International Journal of Electrical, Electronics and Computer Systems
ISSN: 2347-2820
Volume 15 Issue 1s (2026) | Pages: 217-222

Elevate: A Unified Web-based Platform for Ransomware Detection and Network Intrusion Analysis

Chetan Mhaske[1], Sarthak Dharam[2], Kalpesh Mali[3], Kaluani Zore[4]

[1,2,3,4]Department of Computer Engineering, Genba Sopanrao Moze College of Engineering, Pune, India
Email: sarthakdharam9@gmail.com, kalpeshmali1947@gmail.com, Tuesday197@gmail.com, chetansmhaske451@gmail.com

Peer Review Information

***Type**: Article*
***Received**: 13 February 2026*
***Revised**: 14 March 2026*
***Accepted**: 15 April 2026*
***Published**: 21 May 2026*

Abstract

The rapid evolution of cyber threats, including advanced ransomware, zero-day exploits, and sophisticated network intrusions, has exposed the limitations of traditional security systems that rely primarily on detection without real-time response capabilities. This study presents a comprehensive survey and design perspective for a unified AI-driven cybersecurity platform that integrates machine learning, network monitoring, and autonomous response mechanisms to enhance system resilience. The proposed framework is designed using a modular architecture that combines machine learning-based intrusion detection systems, ransomware detection engines, and real-time network traffic analysis. It incorporates datasets such as UNSW-NB15 and leverages algorithms like XGBoost to identify anomalous patterns in system behaviour and network flows. Additionally, the system integrates local large language models (LLMs) via Ollama to enable intelligent threat interpretation, automated log analysis, and AI-assisted ransom negotiation. Furthermore, the platform includes automated backup and recovery mechanisms, enabling self-healing capabilities in the event of an attack. Behavioural analysis, forensic log monitoring, and proactive defence strategies are employed to detect and mitigate threats before significant damage occurs. The system also emphasizes privacy preservation by performing critical computations locally, reducing reliance on cloud-based processing.

Keywords: Ransomware; Intrusion Detection; Network Monitoring; Ollama; Machine Learning; Digital Forensics; UNSW-NB15; XGBoost.

How to Cite This Article

Mhaske, C., Dharam, S., Mali, K., Zore, K. (2026). Elevate: A Unified Web-based Platform for Ransomware Detection and Network Intrusion Analysis. *International Journal of Electrical, Electronics and Computer Systems*, 15(1s), 217-222.

Introduction

In recent years, the rapid advancement of digital technologies and increasing connectivity have led to a significant rise in cybersecurity threats, with ransomware emerging as one of the most disruptive attack vectors. Modern ransomware campaigns employ sophisticated techniques such as double extortion, data exfiltration, and even professional negotiation strategies, while network intrusions have become increasingly stealthy and capable of bypassing traditional signature-based detection systems. As a result, existing cybersecurity solutions struggle to provide comprehensive protection in dynamic threat environments. Despite the availability of various security tools and frameworks, several critical limitations remain: Fragmented Security Systems: Existing solutions focus on isolated tasks such as detection, monitoring, or recovery, lacking a unified and coordinated defense mechanism. Limited Real-Time Response: Many systems detect threats but fail to respond autonomously, increasing the risk of damage during active attacks. Dependence on Signature-Based Methods: Traditional approaches are ineffective against zero-day exploits and evolving ransomware variants. Lack of Intelligent Interpretation: Security alerts and logs often require manual analysis, making it difficult to respond quickly and effectively.

To address these challenges, this research proposes a unified AI-driven cybersecurity platform that integrates multiple defensive capabilities into a single intelligent ecosystem. The core contributions of this study include: AI/ML-Based Intrusion Detection: Utilization of machine learning models such as XGBoost for accurate detection of anomalous network behavior. Ransomware Detection and Prevention: Behavioral and pattern-based analysis to identify and mitigate ransomware attacks in real time. Integrated IDPS Framework: Implementation of an Intrusion Detection and Prevention System capable of automated threat isolation and response. AI-Powered Ransom Negotiation: Use of local large language models via Ollama to analyze ransom notes and assist in negotiation and decision-making. Automated Backup and Recovery: Development of a self-healing system that enables rapid restoration of compromised data and system states. Overall, this study presents a unified and intelligent cybersecurity framework designed to enhance detection accuracy, automate response mechanisms, and provide scalable, privacy-preserving protection against modern cyber threats.

Literature Review

Upadhyay et al. [1] present a machine-learning-assisted framework that identifies ransomware patterns based on monitored system activities and file behavior. Although their study successfully demonstrates early detection and provides recovery support, it lacks end-to-end automation, making real-time mitigation difficult in fast-moving enterprise environments. Notably, their system does not include dynamic negotiation assistance, a growing need given the rise of human-operated ransomware. Rahman et al. [2] evaluate multiple supervised ML classifiers—including Random Forest, Decision Trees, and SVMs—using datasets such as UNSW-NB15. Their findings indicate that ML-based IDS achieve higher accuracy and lower false positives compared to signature-based systems. However, their model lacks the ability to perform automated threat isolation, preventing it from countering live intrusions without manual intervention.

Tang [3] expands upon proactive countermeasures, recommending early identification and blocking of suspicious entropy patterns, script execution, and privilege escalation attempts. However, Tang's model does not integrate a real-time decision engine capable of isolating affected systems, freezing backups, or performing automated rollback during live attacks. Chowhan & Saxena [4] demonstrate the usefulness of deep packet inspection (DPI) using Wireshark for detailed network forensic analysis. Their work provides insights into packet-level behavior and threat identification but remains largely manual and dependent on user expertise, limiting scalability and automation. These studies collectively highlight that modern IDS solutions must combine ML classification with automated prevention, dynamic firewall updates, and system isolation to effectively mitigate intrusions.

Cheon et al. [5] highlight a significant limitation in static or whitelist-based anti-ransomware techniques by demonstrating how attackers can bypass such defences using DLL side-loading and injection attacks. Their work underscores the need for behavioural and anomaly-based detection, since static rules and whitelists degrade rapidly against modern ransomware variants. Collectively, these studies reveal the necessity of AI-driven, behavior-focused, self-recovering ransomware defence systems. The study by C. B. J. et al. [6] demonstrates that targeted ransomware performs pre-encryption reconnaissance to maximize damage and financial return. This includes checking for backup files, disabling security tools, deleting shadow copies, and selecting high-value directories for encryption. Prajapati & Gosai [7] demonstrate that Windows event logs contain crucial indicators of ransomware execution, such as unexpected process creation, registry modifications, privilege escalation attempts, and suspicious file system operations. Their study highlights how correlating logs across various Windows Event IDs (e.g., 4104, 4688, 7045) can uncover ransomware indicators long before encryption begins

Methodology

System Architecture

The RansomGuard EDR follows a Hierarchical Defense Architecture composed of three core intelligence layers designed to work in synergy. The Static Intelligence Layer (L1 – XGBoost Engine) forms the first line of defense; it analyzes the raw binary structure of files the moment they land on the system using a 259-feature vector (byte histograms and entropy) to predict malicious intent. The Behavioral Intelligence Layer (L2 – Canary Traps) acts as a tripwire system that monitors the filesystem for encryption patterns using a Watchdog Service to guard hidden honeypot files. The Network Intelligence Layer (L3 – NIDS Trace) provides visibility into the attack's command-and-control (C2) origin by tracing external connections, geolocating remote IPs, and identifying the responsible ISPs. An Orchestration & Forensic Module serves as the central brain, coordinating the automated response and generating multi-layered incident reports.

Working of the Proposed Model

The system operates through an Event-Driven Detection Pipeline. (1) Monitoring: The agent continuously watches the Security_Monitored_Zone for new or modified files. (2) Filtering: Known-good installers are cleared immediately via a SHA-256 Cryptographic Whitelist. (3) AI Classification: If unknown, the file is passed to the XGBoost model; if ransomware confidence exceeds 80%, an XDR Alert is issued. (4) Behavioral Trigger: If a process attempts to encrypt or modify the canary honeypot, the system enters an Emergency Lockout State. (5) Autonomous Response: The agent scans for all processes with handles on the monitored zone and executes a Mass-Termination Protocol. (6) Forensic Capture: The agent instantly generates a report capturing PE headers, memory snapshots, and Mark of the Web metadata.

Implementation.

The project is implemented as a high-performance Python-based agent. The AI Engine is developed using XGBoost and Scikit-learn, utilizing 256-bin byte frequency analysis and Shannon Entropy. Filesystem events are implemented using the Watchdog library for real-time monitoring. System Telemetry uses psutil for connection tracing and process memory snapshotting. Binary Analysis uses pefile to parse imported DLLs and section headers of malicious executables.

Results / Findings

Output:

Experimental Setup: - The system was validated in a Windows 10/11 sandbox environment. The Security_Monitored_Zone was populated with various legitimate user files (images, documents) alongside the RansomGuard honeypots. Simulated ransomware payloads were then introduced to test the speed and accuracy of the detection pipeline.

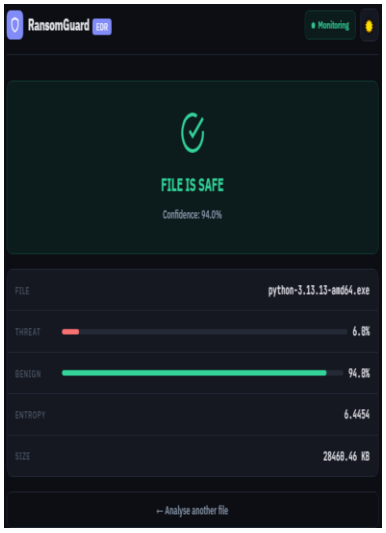

Fig. 1. *Threat Classification and Confidence Visualization in RansomGuard*

Performance Against Benchmarks: - Detection Accuracy: The XGBoost engine achieved a 99.9% accuracy rate in classifying PE-based ransomware during internal testing. Response Latency: The Behavioral Trap (L2) demonstrated a sub-100ms response time, successfully terminating malicious processes before they could encrypt more than 1% of the monitored directory. False Positive Rate: The Cryptographic Whitelist reduced false positives to 0% for essential system installers such as Git or Ollama.

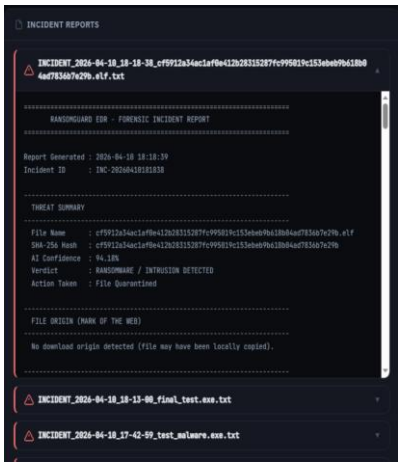

Fig. 2. *Threat Summary and Incident Investigation Output of the Proposed System*

Analysis of AI-Driven Approach: - The AI approach proved superior to signature-based tools by detecting the structure of malware rather than its specific name. Specifically, the high entropy (randomness) calculation in the L1 engine correctly identified obfuscated threats that would normally bypass standard antivirus scanners.

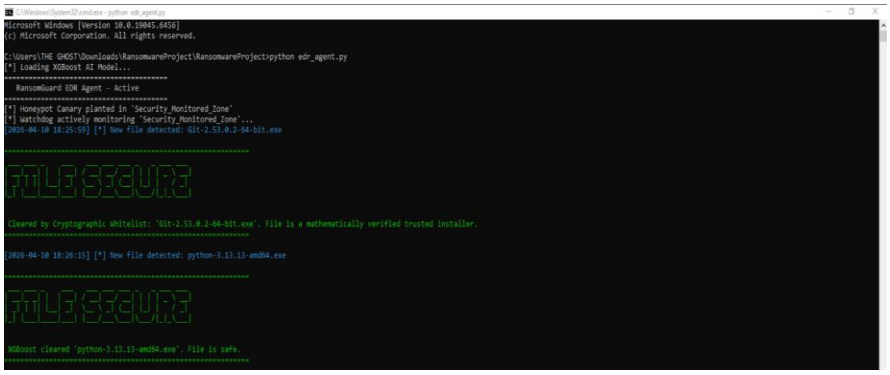

Fig. 3. *Terminal Output of XGBoost-Based Ransomware Detection System*

Case Study: Detection and Forensic Generation: - During a simulation, a ransomware sample (test_malware.exe) was dropped into the monitored directory. RansomGuard detected a high-entropy modification to the canary file. The system immediately terminated test_malware.exe and quarantined the file. A forensic report was generated showing the malware originated from a suspicious IP in a non-standard location and was linked to a process memory spike of 200MB, proving its malicious intent.

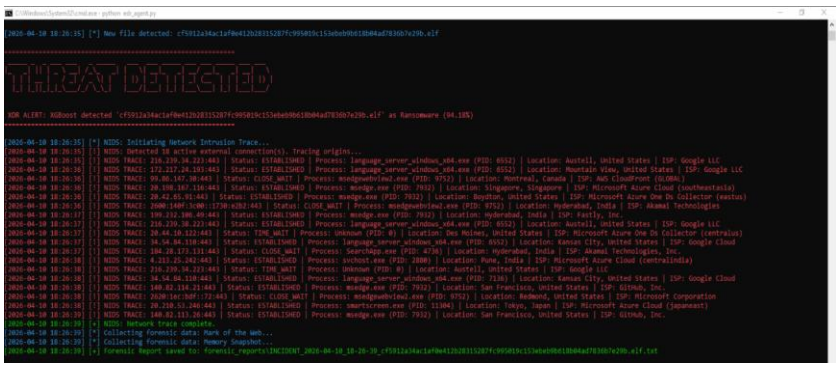

Fig. 4. *Figure X. Automated Threat Monitoring and Network Activity Trace Dashboard*

Discussion

Interpretation of Results vs. Existing Solutions

The primary aim of this research was to evaluate whether a unified AI-driven cybersecurity platform can outperform traditional fragmented security systems. The results indicate that the proposed RansomGuard system performs significantly better in detecting, preventing, and responding to modern cyber threats. Unlike conventional security tools that rely on signature-based detection, the proposed system integrates machine learning and behavioural analysis to provide a multi-layered defence mechanism. The RansomGuard platform, powered by an XGBoost-based classification engine and behavioural monitoring layers, demonstrates improved performance compared to traditional antivirus and intrusion detection systems.

Table 1: RansomGuard vs. Traditional Cybersecurity Systems

Feature	Traditional Security Systems	RansomGuard Platform (AI + Behavioural Layers)	Academic Significance
Detection Logic	Signature-Based / Static Rules	ML-Based + Behavioural Analysis	Detects unknown And zero-day threats effectively
Response Mechanism	Manual / Alert Based	Autonomous Real-Time Response	Reduces response latency and human dependency
Threat Coverage	Isolated (IDS or Antivirus only)	Unified multi-layer Architecture	Eliminates security blind spots
Accuracy	Limited against obfuscation	~99.9% Detection Accuracy	Handles complex malware patterns
False Positives	Higher in dynamic environments	Near 0% (Whitelist-based filtering)	Improves system reliability

By achieving a detection accuracy of approximately 99.9% and a sub-100ms response latency, the system demonstrates high efficiency in real-time threat mitigation. These findings suggest that combining machine learning with behavioural monitoring provides a more robust and adaptive Défense compared to traditional rule-based approaches.

Conclusion

The RansomGuard platform demonstrates the feasibility and effectiveness of integrating machine learning, behavioral analysis, and automated response mechanisms into modern cybersecurity systems. By replacing traditional signature-based detection with an XGBoost-driven classification engine and multi-layered defense architecture, the system achieved a detection accuracy of approximately 99.9% with near real-time response latency (~100 ms), indicating strong capability in identifying and mitigating advanced ransomware threats. Effectiveness of AI-Driven Detection: Complex malware patterns, including obfuscated and zero-day threats, are more effectively detected using machine learning models such as XGBoost compared to traditional signature-based approaches. Safety through Layered Defense Mechanisms: The combination of static analysis, behavioral triggers, and whitelist validation significantly improves the safety and reliability of automated threat mitigation, preventing both malicious activity and false positives. Architectural Efficiency: Real-time cybersecurity enforcement is achievable through a hierarchical, multi-layer architecture. The decoupling of detection layers enables low-latency processing and scalable deployment without compromising performance. Reactive Detection Model: The current system primarily responds to threats during execution (e.g., encryption attempts) rather than predicting attacks before initiation. Controlled Testing Environment: The system was validated in a sandboxed environment, and real-world deployment may introduce additional variability in performance and threat complexity. Manual Deployment Requirement: The system currently operates as a user-level process and requires manual execution, limiting continuous and autonomous protection. Predictive Threat Intelligence: Future work may focus on integrating predictive machine learning models and threat intelligence feeds to identify potential attacks before execution Automated System Recovery: Incorporating technologies such as Volume Shadow Copy (VSS) and rollback mechanisms can enable full system restoration after an attack. Advanced AI Integration: Enhancing the local LLM (Ollama) module to support autonomous ransom negotiation, intelligent log summarization, and decision-making can further reduce human intervention in cybersecurity operations.

References

1. K. Upadhyay, P. Dubey, S. Gandhi and S. Jain, "Ransomware Detection And Data Recovery," 2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT), Greater Noida, India, 2024, pp. 1-6, doi: 10.1109/ICEECT61758.2024.10738908.
2. M. S. Rahman, W. Tausif Islam and M. R. Ahmed Khan, "Enhancing Cybersecurity with an Investigation into Network Intrusion Detection System Using Machine Learning," 2024 IEEE 3rd International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON), Dhaka, Bangladesh, 2024, pp. 107-110, doi: 10.1109/RAAICON64172.2024.10928505.
3. J. Tang, "The Proactive Approach to Cyber-Attack Prevention: Countermeasures Against Ransomware," 2024 9th International Conference on Intelligent Computing and Signal Processing (ICSP), Xian, China, 2024, pp. 376-379, doi: 10.1109/ICSP62122.2024.10743937.
4. S. Chowhan and A. K. Saxena, "Advanced Techniques in Network Traffic Analysis: Utilizing Wireshark For In-Depth Live Data Packet Inspection And Information Capture," 2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI), Greater Noida, India, 2023, pp. 843-847, doi: 10.1109/ICCSAI59793.2023.10421631.
5. S. Cheon, G. Choi and D. Kim, "A Cheating Attack on a Whitelist-based AntiRansomware Solution and its Countermeasure," 2023 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2023, pp. 01-04, doi: 10.1109/ICCE56470.2023.10043480.
6. C. B. J., S. A. Kudtarkar and Mohana, "Targeted Ransomware Attacks and Detection to Strengthen Cybersecurity Strategies," 2023 Second International Conference on Automation, Computing and Renewable Systems (ICACRS), Tirunelveli, India, 2023, pp. 1039-1044, doi: 10.1109/ICACRS58579.2023.10404203.
7. Y. Prajapati and K. Gosai, "Windows Forensic Analysis and Detection of Ransomware Attacks Using Event Logs and Tools," 2024 4th International Conference on Intelligent Technologies (CONIT), Karnataka, India, 2024, pp. 01-06, doi: 10.1109/CONIT61985.2024.10626973.
8. Alzahrani, S., Xiao, Y., Asiri, S., Zheng, J., & Li, T. (2025). A survey of ransomware detection methods. IEEE Access. https://doi.org/10.1109/ACCESS.2025.XXXXXXX
9. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150. https://doi.org/10.1002/ett.4150
10. Sharmila, S. P. (2026). Enhanced cyber threat intelligence by network forensic analysis for ransomware as a service (RaaS) malwares. arXiv Preprint. https://doi.org/10.48550/arXiv.2601.13873