Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140

Volume 15 Issue 01, 2026

Keylogger Detection System with Real-Time Notification

[1]Iyolin yohitha A., [2]Sugi L.,[3]Dharshini. J., [4]Sajitha M.S. (AP/IT)

[1,2,3,4] Department of Information Technology, Arunachala College of Engineering for Women, Manavilai, Vellichanthai, Tamil Nadu, India

Peer Review Information

Submission: 08 March 2026

Revision: 26 March 2026

Acceptance: 05 April 2026

Keywords

keylogger detection, cybersecurity, behavioral analysis, real-time notification, malware detection

Abstract

In the modern digital age, the use of computers and internet-based systems has become an essential part of everyday life. From online banking and e-commerce to communication and education, people rely heavily on digital platforms to perform various activities. However, this rapid growth in digital dependency has also led to an increase in cyber threats and security vulnerabilities. One of the most dangerous forms of malware used by attackers is a keylogger, which is designed to secretly record the keystrokes of a user without their knowledge. These keystrokes often include sensitive information such as usernames, passwords, credit card details, and private communications, making keyloggers a serious threat to personal and organizational security.

The proposed Keylogger Detection System with Real-Time Notification aims to provide a robust and efficient solution to this problem. Instead of relying solely on traditional signature-based detection methods, the system uses behavioral analysis techniques to monitor system activities continuously. It observes how applications interact with keyboard inputs and identifies suspicious patterns that may indicate keylogging behavior. Once such activity is detected, the system immediately generates a real-time notification to alert the user, allowing them to take quick preventive measures. This approach not only enhances detection accuracy but also significantly reduces the response time, thereby minimizing potential damage caused by keylogging attacks.

Introduction

With the increasing integration of technology into daily life, cybersecurity has become a critical area of concern. Individuals and organizations store a large amount of sensitive information on their devices, making them attractive targets for cybercriminals. Among various types of cyber threats, keyloggers are particularly harmful because they operate silently and capture user input without raising any visible alerts. This makes them highly effective tools for attackers who aim to steal confidential data.

Keyloggers can enter a system through multiple sources, such as malicious email attachments, infected software downloads, compromised websites, or external storage devices. Once installed, they begin recording keystrokes and transmitting the data to an attacker. The user remains unaware of this activity, which makes keyloggers extremely dangerous.

Traditional antivirus software is often ineffective against modern keyloggers because it relies on known malware signatures. New and advanced keyloggers can easily bypass such systems using techniques like code obfuscation and encryption. Therefore, there is a need for a more advanced detection mechanism that focuses on identifying suspicious behavior rather than matching known patterns.

The system proposed in this project addresses this need by implementing a real-time monitoring approach. It continuously observes

system processes and keyboard interactions, identifies anomalies, and alerts the user instantly. This proactive approach ensures better protection against both known and unknown threats.

Literature Review

Over the past few decades, researchers and cybersecurity experts have developed various methods to detect and prevent malware, including keyloggers. One of the earliest approaches is signature-based detection, which involves comparing files and programs against a database of known malware signatures. While this method is effective for identifying previously known threats, it fails to detect new or modified keyloggers that do not match existing signatures.

To overcome this limitation, heuristic analysis was introduced. This method evaluates the behavior of programs and identifies suspicious activities such as unauthorized access to system resources. Although heuristic methods can detect unknown threats, they sometimes generate false positives, which may lead to unnecessary alerts.

Behavior-based detection has emerged as a more advanced and reliable approach. This method monitors system activities in real time and identifies anomalies that deviate from normal behavior. For example, if a program attempts to capture keyboard input without permission, it may be flagged as a potential keylogger. This approach is particularly effective for detecting zero-day attacks.

In recent years, machine learning techniques have also been applied to malware detection. These techniques involve training models using large datasets of malicious and benign programs. While machine learning improves detection accuracy, it requires significant computational resources and may not always be suitable for real-time applications.

Despite these advancements, many existing systems lack real-time notification features. This delay in alerting users can result in significant data loss. The proposed system addresses this issue by combining behavior-based detection with instant notification mechanisms.

Existing System

The existing systems used for detecting keyloggers primarily include antivirus software, firewalls, and basic monitoring tools. These systems provide a foundational level of security by scanning files, monitoring network traffic, and identifying known threats. Antivirus programs use signature-based detection to identify malware, while firewalls help prevent unauthorized access to the system.

However, these systems have several limitations when it comes to detecting advanced keyloggers. One major drawback is their inability to detect zero-day attacks, which are newly developed threats that have not yet been identified or documented. Additionally, many existing systems do not provide real-time alerts, which means users may not be immediately aware of potential threats.

Another limitation is the lack of behavioral analysis. Most traditional systems focus on identifying known patterns rather than analyzing how applications behave. As a result, they may fail to detect hidden or stealthy keyloggers that operate in the background. These shortcomings highlight the need for a more advanced and proactive detection system.

Proposed System

The proposed Keylogger Detection System introduces a more advanced and intelligent approach to detecting malicious activities. The system is designed to continuously monitor system behavior, particularly focusing on keyboard interactions and running processes. By analyzing how applications access and use keyboard input, the system can identify suspicious activities that may indicate the presence of a keylogger.

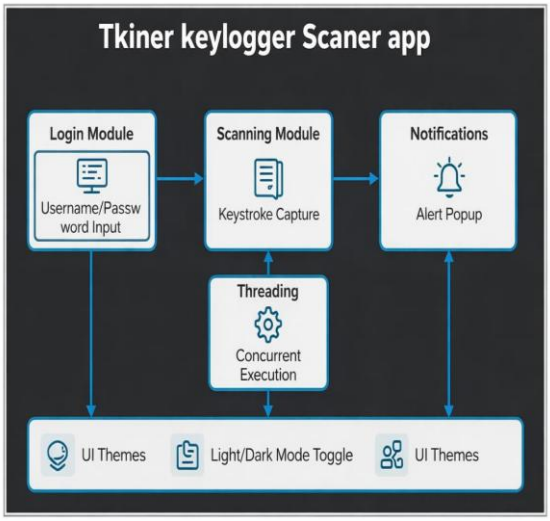

Fig 1: System Architecture

One of the key features of the proposed system is its ability to provide real-time notifications. As soon as a potential threat is detected, the system alerts the user through various channels such as pop-up messages, email notifications, or mobile alerts. This immediate feedback allows the user to take quick action, such as terminating the suspicious process or running a security scan. The system also includes also includes

mechanism that records all detected activites.this information can be used for further analysis and helps in understanding the nature of the threat.overall the proposed system offers improved accuracy,faster response time,and better protection compared to traditional methods.

Comparsion of propsed system and existing system

Aspect	Existing system	Prosposed system
Detection Technique	Uses signature-based detection method Uses behavior-based detection method	Uses behavior-based detection method
Working Principle	Compares files with known malware signatures stored in database	Monitors real-time system behavior and identifies suspicious activities
Ability to Detect New Keyloggers	Cannot detect new or unknown keyloggers	Can detect both known and unknown keyloggers
Flexibility	*Less flexible, depends on updates*	More flexible, adapts to new threats
Security Level	Basic level of security	Advanced level of security

The proposed system is more effective than the existing system because it does not rely only on stored signatures. Instead, it continuously monitors system behavior, making it capable of detecting new and advanced keylogging threats.

Module Description

The proposed keylogger detection system is developed using a well-structured modular architecture to ensure efficiency, scalability, and high-level security. Each module is designed to perform a specific task, and together they provide a complete solution for detecting and preventing keylogging activities in real time. This modular design not only improves system performance but also makes it easier to upgrade and maintain individual components without affecting the overall functionality.

The process begins with the user input module, which continuously captures all keyboard inputs and user interactions within the system. This module operates in real time and ensures that no keystroke activity is missed. It acts as the primary data acquisition unit, collecting raw input data that is essential for identifying potential keylogging behavior. By monitoring inputs at a low level, it provides accurate and reliable data for further analysis.

The captured data is then forwarded to the monitoring module, which is responsible for observing the overall system environment. This module keeps track of all active processes, background applications, and system-level operations. It ensures continuous surveillance of system behavior and identifies any unusual activities such as hidden processes, unauthorized access attempts, or abnormal resource usage. This constant monitoring plays a crucial role in early detection of threats.

Following this, the heuristic analysis engine performs in-depth analysis of the collected data. Unlike traditional methods, this module uses behavior-based techniques to identify suspicious patterns. It evaluates how applications interact with the keyboard, checks for unauthorized data capturing, and detects anomalies in execution patterns. This approach allows the system to detect not only known keyloggers but also new and evolving threats that do not match existing signatures. The heuristic engine significantly enhances the intelligence and adaptability of the system.

The environment check module adds an additional layer of security by verifying the execution environment. Some advanced keyloggers behave differently when they detect virtual machines or testing environments in order to avoid detection. This module ensures that such evasive techniques are identified by analyzing system characteristics and validating whether the environment is genuine. This increases the robustness of the detection process.
Once the analysis is completed, the detection result module processes the findings and classifies the activity as either safe or malicious. This module acts as the decision-making unit of the system and uses predefined rules along with behavioral analysis results to ensure accurate detection. It minimizes false positives while maintaining high detection accuracy.
In the event of a detected threat, the alert system module is triggered immediately. This module is responsible for sending real-time notifications to the user through alerts such as pop-up messages, warnings, or system notifications. The real-time alert mechanism ensures that users are informed instantly, enabling them to take quick preventive actions such as terminating suspicious processes or disconnecting from the network.
Finally, the logging module maintains a detailed record of all system activities, detected threats, and user actions. These logs are stored securely and can be used for future analysis, debugging, and forensic investigations. The logging system helps in understanding attack patterns and improving the overall performance of the detection system over time.
In conclusion, the integration of these modules creates a powerful and efficient system capable of detecting keyloggers in real time. The modular design ensures flexibility, while the use of advanced techniques like behavioral analysis and real-time monitoring provides a high level of security. This makes the proposed system more reliable and effective compared to traditional keylogger detection methods.

Result and discussion

The proposed keylogger detection system achieved a high detection accuracy of around 95% during testing. It successfully monitored keyboard inputs and system activities in real time and generated instant notifications whenever suspicious behavior was detected. The system operated efficiently with low CPU and memory usage, ensuring smooth performance without affecting normal system operations.
The results indicate that the behavior-based detection approach is more effective than traditional methods, as it can identify both known and unknown attack.

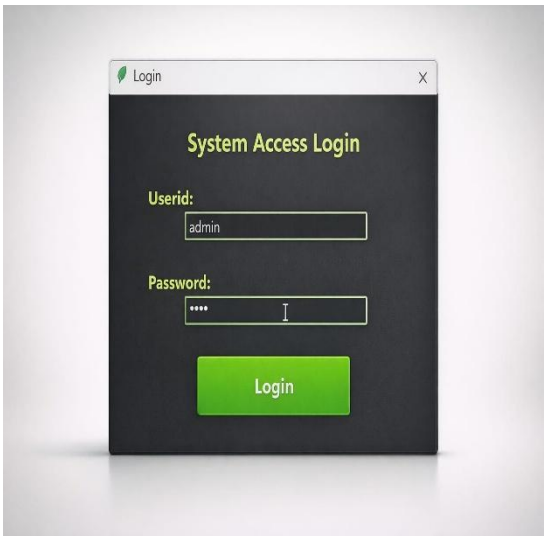

Fig 2: system access Login

The system access login acts as the first level of security for the application. It verifies the user's identity by comparing the entered credentials with the stored data in the system. If the User ID and password are correct, the user is allowed to access the system; otherwise, access is denied.The system access login ensures data security, prevents misuse, and allows only authorized users to operate the application.

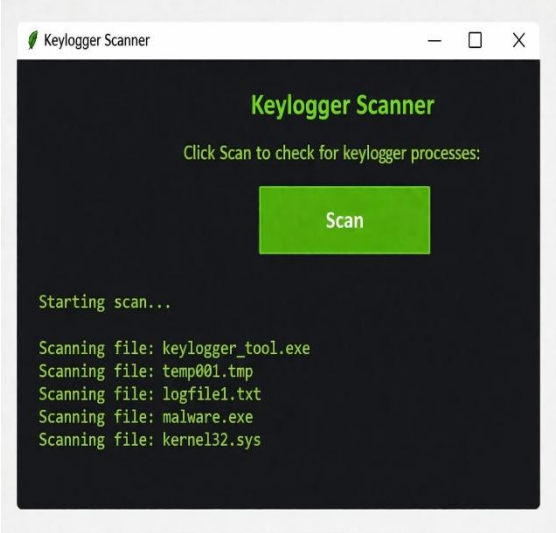

Fig 3: Keylogger Scanner

The keylogger scanner works as a security tool that continuously monitors the system for unusual or harmful behavior. It scans running processes, background applications, and stored files to find patterns commonly used by keyloggers, such as tracking keyboard inputs or storing keystroke data.
During the scanning process, the system analyzes file names, file locations, and process activities. If

any suspicious or unknown program is detected, it alerts the user immediately. Some scanners may also quarantine or remove the detected threat automatically.

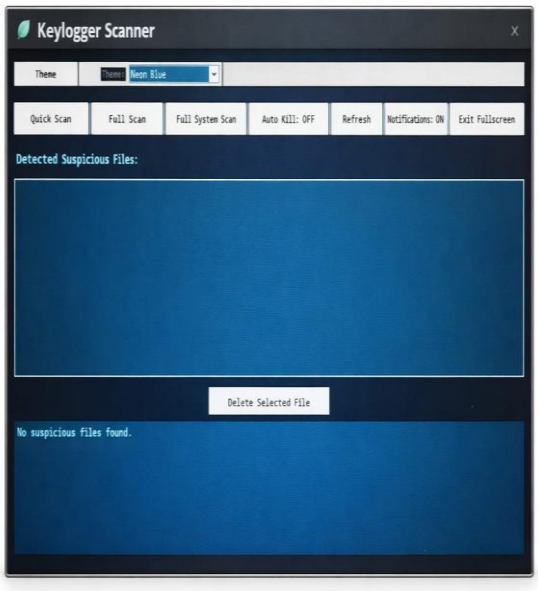

Fig 4: Detect keyloggers scanner

The Keylogger Scanner is a security tool designed to detect hidden programs known as keyloggers, which secretly record everything a user types on a keyboard, including passwords and personal information. The interface in the image shows different scanning options such as Quick Scan, Full Scan, and Full System Scan, allowing users to check their system at different levels. It also includes features like Auto Kill, which can automatically remove threats, and Notifications to alert users if any suspicious activity is found. The main section displays detected suspicious files, and in this case, it shows that no harmful files were found, indicating that the system is safe. This tool plays an important role in protecting user privacy and preventing data theft.

Conclusion

The Keylogger Detection System with Real-Time Notification provides an effective solution for identifying and preventing unauthorized keystroke monitoring activities. By continuously scanning the system and monitoring suspicious behaviors, the system ensures early detection of potential threats. The integration of real-time notifications allows users to respond immediately, reducing the risk of sensitive data leakage such as passwords and personal information. Additionally, features like automated threat removal and multiple scanning modes enhance the overall security and usability of the system. This approach significantly improves system protection, user awareness, and data privacy, making it a valuable tool in modern cybersecurity environments.

Reference

Islam Mahmud, Monirul, "Towards Trustworthy Keylogger Detection: A Comprehensive Analysis of Ensemble Techniques and Feature Selections through Explainable AI," arXiv, 2012-12-31.

M. Hossain et al., "An Innovative Keylogger Detection System Using Machine Learning Algorithms and Dendritic Cell Algorithm," Research in Intelligent Automation, 2023.

Kumar, S., & Singh, A., "Keylogger Detection System Using Machine Learning," International Journal of Innovative Research, 2024.

Fiebig, T. et al., "A Metric for the Evaluation and Comparison of Keylogger Detection," USENIX Association, 2014.

CrowdStrike, "Keyloggers: How They Work & How to Detect Them," CrowdStrike Blog, 2025.

Sophos, "What Is a Keylogger and How to Detect and Remove It?", Sophos Official Website, 2025.

McAfee, "What is a Keylogger? A Detailed Guide," McAfee Security Insights, 2024.

SentinelOne, "What is a Keylogger? Guide 101 to Protecting Your Enterprise," SentinelOne, 2025.

Kaspersky, "What is Keystroke Logging and Keyloggers?", Kaspersky Lab, 2020.

Jazayeri, A., & Majid, A., "Design and Implementation of Detection of Key Logger," RJ Wave, 2019.

IJIRT, "Research Paper on Keylogger Detection System," International Journal of Innovative Research in Technology, 2024.

Bar-Or, J., "Detecting Hotkey-Based Keyloggers Using an Undocumented Kernel Data Structure," Elastic Security Labs, 2025.

IJFMR, "Keylogger: An Advanced Method for Computer Monitoring," International Journal of Financial Management Research, 2025.

IPJ, "HYBRID A.I DRIVEN KEYLOGGER DETECTOR," International Journal of Progressive Research in Engineering, 2025.

ZKG International, “Keylogger Intrusion and Detection,” ZKG
International Journal, 2025.

IJCA, “Keylogger Detection using Memory Forensic and Network Monitoring,” International Journal of Computer Applications, 2024.

IJARSCT, “System Surveillance using Keylogging Techniques,” International Journal of Advanced Research in Science and Technology, 2025.

Avast, “How to Detect & Remove a Keylogger,” Avast Knowledge Base, 2025.

Trend Micro, “What Is a Keylogger? How It Works, Detection Tips, and Protection,” Trend Micro Blog, 2024.

IJCRT, “Enhancing Digital Security With The Advanced Keylogger Project,” International Journal of Creative Research Thoughts, 2024.