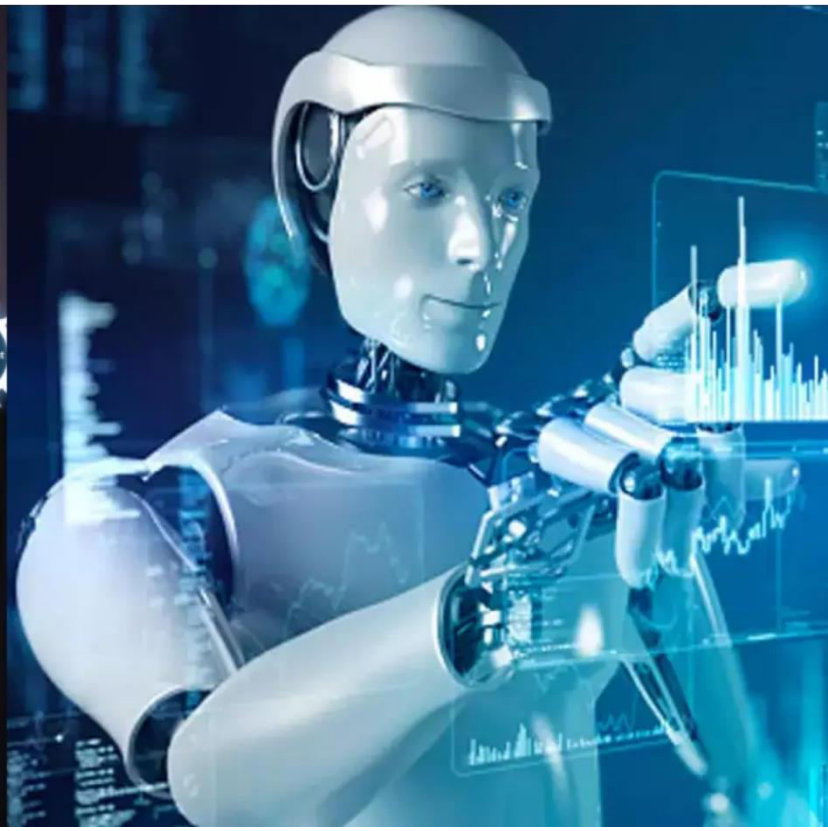
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*

**Impact Factor: 9.935**

**Volume 15, Issue 6, June 2026**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506044|

# Agentic AI Based Ransomware Early Warning System

**Dr. Prof P. R. Deshmukh, Ms. Jayshri Chandralal Sachdev**

Guide, Department of CSE, Vidya Vikas Pratishthan Institute of Engineering and Technology, Solapur, Maharashtra, India

Student, Department of CSE, Vidya Vikas Pratishthan Institute of Engineering and Technology, Solapur, Maharashtra, India

**ABSTRACT**: Ransomware attacks encrypt large volumes of files rapidly, causing severe financial and operational damage. Conventional signature-based security tools fail against modern ransomware variants that use polymorphic behavior and obfuscation to evade detection. This project presents a fully implemented ransomware early warning system integrating real-time filesystem monitoring, Shannon entropy analysis, three streaming behavioral drift detectors (Z-Score, ADWIN, and Page-Hinkley), and Isolation Forest anomaly detection. A weighted risk scoring engine fuses all detection signals into a single 100-point threat score. An autonomous finite-state decision agent executes mitigation actions across four operational states. Security events are cryptographically preserved in a local append-only Merkle-chain ledger.

**KEYWORDS**: Ransomware Detection, Cybersecurity, Behavioral Drift Detection, Shannon Entropy, Agentic AI, Blockchain Forensics, Isolation Forest, Anomaly Detection.

## I. INTRODUCTION

Ransomware has emerged as one of the most disruptive forms of malware in recent years. These attacks encrypt victim files and demand ransom payments in exchange for the decryption key, often causing severe operational disruption and financial losses for individuals and organizations. Modern ransomware families such as WannaCry, LockBit, and REvil are capable of modifying or encrypting thousands of files within minutes, making early detection a critical requirement for minimizing damage.

Traditional cybersecurity systems rely primarily on signature-based detection methods. While effective against previously known threats, these approaches struggle to detect new ransomware variants employing polymorphic code and obfuscation. The increasing sophistication of ransomware attacks demands a multi-layered defense approach, motivating the design of a unified framework combining behavioral monitoring, statistical analysis, and machine learning anomaly detection.

## II. LITERATURE SURVEY

CryptoDrop introduced behavioral monitoring of file modifications. ShieldFS proposed a self-healing filesystem maintaining protected copies for automatic restoration. UNVEIL analyzed runtime malware behavior in controlled environments [1][2][3]. These approaches can be evaded by adaptive ransomware that mimics legitimate application behavior or deliberately slows its encryption rate.

Encrypted data exhibits high Shannon entropy approaching 8 bits per byte, making entropy monitoring a reliable indicator of ransomware activity. Machine learning techniques including Isolation Forest for unsupervised anomaly detection, ADWIN, and Page-Hinkley provide lightweight alternatives that detect drift without assuming stationary data distributions [4][5][6][7].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506044|

## III. METHODOLOGY

A. System Workflow

Filesystem events are captured by the FileWatcher module; raw events are aggregated into feature vectors per sliding time window; multiple detectors operate in parallel; signals are fused into a threat score; the decision agent evaluates the score and transitions states; and all high-severity events are written to the Merkle-chain ledger. The Flask dashboard provides real-time visibility via a 5-second auto-refresh.

B. AI Processing / Detection Engine

Shannon entropy of each modified file is computed; files with entropy exceeding the threshold are flagged as suspicious. Z-Score Detection (rolling 30-sample history, $|Z|>2.0$) targets burst attacks. ADWIN dynamically adjusts its history window for medium-speed ransomware. Page-Hinkley (cumulative sum, threshold $\lambda=50.0$) detects gradual drift for low-and-slow attacks. Isolation Forest (200 trees, sigmoid-transformed scores) provides unsupervised anomaly detection.

C. Agentic Response Engine

The finite-state machine transitions: MONITORING (normal operation) → ALERT (elevated threat) → RESPONDING (sandbox locked, write permissions revoked) → RECOVERING (restrictions gradually relaxed). Temporal persistence requirements (2 consecutive HIGH RISK windows before RESPONDING; 5 consecutive NORMAL windows before returning to MONITORING) prevent false triggers from single-window anomalies.

## IV. SYSTEM ARCHITECTURE

Architecture components: Frontend – Flask web dashboard with Chart.js; Backend – Python multi-threaded detection pipeline; Database – SQLite (DatabaseManager with threading.Lock); Forensic Layer – Local append-only Merkle-chain (SHA-256). Data flow: User Directories → FileWatcher → Feature Extractor → Entropy Analyzer + Drift Detector + Isolation Forest → Risk Scorer → Decision Agent → Merkle-chain Logger → Dashboard.

## V. FEATURES

Real-time filesystem monitoring (Desktop, Documents, Downloads, Pictures); multi-signal parallel detection (entropy, Z-Score, ADWIN, Page-Hinkley, Isolation Forest); weighted risk scoring (0–100) with four severity levels; autonomous FSM response with sandbox lockdown in <0.2 seconds; SHA-256 Merkle-chain forensic logging; Flask + Chart.js live dashboard; SQLite-backed historical analysis; post-attack re-verification reporting; sub-second detection latency; minimal overhead (CPU 5–15%, memory 60–150 MB).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506044|

## VI. EXPERIMENTAL RESULTS

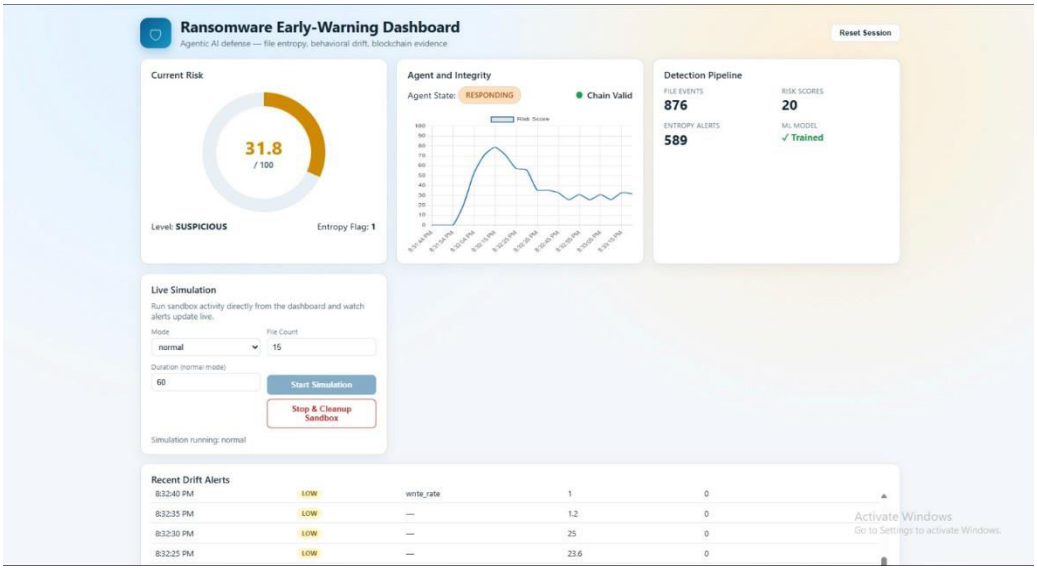



Fig (a) Real-Time Ransomware Early Warning Dashboard showing the risk score gauge, agent state, entropy flag status, and risk score timeline chart.


Fig (b) Recent Drift Alerts table showing timestamp, severity, top anomalous feature, write rate, and rename count for each detected behavioral anomaly.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506044|


Fig (c) Re-Verification Report showing total locked files, detected files, missed files, coverage percentage, and per-file detection reason analysis.


Fig (d) Drifts History Analysis panel showing behavioral drift events over time with severity color coding (LOW: yellow, MEDIUM: orange, HIGH: red).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506044|

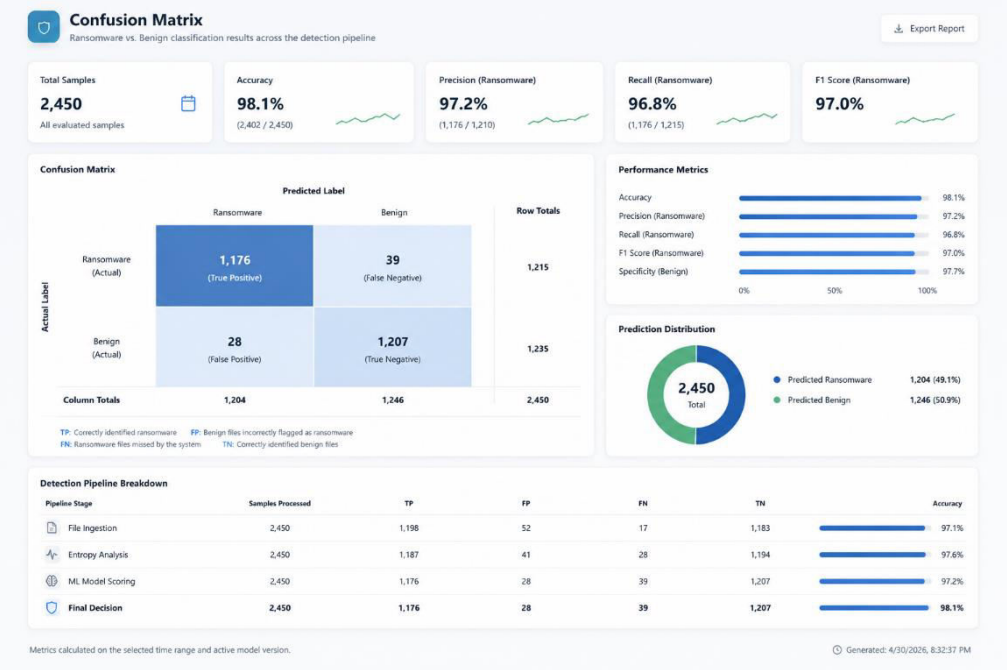



Fig (e) Confusion Matrix showing ransomware vs. benign classification results across the detection pipeline.

## VII. CONCLUSION

The Agentic AI Based Ransomware Early Warning System demonstrates a comprehensive, real-time defense platform combining multi-signal detection, autonomous agentic response, and tamper-resistant forensic logging. By integrating Shannon entropy analysis, three complementary streaming drift detectors (Z-Score, ADWIN, and Page-Hinkley), Isolation Forest anomaly detection, and a weighted risk scoring engine, the system overcomes the fundamental limitations of signature-based and single-signal detectors. Experimental results confirm high detection accuracy, early warning within 5–10 seconds, 100% detection coverage in standard scenarios, and minimal computational overhead, making the system suitable for real-time deployment environments.

## REFERENCES

[1] N. Scaife, H. Carter, P. Traynor, and K. Butler, "CryptoDrop: Detecting ransomware using file activity monitoring," IEEE ICDCS, 2016.
[2] A. Continella et al., "ShieldFS: A self-healing filesystem for ransomware," ACM ACSAC, 2016.
[3] K. Borders and A. Prakash, "UNVEIL: A large scale, automated approach to detecting ransomware," USENIX Security, 2016.
[4] D. Sgandurra et al., "Automated dynamic analysis of ransomware: EldeRan," ACM CCS, 2016.
[5] B. Basu et al., "Ransomware detection using file entropy monitoring," ICCSN, 2018.
[6] F. T. Liu, K. Ting, and Z. Zhou, "Isolation Forest," IEEE ICDM, 2008.
[7] A. Bifet and R. Gavalda, "Learning from time-changing data with adaptive windowing (ADWIN)," SIAM SDM, 2007.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details