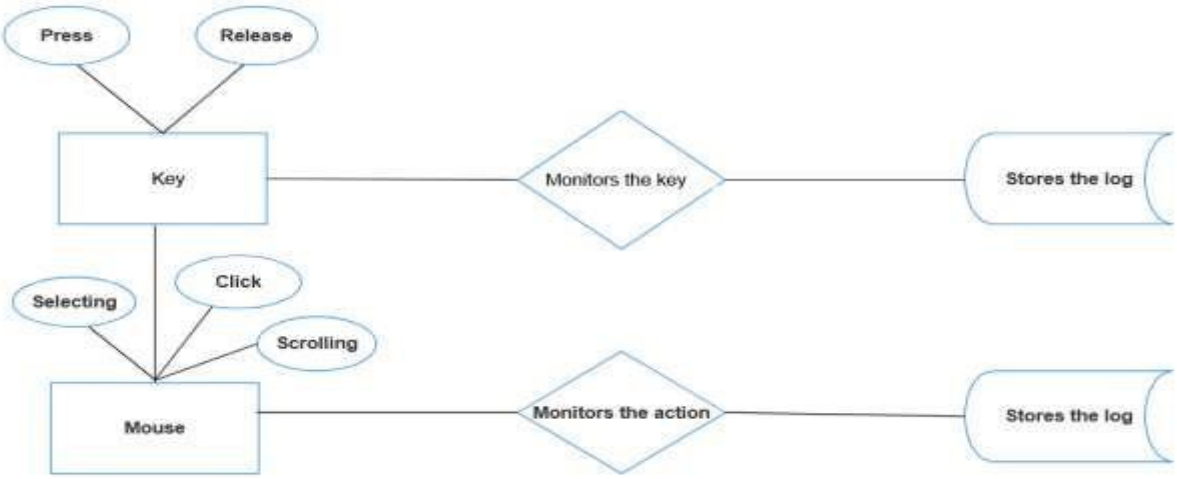


The program will monitor the keys pressed by the user in the system and log them with timestamps. Only the keys that are pressed will be recorded, which is the first attribute of the keylogger.

Level 2:

The program will monitor the keys released by the user in the system and log them with timestamps. Only the keys that are released will be recorded, which is the second attribute of the keylogger. **Level 3:**

At this level, the program will monitor the coordinate point of the mouse click and store it in the log.



CONCLUSION

In conclusion, the implementation of a keylogger and mouse event logger utilizing JSON offers a potent means of capturing and organizing user input data efficiently. By leveraging JSON's structured format, both key presses and mouse events can be comprehensively recorded, enabling detailed analysis and monitoring. This method facilitates seamless integration with various applications and

platforms, enhancing versatility and usability. Moreover, JSON's lightweight nature ensures minimal overhead, optimizing performance and resource utilization. However, it's crucial to prioritize security measures to safeguard sensitive user information from potential breaches or misuse. Overall, the combination of keylogging and mouse event logging with JSON presents a robust solution for monitoring user interactions while maintaining flexibility and data integrity.

Acknowledgment

This article / project is the outcome of research work carried out in the Department of **Computer Science** under the DBT Star College Scheme. The authors are grateful to the Department of Biotechnology (DBT), Ministry of Science and Technology, Govt. of India, New Delhi, and the Department of **Computer Science** for the support.

BIBLIOGRAPHY

Books Referred:

• "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig.
• "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto.
• "Black Hat Python: Python Programming for Hackers and Pentesters" by Justin Seitz.
• "Hacking: The Art of Exploitation" by Jon Erickson.
• "Learning Python" by Mark Lutz.

Websites:

• GitHub Repository: Many developers share code related to keyloggers and mouse event loggers on GitHub.
• Stack Overflow: This popular programming Q&A website often features discussions and solutions related to keyloggers and mouse event loggers, offering insights from experienced developers and security professionals.
• Security-focused Websites and Blogs: Websites such as Krebs on Security, The Hacker News, and Schneier on Security frequently cover topics related to cybersecurity, including keyloggers and mouse event loggers.