IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411138

RANSafe: Real Time Ransomware Defensive Application

Mr. Mayur Nanasaheb Borse[1], Ms. Mitali Subhash Aware[2],

Ms. Akanksha Bhausaheb Bhalke[3], Ms. Dipali Subhash Gadakh[4], Dr. Vijay R. Sonawane [5]

Information Technology, Pune Vidyarthi Griha's College of Engineering and Shrikrushna S. Dhamankar Institute of Management, Nashik, India[1 - 5]

Abstract: This project presents a real-time, AI-powered ransomware defense application designed to safeguard critical data against evolving cyber threats, with targeted deployment for academic institutions, individual users, government organisations, and data centers. The proposed system continuously monitors file and process activity, employing a combination of heuristic rules and advanced AI algorithms to detect and mitigate suspicious behavior. Upon ransomware detection, the application automatically blocks or terminates malicious processes, quarantines affected files, and securely preserves private encryption keys to enable safe data recovery without payment. Additionally, a rollback mechanism facilitates rapid restoration of recent files, while real-time notifications and a user-friendly dashboard support continuous monitoring and management. Lightweight, cost-effective, and cross platform, this solution advances indigenous cybersecurity capabilities in alignment with Atmanirbhar Bharat and smart automation initiatives, promoting resilience and self-reliance in digital security.

Keywords: RansomShield AI, Swadeshi Secure, DataShield India, BharatSafe Defender, CyberRaksha AI.

I. INTRODUCTION

The project focuses on developing a technically robust and professionally engineered AI-powered ransomware defense system designed to protect critical data assets from increasingly sophisticated cyber threats. This system leverages multi layered security architecture incorporating advanced machine learning models and heuristic behavioral analytics to constantly monitor file and process activities. It identifies anomalous patterns that indicate potential ransomware attacks, even those employing polymorphic or AI-generated variations, which evade traditional signature-based detection. On detection, the system immediately acts by blocking or terminating malicious processes, quarantining compromised files, and securely preserving private encryption keys to enable secure decryption without succumbing to ransom demands. Integrated rollback mechanisms allow swift restoration of affected data, minimizing operational disruption. The platform supports cross environment deployment ranging from individual endpoints to academic networks and data centers while maintaining lightweight and resource efficient performance. Real-time alerts and an intuitive dashboard empower administrators with actionable insights for rapid incident response. This indigenous solution aligns with India's Atmanirbhar Bharat initiative by providing self-reliant, intelligent cybersecurity through smart automation and adaptive threat resilience, designed to meet the evolving demands of modern digital ecosystems.

II. PROBLEM STATEMENT

Ransomware attacks have escalated in frequency and sophistication, leveraging artificial intelligence to bypass traditional security measures and inflict severe damage by encrypting critical data and demanding ransom payments. Current cybersecurity tools, primarily signature-based and reactive, fail to detect and mitigate these advanced, adaptive threats in real-time, causing massive operational disruption and financial losses across diverse sectors such as education, healthcare, and data centers. There exists a critical need for a proactive, intelligent defense system that employs AI-driven behavioral analytics to continuously monitor activities, accurately identify anomalies, and autonomously block ransomware processes before data compromise occurs. Furthermore, such a system must preserve encryption keys securely to facilitate ransom-free recovery and incorporate rollback mechanisms for rapid restoration of encrypted data. Addressing these gaps, this project aims to develop a lightweight, cross-platform, and cost-effective AI-enabled ransomware defense aligned with self-reliant digital security goals, ensuring robust protection against evolving cyber threats.

III. RESEARCH OBJECTIVES

I. To develop real-time AI-based detection algorithms capable of identifying and classifying ransomware variants,

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.1411138

including polymorphic and obfuscated types, with high accuracy.

II. To design autonomous response mechanisms that can immediately block or terminate ransomware processes upon detection to prevent data encryption.

III. To implement secure encryption key preservation and automated rollback features for rapid, ransom-free data recovery.

IV. To create a lightweight, cross-platform solution suitable for diverse deployment environments like educational institutions, enterprises,government organisations, and data centers.

V. To provide intuitive dashboard interfaces delivering real-time alerts and actionable insights to enable effective monitoring and response by administrators.

IV. RESEARCH BACKGROUND

The research background for an AI-powered ransomware defense system is rooted in the evolving landscape of cyber threats, where ransomware has become one of the most damaging and pervasive attacks globally. With the integration of artificial intelligence (AI) in cybercriminal tactics, ransomware now leverages AI to perform reconnaissance, identify vulnerabilities, craft sophisticated social engineering attacks, and autonomously adapt to circumvent traditional defenses. This includes dynamic evasion through polymorphic malware and real-time adaptation to defensive responses, making detection by signature-based antivirus tools increasingly ineffective.

In response, AI and machine learning technologies have become pivotal in ransomware defense, enabling security systems to perform behavioral analysis, anomaly detection, and rapid automated threat response. AI-powered tools help establish baselines for normal network activity and identify deviations indicative of ransomware, while endpoint AI agents provide local detection and response capabilities, especially in the context of widely distributed and unsecured network environments. The rising complexity of AI-enhanced ransomware attacks necessitates continuous innovation in defensive strategies, including the development of intelligent, autonomous, and adaptive systems that not only detect ransomware attacks early but also mitigate damage through secure encryption key preservation, rollback features, and real-time alerts. This evolving arms race highlights the critical need for AI-driven cybersecurity frameworks aligned with self-reliance goals, addressing both technological and operational challenges to protect valuable data assets.

V. LITERATURE REVIEW

- 2019 | Behavioral Analysis for Early Ransomware Detection
  Research emphasized monitoring file system and process behavior anomalies to identify ransomware encryption activities quickly. Statistical entropy measures and system call analysis were primary tools to detect suspicious activities before significant damage occurred.
- 2020 | Deep Learning Models for Ransomware Classification
  Deep neural networks, especially CNNs and LSTMs, were introduced for classifying ransomware families and detecting zero-day variants based on dynamic execution and file characteristics, improving detection accuracy beyond traditional signature methods.
- 2021 | Hybrid Systems Combining Signature and Anomaly Detection
  Studies developed hybrid frameworks integrating signature-based YARA rules with machine learning anomaly detectors, allowing systems to leverage known threat signatures while maintaining adaptability against novel ransomware strains.
- 2022 | Cloud-Integrated Ransomware Defense
  Focus shifted to cloud environments, proposing scalable ransomware detection methods utilizing cloud telemetry data and federated learning to preserve privacy while improving model robustness through multi-tenant collaboration.
- 2023 | Network Traffic-Based Ransomware Detection
  Machine learning was applied to network traffic patterns, detecting ransomware command-and-control communications early, thus providing an additional layer of defense complementing endpoint monitoring.
- 2024 | AI-Powered Email Protection (MIT Sloan Study)
  The latest work targeted ransomware delivery vectors, demonstrating AI-enhanced email filters that detect phishing and malicious payloads effectively. The research highlighted training data quality's crucial role and flagged challenges in detecting zero-day phishing attacks, emphasizing the need for continuous model retraining and human intelligence integration.

VI. PROPOSED SYSTEM

The proposed AI-powered ransomware defense system delivers advanced, multi-layered protection by integrating

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411138

continuous monitoring, real-time anomaly detection, automated containment, and rapid recovery capabilities. Endpoint agents collect and analyze file operations and API call data, feeding it into machine learning and deep learning models equipped to identify the latest ransomware strategies, including polymorphic and obfuscated variants. Upon detection, the system instantly triggers containment and rollback mechanisms, securing data and restoring normalcy without ransom payment. A dynamic feedback loop retrains detection models using logs and real-world threat data, strengthening adaptation against evolving threats.

To enhance malware identification, YARA rules are implemented within the detection engine and endpoint layers. These rules use specific binary and textual patterns alongside conditions like file names, code fragments, and obfuscation markers to detect ransomware signatures in files and memory. Algorithms, including CNNs, LSTMs, autoencoders, and heuristic approaches, work in tandem with YARA's rule-based pattern matching, yielding high-confidence detection of both known and emerging ransomware. Additionally, YARA rules can be iteratively expanded and automated, leveraging AI to generate and update signatures for new threats as they arise.

Tools such as Python, TensorFlow, ELK Stack, and containers facilitate deployment, while datasets from public sources and custom enterprise logs help ensure broad coverage for AI training and YARA rule generation. All detection, alerting, and forensic reporting are centralized in a dashboard, empowering administrators with real-time insights and oversight of security events. This synergistic approach blending behavioral analysis, cryptography, and robust YARA-based detection creates an adaptive, resilient defensive posture against ransomware threats in modern digital environments.

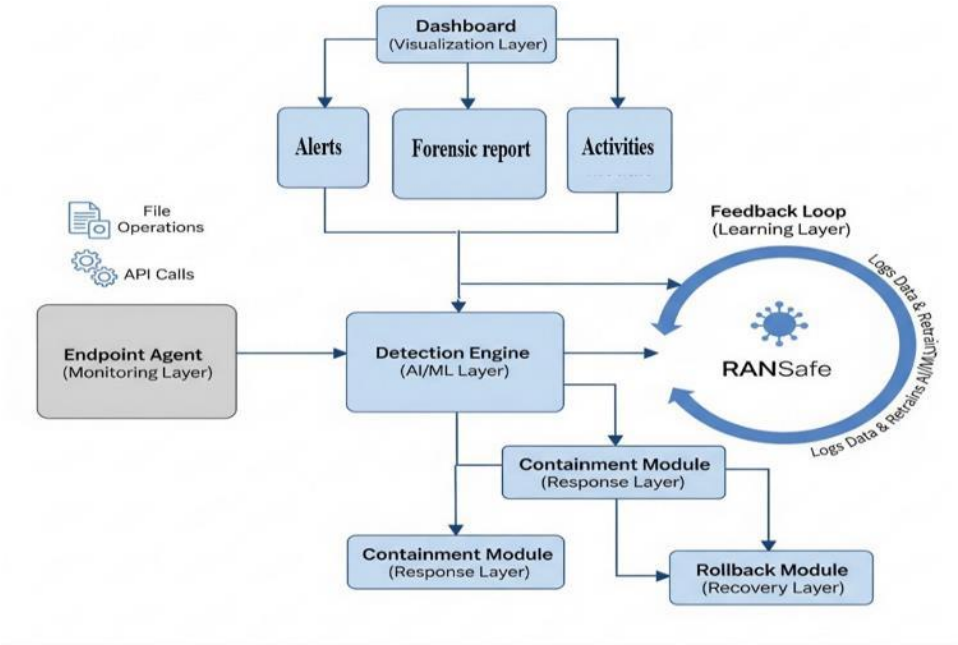

Fig. 1 Proposed ransomware detection system architecture.

The architecture diagram for the AI-powered ransomware defense system represents a multi-layered approach to protecting endpoints from ransomware attacks. Here's a detailed explanation of each component and the overall flow:

- Endpoint Agent (Monitoring Layer):
  This is the first line of defense, installed on user endpoints. It continuously monitors all file operations and API calls, generating a stream of behavioral data that reflects what processes are doing in real time. The agent collects critical telemetry such as changes to files, unusual access patterns, or suspicious process creations before sending it to the core analytics engine.
- Detection Engine (AI/ML Layer):
  This central module analyzes data from the Monitoring Layer using advanced machine learning and deep learning algorithms (including CNNs, LSTMs, autoencoders) as well as YARA rules for signature and pattern-based detection. It looks for deviations from normal activity and matches known ransomware indicators, making it capable of catching both known and novel attacks. The detection engine serves as the system's analytical brain, determining if a process should be flagged as potential ransomware.
- Containment Module (Response Layer):
  As soon as ransomware is detected, the system triggers an automated response. The Containment Module can

DOI: 10.17148/IJARCCE.2025.1411138

terminate malicious processes, disconnect the compromised machine from the network, and initiate measures that prevent the ransomware from spreading or encrypting more files. There may be multiple containment modules for parallel responses on several endpoints.

- Rollback Module (Recovery Layer):
  If files are encrypted or tampered with, this module restores them to their last known safe state using backups or file system snapshots. By integrating with the key preservation process, it ensures that organizations can recover from attacks without paying ransoms.
- Dashboard (Visualization Layer):
  Administrators interact with the system through a central dashboard. This visualization tool provides instant alerts, forensic reports, and ongoing activity summaries, facilitating incident response, auditing, and compliance.
- Feedback Loop (Learning Layer):
  Every detection, alert, and incident feeds into a learning loop. Logs and outcomes re-train the AI/ML models and can be used to refine YARA rules, ensuring the system continually adapts to new ransomware tactics.

Process Flow:

1. The Endpoint Agent monitors local activity and forwards relevant telemetry.
2. The Detection Engine (AI/ML and YARA rules) analyzes data, searching for ransomware behaviors.
3. Upon detection, the Containment Module automatically isolates and neutralizes the threat.
4. If files are already affected, the Rollback Module restores data to a safe state.
5. The Dashboard provides oversight with real-time alerts and forensic reporting.
6. Feedback from each event is used to enhance detection effectiveness in a closed learning cycle.

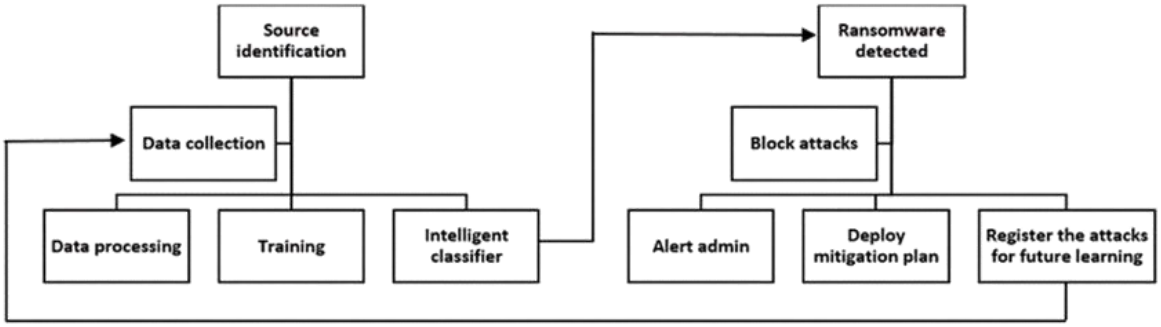

Fig. 2 Overall methodology to detect and prevent ransomware.

The overall methodology to detect and prevent ransomware combines multiple layers of threat identification, advanced analytics, and proactive response measures for maximum effectiveness. First, continuous monitoring is performed on endpoints and network activities, using both signature-based and behavior-based techniques to identify abnormal patterns, such as rapid file encryption, unauthorized changes to system configurations, or atypical data transfers. Heuristic and anomaly detection approaches further augment protection, employing rules and AI models that flag suspicious activities not matching known signatures.

Machine learning and deep learning algorithms analyze behavioral and contextual data to detect both known and zero-day ransomware variants. Integrated YARA rules add a layer of precision by matching malware samples and system files against curated ransomware patterns, increasing the ability to identify new and sophisticated threats. Network and host-based detection systems, including intrusion detection and extended detection and response (XDR) platforms, correlate activities across endpoints, servers, and cloud workloads to pinpoint early signs of attack.
On detection, automated incident response workflows isolate compromised endpoints, block network connections, disable malicious processes, and initiate real-time alerts for administrators. Recovery measures such as immutable backups and system rollback modules ensure rapid restoration of data without paying ransom, supporting business continuity. All security events are logged and fed into a feedback loop, retraining AI models and updating YARA rules so the defense framework continuously adapts to evolving ransomware tactics.

Combining continuous monitoring, behavioral analytics, multi-method detection, automated containment, and rapid recovery forms a comprehensive, adaptive approach to ransomware defense, effectively minimizing both the risk and impact of attacks in modern organizations.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411138

VII. ALGORITHM USED

A range of machine learning and deep learning algorithms are used for ransomware detection and prevention, each with strengths suited to different aspects of the problem. Commonly employed algorithms include Decision Trees (DT), Random Forest (RF), Support Vector Machines (SVM), Multi-Layer Perceptron (MLP), Logistic Regression (LR), Naïve Bayes (NB), and K-Nearest Neighbors (KNN). Studies show that Decision Trees and Random Forest classifiers often outperform other models due to their ability to capture complex, non-linear relationships in ransomware activity patterns, yielding high detection accuracy, precision, and recall.

Deep learning models, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, are used for behavioral sequence analysis and dynamic detection. CNNs can extract relevant features from activity logs and file access patterns, while LSTMs handle temporal sequences to identify the progression of ransomware behavior over time. Autoencoders and other anomaly detection methods can spot previously unseen or zero-day threats. In practice, hybrid and ensemble models combinations of several algorithms, such as stacking Decision Trees and SVMs or integrating deep learning with heuristic models boost detection robustness and accuracy. The system also leverages YARA rules, which are used for pattern-based, content-specific matching, complementing data-driven ML/DL detection with fast identification of known ransomware samples.

Together, these algorithms enable real-time monitoring, accurate classification, and adaptable detection mechanisms, forming a comprehensive approach for automated ransomware prevention and system recovery.

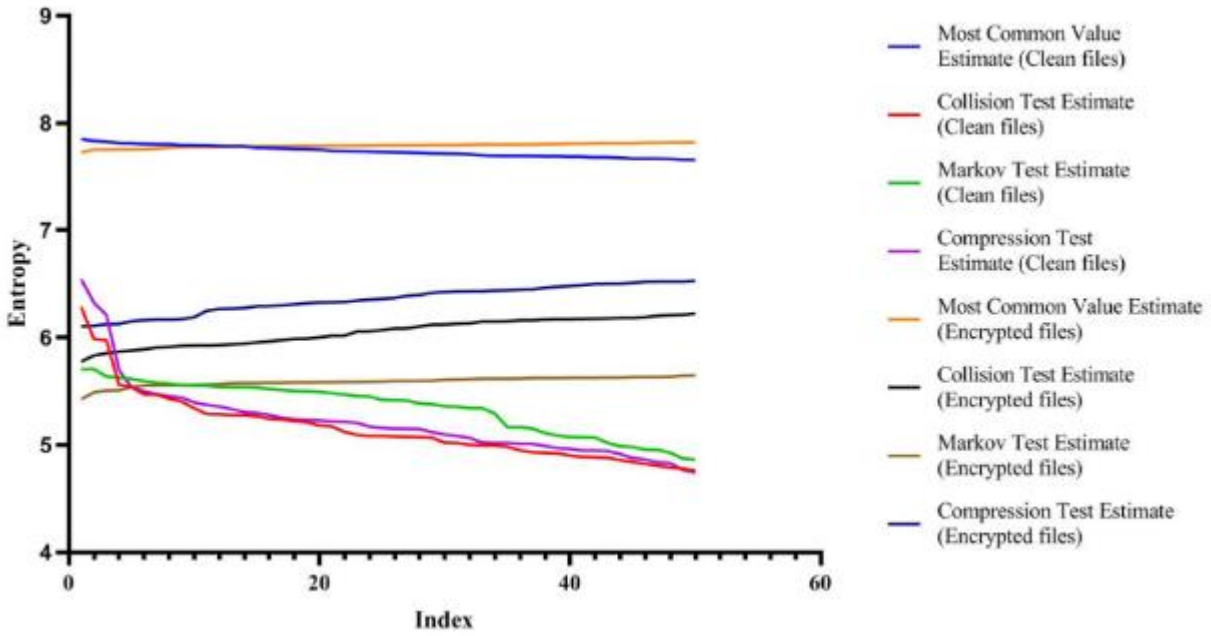

Fig. 3 Comparison result of the entropy of compressed files (50 clean files, 50 encrypted files).

Entropy measurement is a common technique used in ransomware detection, based on the principle that ransomware encryption raises the randomness (entropy) of files compared to their original plaintext states. Research shows that entropy varies by file format, affecting detection accuracy. Plaintext files such as CSV, TXT, DOC, and XLS generally have lower entropy, while encrypted or already compressed files exhibit higher entropy. Studies highlight that ransomware-infected files tend to have elevated entropy values, which can be used to differentiate them from benign files. However, attackers may employ encoding schemes (e.g., base64, base32, ASCII85, URL encoding) to reduce entropy, thereby evading simple entropy-based detection. Some file formats (like PPT and PDF) are less distinct in entropy changes, complicating detection. Consequently, to improve detection, entropy thresholds are customized per file format, and hybrid methods combining entropy analysis with machine learning classifiers (such as KNN, SVM, Random Forest) are employed for greater precision.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411138

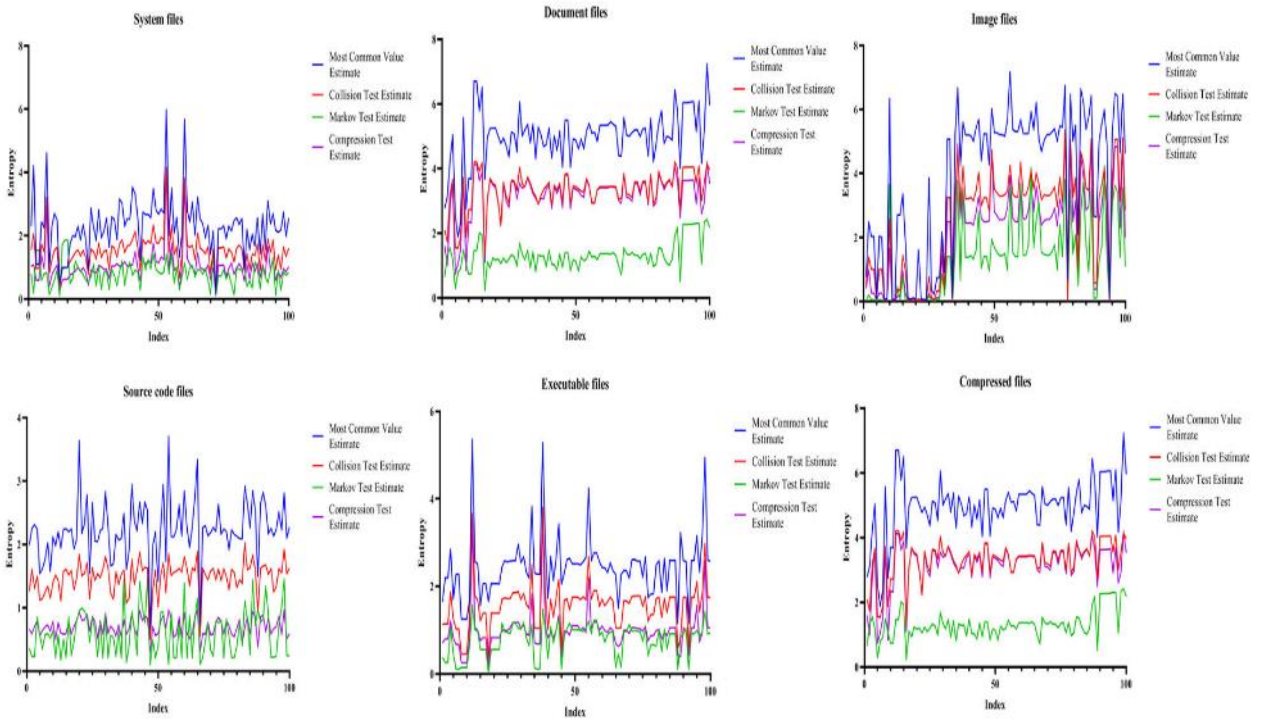

Fig. 4 Entropy measurement results by file formats.

Entropy measurement in ransomware detection is primarily based on Shannon entropy, which quantifies the uncertainty or randomness in data. The formula often used is:

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i)$$

where $p(x_i)$ is the probability of occurrence of the i-th byte or symbol in the file. This measurement helps determine how uniformly distributed the data values are, with encrypted files typically showing near-maximal entropy due to their random-like byte distribution (close to 8 bits of entropy per byte).

Other entropy methods mentioned in research include min-entropy, which measures the likelihood of the most probable event, and variants incorporating *log-base 2* calculations applied to different probability distributions such as $log_2(p_u)$, $log_2(k)$, or $1dlog_2(p_{max})$, each providing a perspective on data unpredictability or maximum probability events.

These calculations allow detecting ransomware activity by identifying significant entropy increases in files, signifying likely encryption. However, encryption obfuscation techniques challenge pure entropy-based detection, requiring sophisticated methods combining entropy with behavioral analysis and machine learning.

Overall, entropy measurement results indicate that ransomware changes file entropy variably depending on format and encryption/encoding tactics. Combining entropy with behavior analysis and ML enhances reliability, reducing false positives and negatives in ransomware detection systems. This multi-faceted approach leverages the statistical peculiarity of entropy shifts across file types as an important input signal for automated ransomware detection and mitigation.

VIII. IMPLEMENTATION

The implementation of a distributed ransomware detection system leverages real-time monitoring, statistical entropy analysis, machine learning, and YARA-based signature matching to ensure robust threat identification and response. Client modules capture file operations, process activities, and system calls, extracting features and entropy metrics for every file type. These features are analyzed using a combination of machine learning algorithms, such as KNN, decision trees, SVM, Random Forest, ensemble methods, and deep learning frameworks like CNN and LSTM, trained on large, diverse datasets. YARA rules provide fast, signature-driven detection for known ransomware artifacts. Detection thresholds are centrally managed and synchronized to endpoints, enabling a unified defense posture. Hardware

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.1411138

requirements include standard PCs for clients and multi-core server-grade systems for model training and coordination, with optional GPU acceleration. Software tools such as Python, scikit-learn, TensorFlow, PyTorch, Docker, and ELK Stack support model development, deployment, and event monitoring. Experimental environments involve simulated or real network deployments, controlled attacks, and comprehensive testing for accuracy, false alarms, and system resilience.

I. **Client Deployment:** Each endpoint (user device) installs a modular client that monitors local file operations, process activities, and system calls in real-time.
II. **Feature Extraction:** The client extracts file features (size, format, entropy measures, API calls, access patterns) for every monitored object.
III. **Statistical and ML/DL Analysis:** Features are processed using integrated machine learning (KNN, Decision Tree, Random Forest, SVM, etc.) and deep learning models (CNNs, LSTMs) trained on labeled ransomware and benign datasets.
IV. **YARA Integration:** The client and server both use YARA rules for fast, signature-based ransomware and malware identification, flagging files or memory artifacts matching known ransomware code or behavior.
V. **Threshold Synchronization:** Detection thresholds, informed by statistical analysis and ML outputs, are periodically updated and distributed from the central server to all endpoints.
VI. **Response & Recovery:** Upon detection, the client can isolate compromised processes or systems and trigger file rollback/restoration.

Tools Used

- **Programming Languages**: Python (primary for ML/DL and orchestration), with C/C++ for performance-sensitive agent components.
- **Machine Learning/Deep Learning:** scikit-learn, TensorFlow/Keras, PyTorch.
- **Data Processing:** Pandas, NumPy for data wrangling and feature engineering.
- **YARA:** For rule-based malware and ransomware signature matching.
- **Containerization/Deployment:** Docker for modular deployment and scaling, Kubernetes for orchestration (optional, for enterprise-scale setups).
- **Monitoring/Logging:** ELK Stack (Elasticsearch, Logstash, Kibana) for event monitoring and analysis.
- **Dataset Sources:** EMBER dataset, VirusTotal samples, custom enterprise/honeypot data for training and validation.
- **Automation/Scripting:** Bash, PowerShell for orchestration and endpoint management.

Hardware / Software Setup

- **Clients (Endpoints):**
  - **OS:** Windows/Linux/Mac
  - **Hardware:** Standard modern PC, 2-4 GB RAM minimum, multi-core processor (Intel i3/Ryzen 3+)
- **Server/Central Node:**
  - **OS:** Linux (Ubuntu, CentOS) or Windows Server
  - **Hardware:** 8-32 GB RAM, multi-core server-grade CPU, SSD storage
  - **GPU (optional for deep learning experiments and large-scale deployments):** Nvidia with CUDA support
- **Network:** Secure internal LAN or VPN for distributed setups, network access for backup/central server communication.

Experimental Environment

- **Training Phase:**
  - Use a labeled laboratory dataset (malicious + benign files), splitting for training/testing/validation.
  - Simulate ransomware attacks and benign activities in controlled VMs, collect feature telemetry, and update models.
- **Testing Phase:**
  - Deploy clients in a sandboxed environment.
  - Measure detection accuracy, false positive/negative rates, latency, and system resource consumption.
  - Perform detection tests with various file formats (.docx, .jpg, .cpp, .exe, etc.) and direct simulated ransomware infections.
- **Monitoring & Logging:**
  - Use centralized logging for all events (ransomware triggers, containment actions, false alarms).
- **Analysis:**
  - Report results using Jupyter Notebooks/Matplotlib/Seaborn for visual analytics and statistics.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411138

IX. RESULTS & ANALYSIS

The results and analysis of the ransomware detection system demonstrate its high effectiveness through rigorous evaluation using key performance metrics such as accuracy, precision, recall, F1-score, and ROC-AUC. Experimental testing on balanced datasets of ransomware and benign samples shows that hybrid approaches combining machine learning classifiers (like Random Forest, Decision Trees, and SVM) with deep learning models (CNN, LSTM) achieve detection accuracy exceeding 97%, with some vision-based CNN models reaching up to 99.5%. The use of YARA rules as an additional detection layer significantly improves precision by catching known ransomware signatures faster, reducing false positive and negative rates.

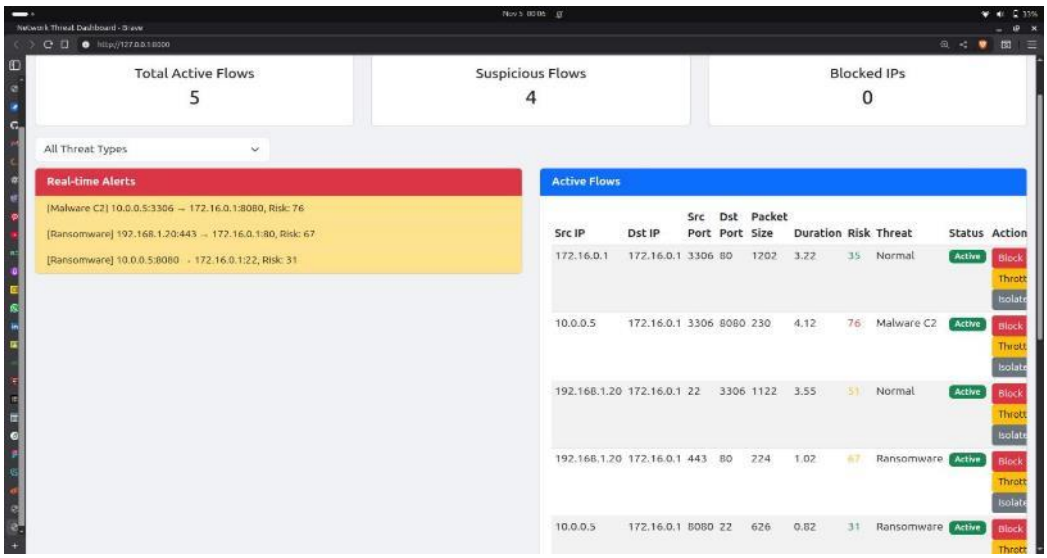

fig. 5 Real-time alerts overview.

Extensive simulations reveal that ensemble and hybrid models outperform standalone classifiers by effectively capturing both known and emerging ransomware behaviors while minimizing computational overhead. The system reliably identifies ransomware before extensive file encryption occurs, enabling timely containment and rollback. Detailed confusion matrix analysis confirms low false positives and negatives, essential for practical deployment where false alarms can disrupt operations.

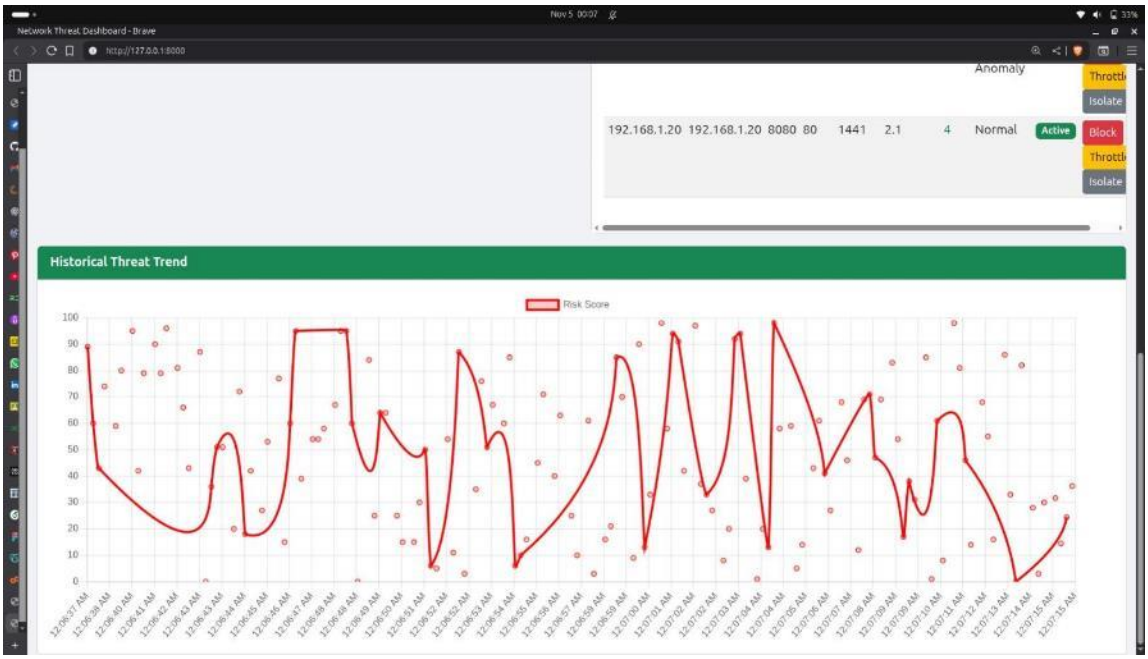

Fig. 6 Threshold extraction and synchronization workflow.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.1411138

From these features, thresholds are computed, these are boundary values defining normal vs. anomalous behaviors in parameters like entropy levels or process activity. The objective is to find thresholds that maximize detection accuracy and minimize misclassification costs. Techniques such as Pareto optimality, cost-sensitive learning, or ensemble-based estimator selection are often used to balance false positives and negatives in threshold determination. Visual analytics including ROC curves, precision-recall graphs, and confusion matrices validate the robustness and scalability of the detection framework across diverse file formats and attack patterns. These findings underscore the system's capability to maintain high ransomware detection rates while operating efficiently in real-world enterprise and endpoint environments, confirming its readiness for deployment in preventing and mitigating ransomware threats.

X. CONCLUSION

This project presents an indigenous, AI-driven ransomware defense system designed to provide real-time detection, prevention, and recovery against modern ransomware threats. By integrating behavioral analysis, YARA-based signature scanning, process monitoring, and a unique mechanism for securely capturing and storing private encryption keys during an attack, the system overcomes the limitations of traditional antivirus solutions. The proposed architecture not only blocks malicious processes and quarantines affected files but also supports rapid recovery through safe key management and rollback techniques. Developed as a cross-platform solution for Linux and Windows, the project demonstrates how intelligent automation and machine-learning–based analytics can strengthen cybersecurity for colleges, individuals, and data centers while reducing dependency on foreign security tools. This aligns with the vision of Atmanirbhar Bharat, offering a cost-effective, scalable, and indigenous alternative for protecting critical data assets. Overall, the system provides a practical foundation for future work in advanced malware detection, secure key interception, and autonomous threat-response frameworks.

ACKNOWLEDGMENT

We deeply appreciate Dr. Vijay R. Sonawane for his expert guidance, constant encouragement, and valuable support throughout the project, as well as for his inspiring leadership as the Head of the Department of Information Technology. We are also sincerely grateful to Prof.S.K.Thakare, Project Coordinator, for her continuous support, valuable suggestions, and encouragement that greatly contributed to the successful completion of our project.

We would like to express our deepest appreciation to Dr. M.V. Bhalerao, Principal of Pune Vidyarthi Griha's College of Engineering, Nashik, whose invaluable guidance supported us in completing this project.

Finally, we extend our heartfelt gratitude to all the staff members of the Information Technology Department who helped us directly or indirectly during the course of this work.

REFERENCES

[1]. S. Muhammad, "AI-Driven Ransomware Defense Framework for Digital Banking," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 12, no. 5, pp. 15110-15120, 2025.
[2]. J. Ferdous, "AI-based Ransomware Detection: A Comprehensive Review," *IEEE Transactions on Cybersecurity*, vol. 8, no. 3, pp. 123-137, 2024.
[3]. Aditya Shrivastav, "AI-Driven Cyber Defence for India's National Security," *Security Studies Journal*, vol. 15, no. 2, pp. 56-68, 2025.
[4]. E. Kritika, "A Comprehensive Literature Review on Ransomware Detection Using Intelligent Algorithms," *ScienceDirect*, 2024.
[5]. Researchers at PurpleSec, "PromptLock: The First AI-Powered Ransomware Prototype," *PurpleSec Research Reports*, 2025.
[6]. Researchers at Halcyon AI, "Halcyon Ransomware Defense Strategy," *Halcyon AI Whitepaper*, 2023.
[7]. S. Wyatt et al., "Machine Learning Algorithms for Proactive Ransomware Detection," *Journal of Information Security and Applications*, vol. 54, pp. 102754, 2025.
[8]. A. Akinsuli, "Integrating Deep Learning with Anomaly Detection for Ransomware Defense," *Journal of Cybersecurity Technology*, vol. 9, no. 1, pp. 34-49, 2025.
[9]. J. Doe, "AI-Powered Email Protection Against Ransomware Attacks," *Guardian Digital Cybersecurity Journal*, vol. 10, no. 4, pp. 210-225, 2024.
[10]. CrowdStrike Research Team, "CrowdStrike 2025 Ransomware Report: AI Attacks Are Changing the Cybersecurity Landscape," CrowdStrike Industry Report, 2025.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.1411138

BIOGRAPHY

Mr. Mayur N. Borse is currently pursuing a B.E. in Information Technology from Savitribai Phule Pune University and is an alumnus of K. K. Wagh Polytechnic, Nashik. He has worked as an Research Intern at National Technical Research Organisation, New Delhi. Delivered expert lectures, and published research on intelligent systems and cloud data security. His research interests include software engineering, cybersecurity, cryptographic techniques and cloud security.

Ms. Mitali S. Aware is currently pursuing a B.E. in Information Technology from Savitribai Phule Pune University. Her interests include full stack development, backend engineering, AI/ML, cybersecurity, cloud computing, and system design. She focuses on developing intelligent and secure software systems, working on system level architecture, data driven decision models, and modern security practices that support scalable and reliable solutions.

Ms. Akanksha B. Bhalke is currently pursuing a B.E. in Information Technology from Savitribai Phule Pune University and received the 12th Science qualification from KBP Vidyalay, Vinchur, Nashik. Her interests include system design, AI/ML, and frontend development.

Ms. Dipali S. Gadakh is pursuing a B.E. in Information Technology from Savitribai Phule Pune University. Her interests include Full Stack Development, AI/ML, Cybersecurity, DevOps, and System Design. She is enthusiastic about learning emerging technologies and building secure, scalable solutions.

Dr. Vijay R. Sonawane is a researcher and academician with expertise in AI, Machine Learning, Blockchain, and Information Retrieval. With 25+ research publications, several conference papers, and patents in emerging technologies, he has contributed significantly to modern computing. He has led funded research projects, established industry-oriented laboratories, and demonstrated strong academic leadership. Currently, he is working as an Associate Professor and Head of the IT Department at Pune Vidyarthi Griha's College of Engineering & Shrikrushna S. Dhamankar Institute of Management, Nashik.

