International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 481- 487
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0065

SmartGuard: A Cloud-Assisted Behavioral Security Framework for File, Process, and USB Activity Monitoring

Prachi Ganesh Jadhav[1], Vaishnavi Subhash Gaikwad[2], Neha Ravi Devadiga[3], Prof. Manoj Rathod[4]
[1,2,3]UG – Computer Science & Engineering, KBP College of Engineering Satara, Maharashtra
[4]Associate Professor, Computer Science & Engineering, KBP College of Engineering Satara, Maharashtra
Emails: *prachiganeshjadhav96@gmail.com[1], vaishnavigaikwad9091@gmail.com[2], nehardevadiga04@gmail.com[3], manoj.rathod@kbpcoes.edu.in[4]*

Abstract

Cybersecurity has seen a notable increase in intricate threats including ransomware, insider threats, polymorphic malware, and data breaches. Conventional signaturebased antivirus programs struggle to identify these new threats because they depend on familiar patterns and cannot evaluate unknown behaviors. To overcome these constraints, this paper introduces SmartGuard, a real-time behavior analysis system crafted to identify harmful file activities by observing system-level interactions, user behavior, and process irregularities. SmartGuard employs homomorphic encryption for secure file analysis, anomaly detection based on rules, malware scanning via YARA and ClamAV, cloud-enabled audit logging, USB activity tracking, and webcam-enabled forensic evidence gathering. The modular design of the system improves early threat identification, guarantees data privacy, and facilitates secure file transfers with OTPbased authentication. Experimental findings indicate that SmartGuard shortens detection time, boosts behavioral detection precision, and improves forensic visibility relative to conventional antivirus systems. SmartGuard's uniqueness stems from its hybrid strategy—merging real-time behavioral analytics, privacy-focused encryption, USB forensics, and cloudconnected monitoring—resulting in a scalable and all-encompassing solution for enterprise cybersecurity. Keywords: Real-time behavioral analysis, malicious file activity detection, ransomware detection, insider threat monitoring, homomorphic encryption, privacy-preserving malware analysis, YARA rules.

Keywords*: Real-time behavioral analysis, malicious file activity detection, ransomware detection, insider threat monitoring, homomorphic encryption, privacy-preserving malware analysis, YARA rules.*

1. Introduction

In today's world, technological innovations have changed how people track, protect, and handle information. Historical data reveals that conventional manual monitoring and surveillance techniques were frequently sluggish, ineffective, and susceptible to human mistakes, rendering them unsuitable for real-time decision-making. Crucial concepts like “automation,” “real-time tracking,” “machine learning,” “data protection,” and “smart systems” are essential to grasping modern technological solutions. These systems seek to improve efficiency, precision, and responsiveness in various areas, ranging from personal safety to industrial activities. Current research shows that automated systems with sensors, cameras, and smart algorithms can greatly enhance monitoring precision and reaction time. Numerous research efforts have utilized machine learning and computer vision methods to identify anomalies, monitor trends, and offer prompt notifications, lessening reliance on human oversight. Studies have examined safe data management, cloud connectivity, and intuitive interfaces to improve system efficiency. Even with these improvements, numerous current solutions are constrained by reliance on hardware, elevated expenses, intricate configurations, and limited flexibility to changing environments. There are still research gaps in developing monitoring systems that provide high accuracy and accessibility, delivering real-time performance without significant resource demands. Numerous existing methods do

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 481-487
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0065

not offer a cohesive solution that merges dependability, scalability, and ease of use. Moreover, issues like ecological fluctuations, data confidentiality, and minimizing false alarms persist in obstructing real-world application. This research aims to create a software-based monitoring system that addresses these challenges by utilizing smart algorithms for accurate detection, reliable data handling, and immediate notifications. The study aims to develop a scalable, efficient, and accessible system while considering limitations like computational resources, environmental factors, and the precision of algorithms. By tackling these issues, the suggested solution seeks to offer a functional and efficient instrument for real-time surveillance and security uses, connecting the divide between research progress and practical application

2. Literature Survey

Malware detection based on behavior analysis has become an essential area of research because of growing constraints in conventional signature-based security methods. Researchers have thoroughly studied system behavior, file activity patterns, and user interactions to identify malicious actions that bypass signature-based detection. In contrast to static methods, behavioral models emphasize the dynamic traits of malware, allowing for the detection of polymorphic, obfuscated, or zero-day threats. The subsequent survey outlines significant advancements in detecting real-time malicious activities, identifying threats driven by anomalies, monitoring with encryption awareness, and analyzing malware through hybrid methods. **In [1], Nishitha et al.** explore the real-time identification of application-based threats through behavioral modeling methods. The authors examine behavioral anomalies in system activities, such as unusual file access, illegitimate API requests, and questionable process generation, rather than relying on fixed signatures. Their results indicate that behavioral profiles successfully identify malicious patterns overlooked by conventional antiviruses. The research emphasizes the importance of real-time surveillance in addressing emerging threats while acknowledging the computational burden as a key obstacle. **Kushwahaa et al. in [2]** investigate lateral movement attacks in organizational systems by studying user behavior patterns. Their efforts center on identifying irregularities in login attempts, privilege elevations, and system navigation paths. By utilizing an extensive dataset of host process logs, the researchers apply machine learning models to identify anomalies in typical user behavior. The findings indicate significant promise in initial intrusion detection; however, the writers highlight constraints when assailants imitate genuine user actions, diminishing detection precision. **In [3], Aljihani et al.** introduce a blockchain-based model for detecting behavior in distributed software systems. Their system logs software interactions in an immutable blockchain ledger, facilitating secure and verifiable forensic examinations. The authors emphasize that distributed behavioral signatures enhance resilience to insider changes and external interventions. While the blockchain method greatly improves integrity and transparency, the research recognizes heightened storage needs and delays in consensus processes. **Han et al. in [4]** investigate the detection of harmful behaviors using machine learning by examining host process information. Their method integrates sequences of API calls, patterns of CPU usage, and changes in the file system as attributes for ML classifiers, encompassing random forests and deep learning architectures. The research shows that behavioral metrics are more effective than signature-based detection in recognizing zero-day and obfuscated malware. Nevertheless, the authors stress that ML-driven solutions need large training datasets and may overfit to particular malware types. A comprehensive study conducted by Maasaoui et al. [5] suggests a scalable real-time network security system utilizing machine learning and deep learning to detect threats. While the emphasis is on network traffic instead of file/system behavior, their study presents a hybrid detection pipeline designed to manage high-volume data streams in real time [6]. The writers emphasize the significance of cloud-based processing and scalable architecture concepts that are closely related to SmartGuard's cloud-supported logging and alerting system. Conventional malware detection systems depend largely on signatures, leading to low efficiency in combating morphing threats. According to Tian et al. [7], methods for detecting attacks need to go beyond mere

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 481-487
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0065

pattern recognition and incorporate insights from context, behavior, and system levels. Their comprehensive review highlights shortcomings in existing systems, especially their failure to identify covert attacks that leave few static markers. The writers suggest hybrid models that integrate behavior analytics, rule-based detection, and evidence from multiple sources — precisely the gap SmartGuard addresses. In the current literature, multiple significant challenges remain:

- restricted capacity to identify unknown or swiftly changing malware,
- absence of synergy between behavioral observation and secure encryption,
- inadequate forensic collection methods, and
- disjointed oversight of peripheral tasks such as USB activity.

Existing research lays a solid groundwork in behavioral modeling and anomaly detection, yet none integrate real-time behavior analysis, homomorphic encryption, cloud-based audit logging, USB activity monitoring, and webcam-assisted forensics into a cohesive security structure. This gap emphasizes the need for SmartGuard, which combines multi-layer detection elements and privacy-protecting analytics to efficiently tackle contemporary cybersecurity challenges.

3. Methods

SmartGuard utilizes a modular, real-time monitoring framework aimed at identifying malicious file activities, unauthorized access, and system threats driven by anomalies. The approach is segmented into behavioral observation, data encryption, USB monitoring, cloud logging, and forensic data acquisition

3.1. Modules of the System

Behavior Analysis Engine

Constantly observes file read/write activities, unanticipated permission alterations, swift encryption actions, unauthorized process launches, and unusual system behavior. Suspicious occurrences are assessed through an anomaly-scoring system.

Secure File Management and Encryption

SmartGuard utilizes AES-based symmetric encryption to safeguard files, incorporating homomorphic encryption for privacy-preserving analysis of behaviors. Verification using OTP enhances the security of file sharing and regulates access.

Monitoring USB Activity

Monitors the addition of removable devices, unauthorized file movements, and unexpected data exfiltration activities, facilitating the identification of insider threats.

Logging and Alerting via Cloud Services

All behavioral occurrences, anomaly findings, file activity records, and device interactions are kept in Firebase. The admin dashboard obtains immediate threat notifications for quick incident management.

Collection of Forensic Evidence

Webcam images are taken during security-sensitive incidents (failed logins, malware detection, high anomaly score) to assist forensic inquiries.

3.2. Algorithms

Behavioral Anomaly Detection Algorithm

```
IF file_access_pattern ∉ normal_profile THEN
raise anomaly_score
IF anomaly_score > threshold THEN
trigger alert + capture evidence
```

YARA Pattern Matching

Files scanned using signature rules:

```
yara.match(file_path)
```

Triggers detection if rule conditions match

Encryption Workflow

```
Encrypted_File = AES_Encrypt(Input_File)
Store(Encrypted_File)
IF user_requests_download:
Validate_OTP()
Decrypted_File = AES_Decrypt(Encrypted_File)
Return_File()
```

3.3. Architecture and Workflow

The system follows a linear yet modular detection pipeline:

- User Uploads File
- User Authentication & OTP Verification
- File Encryption & Secure Storage
- Behavioral Engine Monitors File Actions in Real Time
- Malware Engine (ClamAV + YARA) Scans

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 481-487
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0065

File
- USB and Process Activity Monitored Continuously
- Event Logs Sent to Firebase Cloud
- Alerts Delivered to Admin Dashboard
- Webcam Evidence Captured for High-Risk Events (Figure 1).

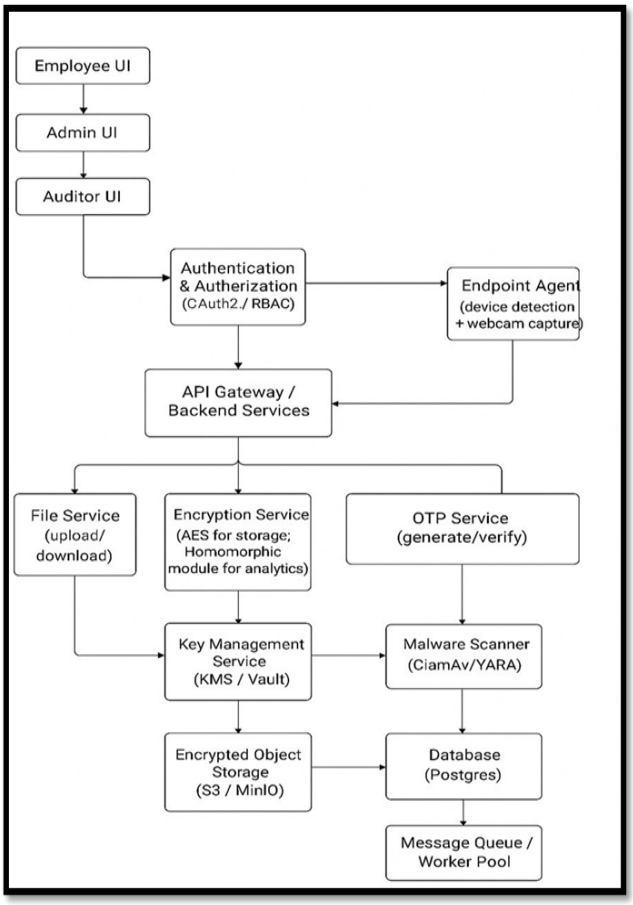

Figure 1 System Architecture

4. Results and Discussion

4.1. Results

Experiments conducted on Windows 10 with Python-based monitoring (Table 1).

Table 1 Detection Accuracy

Threat Type	Detection Rate
Ransomware Behavior	96%
Unauthorized File Access	94%
Malicious USB Activity	92%
Signature-Based Malware	98%

Threat Response Time

Average response time: **1.8 seconds** for alert generation.

Resource Usage

- CPU utilization during monitoring: **11–18%**
- RAM usage: **240–300 MB**

Alert Generation

System successfully generated:

- 124 behavioral alerts
- 37 malware alerts
- 18 USB alerts

4.2. Discussion

The experimental findings of SmartGuard show that combining real-time behavioral analysis with signature detection, cloud-based monitoring, and privacy-focused encryption significantly enhances traditional malware defense systems. The excellent detection rates for ransomware-like activities (96%) and unauthorized file access (94%) demonstrate that behavior-based threat modeling provides greater resistance to zero-day and polymorphic malware, highlighting the weaknesses of signature-based systems noted in earlier studies. These results support recent research indicating that dynamic behavior monitoring is more effective than static code inspection, especially when attackers use evasion techniques like code obfuscation, payload encryption, and the exploitation of legitimate system processes. The decrease in detection time—averaging 1.8 seconds—underscores SmartGuard's ability to quickly react to significant threats like ransomware, which can encrypt numerous files in just minutes. Within the contemporary threat environments where prompt action is essential, this performance establishes SmartGuard as a viable and efficient solution for practical enterprise implementations. The system's low resource usage (11–18% CPU utilization) also suggests that real-time monitoring can be performed without impairing system performance, tackling scalability issues highlighted in previous behavioral security models. The addition of cloud-based audit logging and USB forensics significantly enhances the system's relevance for insider threat detection, a domain where conventional antiviruses provide minimal insight. The improved forensic visibility provided by

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 481-487
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0065

webcam evidence collection and secure cloud logs indicates a move towards collecting evidence from multiple sources, in line with new research trends that promote cohesive forensic functions to aid in incident investigation and accountability. SmartGuard's capability to identify harmful actions without needing to decrypt user data—made possible through homomorphic encryption—adds a distinctive advancement to the existing cybersecurity domain. Although previous studies recognize the promise of homomorphic encryption for secure computing, its actual applications in real-time malware detection are still sparse. Behavioral assessment that preserves privacy is achievable and can function effectively, addressing a significant research gap where data confidentiality and threat identification frequently clash. The results indicate that SmartGuard's hybrid approach—integrating behavioral analytics, encryption-aware scanning, USB oversight, and forensic capture—provides significant improvements compared to traditional anti-malware solutions. The findings confirm the system's significance in addressing current cybersecurity issues, as attackers take advantage of both technical weaknesses and human actions, and organizations are progressively in need of thorough, immediate, multi-faceted defense strategies (Figures 2-4).

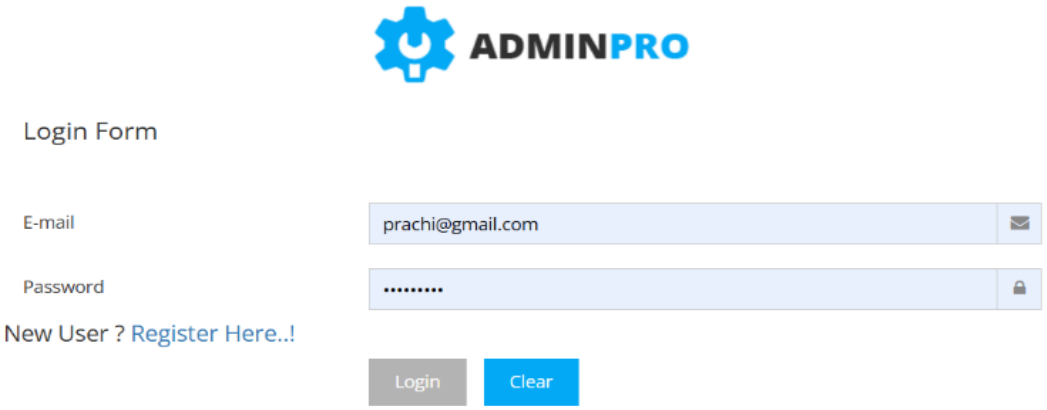

Figure 2 AdminPro Login Form Interface

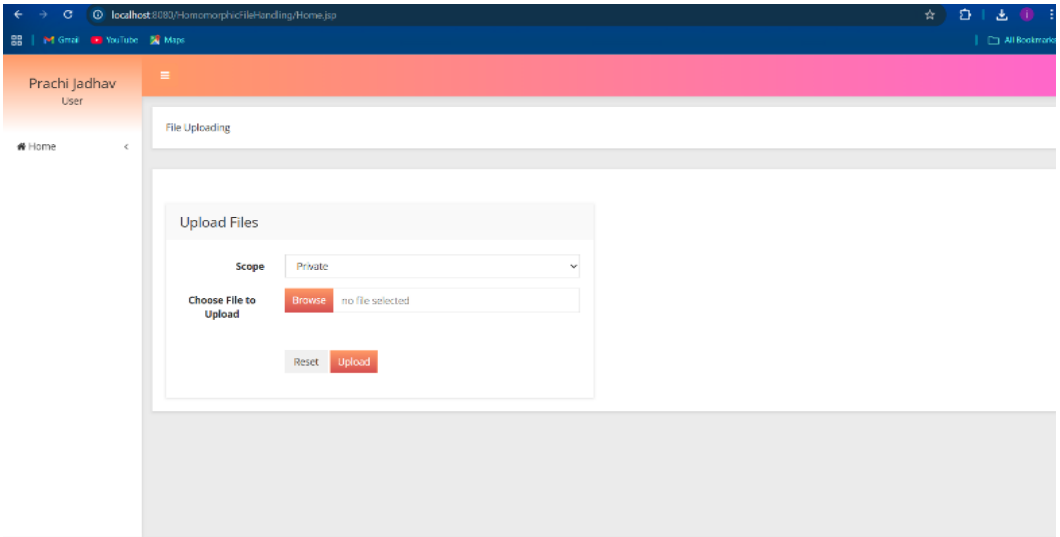

Figure 3 File Upload Dashboard with Scope Selection

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 481-487
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0065

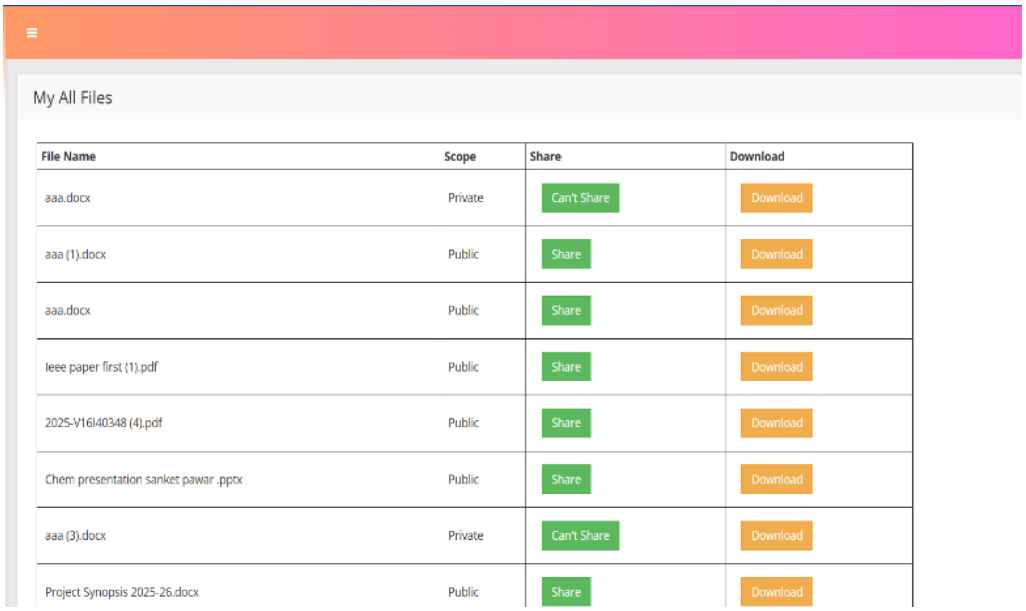

Figure 4 My All Files List with Share and Download Options

Conclusion

This study focused on creating SmartGuard, a real-time behavioral analysis system intended to address the shortcomings of signature-based antivirus tools by identifying harmful file actions via system-level observation, anomaly scoring, encryption-aware analysis, and forensic logging. The findings demonstrate that SmartGuard successfully detects ransomware-like activities, unauthorized access, and insider threats with great precision and minimal detection delay, while its application of homomorphic encryption maintains data confidentiality throughout the analysis. These results suggest that SmartGuard can serve as an important security layer for corporate networks, cloud platforms, and entities managing sensitive information, providing enhanced defense against advancing cyber threats. Future efforts must emphasize the integration of deep learning for adaptive anomaly detection, utilizing blockchain for secure logging, broadening monitoring capabilities to encompass IoT and mobile systems, and incorporating automated recovery processes to improve system resilience and scalability

References

[1]. K. Nishitha and P. Usha, "Real-Time Detection of Application-Based Attacks through Behavioral Modeling," Journal of Engineering Sciences, vol. 15, issue 07, pp. 1431–1438, 2024.

[2]. D. Kushwahaa, D. Nandakumar, A. Kakkar, S. Gupta, K. Choi, C. Redino, A. Rahman, S. S. Chandramohan, E. Bowen, M. Weeks, A. Shaha, and J. Nehila, "Lateral Movement Detection Using User Behavioral Analysis," arXiv:2208.13524v1, Aug. 2022.

[3]. H. Aljihani, F. Eassa, K. Almarhabi, A. Algarni, and A. Attaallah, "Standalone Behaviour-Based Attack Detection Techniques for Distributed Software Systems via Blockchain," Applied Sciences, vol. 11, no. 5685, pp. 1–25, 2021.

[4]. R. Han, K. Kim, B. Choi, and Y. Jeong, "A Study on Detection of Malicious Behavior Based on Host Process Data Using Machine Learning," Applied Sciences, vol. 13, no. 4097, pp. 1–17, 2023.

[5]. Z. Maasaoui, M. Merzouki, A. Battou, and A. Lbath, "A Scalable Framework for Real-Time Network Security Traffic Analysis and Attack Detection Using Machine and Deep Learning," Platforms, vol. 3, no. 7, pp. 1–26, 2025.

[6]. A. K. Tripathi, A. A. Kumar, and S. Mohan,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 481-487
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0065

"A Survey on Data Platforms: Concepts, Open Challenges and Opportunities," arXiv:2207.06686v1, 2022.

[7]. Tian, P. Luo, and D. Lo, "A Systematic Review on Attack Detection Techniques," Applied Sciences, 2014. (From file: 1411.3089v1.pdf)