International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

KEYLOGGER ETHICAL KEY LOGGING APPLICATION FOR BALANCING USER PRIVACY WITH SYSTEM SAFETY

ARUNPANDI M[1], HEMANTHRAJ S[2], SUMAN S[3]

[1]*Department of Computer Science and Business Systems, Jeppiaar Institute of Technology*
[2]*Department of Computer Science and Business Systems, Jeppiaar Institute of Technology*
[3]*Department of Computer Science and Business Systems, Jeppiaar Institute of Technology*

Abstract - The project presents a Python-based ethical keylogging application designed for use in controlled environments to enhance system security while maintaining user privacy. The system records user keystrokes, stores them in log files, and sends periodic email reports to authorized administrators. It operates either in the background or through a user interface, ensuring flexibility and transparency. The primary objective is to monitor user activity, detect unauthorized access, and identify potential insider threats at an early stage. Unlike traditional security mechanisms such as firewalls and antivirus software, this application provides detailed, real-time keystroke-level monitoring. The methodology involves capturing keyboard inputs, securely logging data, and automating email notifications. Testing results demonstrate accurate keystroke capture, reliable log storage, and successful email delivery. The system emphasizes ethical usage through proper authorization and user consent. This approach ensures a balance between security monitoring and privacy protection. The project also highlights future enhancements, including graphical user interface development, encrypted log storage, multi-platform compatibility, and integration with advanced security systems such as SIEM tools.

Key Words: Keylogger, Ethical Monitoring, Keystroke Logging, Cybersecurity, User Activity Tracking, Python Application.

1.INTRODUCTION

In the modern digital era, the security of computer systems and networks has become a paramount concern for organizations, educational institutions, and individuals alike. As technology continues to evolve rapidly, threats to information security have also increased in complexity and frequency. Among these, insider threats, unauthorized access, and internal misuse of systems represent some of the most critical challenges in cybersecurity.

To address these concerns, monitoring tools such as keyloggers have been developed. A keylogger is a software-based application designed to record the keystrokes entered by a user on a computer system. It can operate discreetly in the background without interrupting normal operations or function as a visible program with an interface accessible to authorized administrators. When implemented ethically with proper authorization and user consent, keyloggers become valuable tools for system monitoring, threat detection, and user behavior analysis.

In controlled environments such as organizational IT infrastructures, educational laboratories, and enterprise security systems, keyloggers assist administrators in tracking user activities, identifying suspicious behavior, and ensuring compliance with security policies. Unlike traditional passive security mechanisms such as firewalls and antivirus software, keyloggers provide an active monitoring layer by capturing detailed input-level data, enabling early detection of potential security breaches.

2. Body of Paper

2.1 Existing System

Existing security systems such as firewalls, antivirus software, and system logs provide protection against external threats. However, they do not offer real-time monitoring of user activities and have limited capability in detecting insider threats or misuse within the system.

2.2 Limitations

- Lack of real-time user activity tracking
- Ineffective detection of insider threats
- Limited visibility into user behavior
- Dependence on predefined threat patterns
- Delayed response to suspicious activities

2.3 Proposed System

The proposed system is a Python-based ethical keylogger designed to monitor user keystrokes in real time. It records inputs, stores them in log files, and sends email reports to authorized administrators. The system ensures ethical usage through proper authorization and user consent while improving security monitoring.

2.4 Implementation

The system is implemented using Python with modules for capturing keystrokes, storing logs, and sending emails. It operates in the background without affecting system performance, continuously records user input, and periodically sends the collected data to authorized users for analysis.

Table -1: System features and descriptions

Feature	Description	Purpose
Keystroke Logging	Captures user keystrokes in real time	Monitor user activity
Background Operation	Runs silently in the background	Ensure continuous monitoring
Log Storage	Stores data in log files	Maintain activity records
Email Reporting	Sends logs to admin via email	Enable remote monitoring
Data Formatting	Converts special keys to readable format	Improve data clarity
Authorization	Works with user permission	Ensure ethical usage
Real-time Monitoring	Tracks activity continuously	Detect suspicious actions early

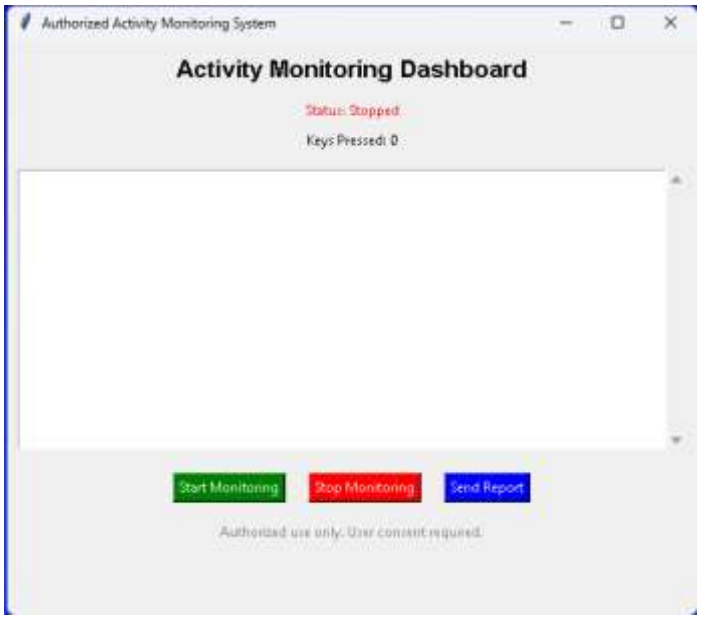

Fig -1: Figure

Output
the dashboard displays the current status and shows the number of keys pressed. A large area is provided to display captured keystrokes, and the interface is designed to be simple and easy to use while ensuring authorized and ethical monitoring.

- Start Monitoring: Begins capturing keystrokes
- Stop Monitoring: Stops the keylogging process
- Send Report: Sends the recorded data via email

3. CONCLUSIONS

The project "KEYLOGGER - Ethical Key Logging Application" provides an effective solution for real-time monitoring in controlled environments. It captures keystrokes, stores logs, and sends email reports to authorized users using Python libraries. The system is lightweight, accurate, and supports ethical monitoring with user consent. Compared to existing systems, it offers real-time tracking and automated reporting at no cost. Although currently a prototype, it can be further improved with features like GUI, encryption, and advanced security integration.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to the faculty members for their valuable guidance, support, and encouragement throughout the development of this project. We also thank our institution for providing the necessary resources and environment to successfully complete this work. We are grateful to all those who directly or indirectly contributed to the completion of this project.

REFERENCES

1. N. Provos and D. Mavrommatis, "Virtual honeypots: From botnet tracking to intrusion detection," USENIX Security Symposium, 2006.
2. W. Stallings, Network Security Essentials: Applications and Standards, 6th ed., Pearson Education, 2017.
3. P. Samarati and S. de Vimercati, "Access control: Policies, models, and mechanisms," Foundations of Security Analysis and Design, Springer, 2001.
4. ISO/IEC 27001, Information Technology - Security Techniques - Information Security Management Systems, International Organization for Standardization, 2013.
5. Laudon, K. C., & Traver, C. G. (2022). E-commerce: Business, Technology, Society. Pearson Education.