IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 6, Issue 1, March 2026

Impact Factor: 8.2

Advanced Keylogger Detection and Defence System: Behavioral Spyware Analysis Using Machine Learning

Rahul Lilhare[1], Jyotirmay Karemore[2], Saurabh Udapure[3]

Assistant Professor, MCA, KDK College of Engineering, Nagpur, India[1]

PG Scholar, MCA, KDK College of Engineering, Nagpur, India[2,3]

rahul.lilhare@kdkce.edu.in, jyotirmayakaremore.mca24f@kdkce.edu.in,
udapureskishorrao.mca24f@kdkce.edu.in

Abstract: *The rapid evolution of malware, particularly stealthy keyloggers, poses a significant threat to user privacy and data security in personal and enterprise environments. Traditional antivirus solutions rely heavily on signature-based detection, which often fails against custom-made "Zero-Day" spyware that lacks a known digital fingerprint. This paper presents the design and implementation of an Advanced Keylogger Detection and Defence System developed as a hybrid local application. The proposed system integrates kernel-level metric extraction, a Hybrid Logic detection engine, and the Isolation Forest Machine Learning algorithm to identify malicious behavior patterns. Uniquely, the system employs a dual-interface architecture: a native CustomTkinter desktop controller for real-time threat management and a rich HTML/CSS dashboard for detailed behavioral analytics. The application enables users to monitor CPU and network anomalies, receive immediate visual alerts, and terminate threats via a "Kill Switch" interface without relying on external cloud analysis. Experimental evaluation demonstrates high accuracy in detecting high-resource surveillance scripts while maintaining low system overhead.*

Keywords*:* Keylogger Detection, Behavioral Analysis, Isolation Forest, Machine Learning, Anomaly Detection, Cybersecurity, Real-time Monitoring, Python

DOI: 10.48175/IJARSCT-31410