FIM
Intelligent File Integrity Monitoring System With Ransomware Detection

Sarulatha S[1], SrideviS[2], Rithika B[3], Santhosh Krishna S[4]
[1, 2, 3, 4] J.J.College of Engineering and Technology (JJCET), Tiruchirappalli, Tamil Nadu, India

Abstract- *File integrity monitoring has become an essential component of modern cybersecurity systems as organizations increasingly rely on digital infrastructure to store and process critical data. Unauthorized modification of files and ransomware attacks can lead to severe data loss, operational disruption, and financial damage. Traditional file monitoring systems primarily focus on detecting file changes but often fail to analyzebehavioral patterns associated with malicious activities. This paper presents an Intelligent File Integrity Monitoring System with integrated ransomware detection capabilities designed to improve host-based security monitoring. The proposed system continuously monitors file system activities such as file creation, modification, and deletion in real time. A behavioral profiling mechanismalong with a hybrid risk scoring model is applied to analyze abnormal activity patterns and classify potential threats. To detect possible ransomware encryption behavior, entropy-based analysis is performed on modified files. The framework also incorporates directory traversal detection and multi file-type monitoring to identify suspicious file access patterns that commonly occur during ransomware attacks. When abnormal activity is detected, automated response mechanisms including email alerts and file quarantine are triggered to mitigate potential damage. The system also provides a graphical dashboard for real-time monitoring and generates structured security reports for forensic analysis. Experimental testing demonstrates that the proposed monitoring system effectively detects abnormal file behavior and enhances the ability to identify potential ransomware activities in host-based environments.*

Keywords: File Integrity Monitoring (FIM), Ransomware Detection, Behavioral Analysis,Hybrid Risk Scoring, Entropy-Based Detection, Directory Traversal Detection, Cybersecurity.

I. INTRODUCTION

The rapid growth of digital technologies and interconnected computing systems has significantly increased the importance of cybersecurity in modern organizations. Sensitive data such as financial records, personal information, and organizational documents are stored and processed within computer systems. Unauthorized modification or destruction of these files can lead to serious consequences including data loss, financial damage, and operational disruption. One of the most critical cyber threats affecting modern systems is ransomware, which encrypts files and demands payment from victims to restore access.

File Integrity Monitoring (FIM) is a security technique used to detect unauthorized changes to files within a system. Traditional FIM solutions typically rely on simple methods such as file hashing or timestamp comparison to identify modifications. While these approaches are effective for detecting basic changes, they often fail to identify advanced attack patterns where malicious programs rapidly modify multiple files or scan system directories before launching attacks.

Modern ransomware attacks follow a sequence of activities that includes directory scanning, accessing multiple file types, and encrypting files in a short period of time. These behavioral patterns cannot always be detected using conventional monitoring techniques. Therefore, intelligent monitoring mechanisms are required to analyze file activity patterns and detect suspicious behavior in real time.

To address these challenges, this paper proposes an Intelligent File Integrity Monitoring System with integrated ransomware detection capabilities. The proposed system continuously monitors file system events such as file creation, modification, and deletion. A behavioral profiling mechanism is used to analyze patterns of file operations and identify abnormal activities. A hybrid risk scoring model is applied to evaluate the severity of detected events and classify potential threats.

In addition, the system employs entropy-based analysis to detect potential ransomware encryption behavior by analyzing the randomness of file content. Directory traversal detection is also incorporated to identify situations

where multiple directories are accessed rapidly, which is a common characteristic of ransomware scanning activities. Furthermore, the system monitors access to multiple file types to detect abnormal file targeting patterns.

When suspicious activity is detected, automated response mechanisms such as email alerts and file quarantine are triggered to prevent further damage to the system. The system also provides a graphical dashboard for real-time monitoring and generates detailed security reports that can assist administrators in forensic investigation.

The main objective of this research is to develop an intelligent monitoring framework that enhances traditional file integrity monitoring by integrating behavioral analysis and ransomware detection mechanisms. The proposed approach aims to improve early detection of malicious activities and strengthen host-based cybersecurity defences.

II. LITERATURE SURVEY

A. File Integrity Monitoring Systems

File Integrity Monitoring (FIM) has been widely used as a security mechanism to detect unauthorized modifications in system files. Traditional FIM systems typically rely on techniques such as file hashing, checksum verification, and timestamp comparison to identify changes in files. These methods are effective in detecting simple modifications and ensuring data integrity. However, conventional FIM approaches mainly focus on identifying file changes and often fail to detect complex attack patterns or analyzebehavioral activities associated with malicious programs.

B. Behavior-Based Intrusion Detection

Behavior-based intrusion detection systems have been proposed to improve the detection of suspicious activities in computer systems. These systems monitor patterns of system events such as file access frequency, process behavior, and system calls. By analyzing abnormal patterns in system behavior, such approaches can detect previously unknown attacks that signature-based systems may fail to identify. However, behavior-based detection methods may sometimes produce false positives when legitimate user activities appear abnormal to the monitoring system.

C. Ransomware Detection Techniques

Ransomware attacks have become one of the most critical cybersecurity threats in recent years. Many ransomware detection techniques focus on identifying encryption behavior within files. One commonly used method is entropy-based analysis, which measures the randomness of file data to detect possible encryption activity. Encrypted files typically exhibit higher entropy values compared to normal files. In addition, researchers have also studied abnormal file access patterns such as rapid directory traversal and access to multiple file types within a short period of time, which are common characteristics of ransomware behavior.

Despite these advancements, many existing systems rely on a single detection technique, which limits their effectiveness against sophisticated cyber-attacks. The proposed system addresses these limitations by integrating multiple monitoring mechanisms including file integrity monitoring, behavioral profiling, entropy-based ransomware detection, directory traversal detection, and multi file-type monitoring within a unified framework. This integrated approach improves the ability to detect abnormal file activities and enhances the effectiveness of host-based intrusion detection systems.

III. SYSTEM DESIGN AND METHODOLOGY

A. System Architecture

The proposed Intelligent File Integrity Monitoring (FIM) system is designed as a host-based security monitoring framework that integrates real-time file activity monitoring, behavioral profiling, ransomware detection, and automated response mechanisms. The system follows a modular architecture in which each module performs a specific function within the monitoring workflow to detect abnormal file activities and potential ransomware behavior.

The architecture is designed to continuously observe file system events and analyze them using multiple detection techniques such as hybrid risk scoring, entropy analysis, directory traversal monitoring, and multi file-type access detection. Each module contributes to identifying suspicious activities and improving the overall reliability of threat detection.

The overall workflow of the proposed system is illustrated below:

File System Monitoring
↓
File Event Detection (Create / Modify / Delete)
↓
Behavior Profiling
↓
Hybrid Risk Scoring

↓
Entropy-Based Ransomware Detection
↓
Directory Traversal Detection
↓
Multi File-Type Access Detection
↓
Alert and Response Mechanism
↓
Dashboard Visualization and Report Generation

This architecture enables the system to monitor file activities in real time, detect abnormal behavior patterns, and automatically generate alerts and security reports for system administrators.

B. Hardware Requirements

The hardware requirements for implementing the Intelligent File Integrity Monitoring system are minimal and suitable for standard computing environments or laboratory setups.

Processor: Intel Core i5 or higher
RAM: Minimum 8 GB
Storage: Minimum 100 GB free disk space
Network Interface: Ethernet or Wireless Network Adapter

These hardware specifications are sufficient for running the monitoring system, performing real-time file analysis, and generating security reports without significant performance overhead.

C. Software Requirements

The proposed system is implemented using widely available software tools and programming libraries that support real-time monitoring and security analysis.

Operating System: Windows / Linux
Programming Language:Python
FileMonitoring Library : Watchdog
Graphical Interface : Tkinter
Visualization Library : Matplotlib
Report Generation : Report Lab PDF library

These tools enable the development of a flexible monitoring framework capable of detecting file system events, analyzing suspicious behavior, and generating structured security reports.

D. Implementation Methodology

The Intelligent File Integrity Monitoring system follows a multi-stage methodology to monitor file activities and detect potential ransomware behavior.

Phase 1: File Monitoring Initialization

The monitoring process begins by selecting a target directory or file system location. The system initializes the file monitoring engine and continuously listens for file system events such as file creation, modification, and deletion.

Phase 2: File Event Detection

Whenever a file operation occurs, the monitoring module captures the event and records details such as file path, event type, and timestamp. These events are forwarded to the behavior profiling module for further analysis.

Phase 3: behavioral Profiling

The behavior profiling module analyzes the frequency and pattern of file operations within a specific time window. Rapid modification of multiple files or repeated access to system directories may indicate suspicious activity

.**Phase 4: Hybrid Risk Scoring**

A hybrid risk scoring mechanism evaluates each event based on its severity and behavioral characteristics. Different file events such as creation, modification, and deletion are assigned risk values that contribute to an overall threat score.

Phase 5: Ransomware Detection using Entropy Analysis

To detect potential ransomware encryption, the system performs entropy analysis on modified files. Encrypted files generally exhibit higher randomness compared to normal files, which helps identify possible encryption activity.

Phase 6: Directory Traversal Detection

The system also monitors the number of directories accessed within a short period of time. Rapid traversal across multiple directories is considered a suspicious pattern commonly associated with ransomware scanning behavior.

Phase 7: Multi File-Type Monitoring

The monitoring system tracks access to different file extensions such as documents, images, and spreadsheets.

Access to multiple file types within a short time interval increases the risk level of the detected activity.

Phase 8: Alert and Response Mechanism

If the calculated risk score exceeds a predefined threshold, the system triggers automated response actions such as sending email alerts to administrators and moving suspicious files to a quarantine directory.

Phase 9: Report Generation and Visualization

Finally, the system generates a structured security report containing detected events, risk levels, and attack activity summaries. A graphical dashboard is also provided to visualize monitoring statistics and system activity in real time.

IV. RESULTS AND ANALYSIS

A. Experimental Setup

The Intelligent File Integrity Monitoring system was tested in a controlled laboratory environment to evaluate its effectiveness in detecting abnormal file activities and potential ransomware behavior. The testing environment consisted of a monitoring system and a target directory where multiple file operations were performed to simulate normal user activity as well as suspicious activity patterns.

Monitoring System : Windows / Linux system running theFIMmonitoring application
Target Environment : Local directory containing multiple files of different types

The monitoring system continuously observed the target directory and recorded file events such as file creation, modification, and deletion. During the testing process, various file operations were performed to analyze the behavior of the monitoring framework and evaluate the accuracy of threat detection.

B. File Activity Monitoring Results

The monitoring framework successfully detected different types of file system events occurring within the target directory. The system captured file creation, modification, and deletion events in real time and recorded them within the monitoring log.

Each detected event was analyzed using the hybrid risk scoring mechanism to determine the severity of the activity. The monitoring dashboard displayed the detected events along with the corresponding risk levels and timestamps.

Table 1 summarizes the detected file activity events during the experimental testing phase.

Table 1. File Activity Monitoring Results

Event Type	Description	Detection Result ID
File Created	New file generated in monitored directory	Detected Successfully
File Modified	Existing file content modified	Detected Successfully
File Deleted	File removed from monitored directory	Detected Successfully

The results demonstrate that the monitoring system effectively captures file system events and provides real-time visibility into file activities occurring within the monitored environment.

C. Risk Classification Results

The proposed system evaluates each file event using a hybrid risk scoring mechanism that assigns risk values based on event type and behavioral characteristics. This approach enables the system to classify detected activities into different risk levels such as Low, Medium, High, and Critical.

During the experimental testing process, file creation events were categorized as low risk activities, while repeated modification or deletion of files increased the overall risk score. When multiple suspicious activities occurred within a short time interval, the system automatically increased the risk classification level.

Table 2 presents the risk classification results generated by the monitoring system.

Table 2. Risk Classification Results

Event	Risk Score	Risk Level
File Creation	Low Score	Low
File Modification	MediumScore	Medium
File Deletion	Higher Score	High
Encryption Behavior Detected	Very High Score	Critical

The risk classification mechanism enables system administrators to quickly identify suspicious activities and prioritize investigation efforts.

D. Ransomware Behavior Detection

To evaluate the ransomware detection capability of the system, simulated encryption behavior was performed by modifying multiple files rapidly within the monitored directory. The entropy analysis module analyzed the randomness of modified file content to determine whether encryption activity was present.

The results indicated that files with higher entropy values were flagged as suspicious by the system. When combined with behavioral indicators such as rapid modification of multiple files and access to various file types, the system successfully detected potential ransomware-like behavior.

The monitoring dashboard displayed warnings for abnormal activity and increased the overall system risk score. These results demonstrate that the entropy-based detection mechanism can effectively assist in identifying potential ransomware encryption behavior.

E. Performance Metrics

The performance of the Intelligent File Integrity Monitoring system was evaluated by measuring the responsiveness of the monitoring framework and the time required to process file events.

The system performs multiple operations including event detection, behavioral profiling, risk scoring, ransomware detection analysis, and report generation. The overall system performance depends primarily on the number of file operations occurring within the monitored directory.

Table 3 summarizes the observed performance characteristics of the monitoring framework.

Table 3. Performance Metrics

Process Stage	**Description**	**Performance Observation**
File Event Detection	Detecting file creation, modification, and deletion	Instant detection
Behavior Profiling	Analyzing event patterns	Completed quickly
Risk Scoring	Assigning severity levels	Completed instantly
Ransomware Detection	Entropy analysis of modified files	Completed within seconds
Report Generation	Completed within seconds	Completed quickly

The results indicate that the proposed monitoring framework performs efficiently with minimal processing delay while continuously monitoring file activities.

F. False Positive Analysis

During file monitoring operations, there is a possibility that certain legitimate user activities may appear suspicious to the monitoring system. For example, users may legitimately modify multiple files within a short period of time during normal work processes such as editing documents or performing software updates.

In such cases, the monitoring system may temporarily increase the risk score even though the activity is not malicious. These situations are referred to as false positives in intrusion detection systems.

To reduce the occurrence of false positives, the proposed system uses multiple detection mechanisms including behavioral profiling, entropy analysis, and file-type monitoring. By combining multiple indicators, the system improves the accuracy of threat detection and reduces the likelihood of incorrectly classifying normal user activity as malicious behavior.

Future improvements may include integrating machine learning based behavior analysis and adaptive risk scoring techniques to further enhance detection accuracy and minimize false positive alerts.

V. DISCUSSION

A. Advantages ofIntelligent Monitoring

The proposed Intelligent File Integrity Monitoring system provides several advantages compared to traditional file monitoring solutions. Conventional monitoring systems mainly focus on detecting file modifications without analyzing the behavioral patterns associated with malicious activities. In contrast, the proposed system integrates multiple detection mechanisms such as behavioral profiling, entropy-based ransomware detection, hybrid risk scoring, directory traversal monitoring, and multi file-type access detection.

The integration of these mechanisms enables the system to detect suspicious file activity more accurately. Real-time monitoring allows administrators to quickly identify abnormal events occurring within the system. In addition, the automated alert mechanism and file quarantine feature help reduce the impact of potential ransomware attacks by responding immediately when suspicious activity is detected.

Another advantage of the system is the visualization capability provided through the monitoring dashboard. The dashboard displays file activity statistics, risk levels, and event logs in real time, allowing administrators to easily monitor system security status. The automated report generation module also simplifies forensic analysis by providing structured documentation of detected events and security alerts.

B. Limitations and Challenges

Despite the advantages of the proposed monitoring framework, certain limitations exist. The detection mechanism primarily relies on file behavior analysis and entropy measurement, which may occasionally classify legitimate user activities as suspicious. For example, situations where users perform large numbers of file modifications within a short time period may temporarily increase the system risk score.

Another challenge is related to performance in environments where extremely large numbers of file operations occur simultaneously. Continuous monitoring of high-frequency file events may increase system resource usage in large-scale enterprise environments. However, the system is optimized to minimize processing delays and maintain efficient monitoring performance.

Future improvements may include integrating machine learning based anomaly detection techniques to enhance behavioral analysis and further reduce false positive alerts.

C. Ethical and Security Considerations

File monitoring and security analysis must always be performed within appropriate ethical and legal boundaries. Monitoring tools should only be deployed on systems where administrators have proper authorization to analyze file activities.

The experiments conducted in this research were performed in a controlled laboratory environment using a dedicated test directory to simulate file activity scenarios. The system was not used to monitor unauthorized user data or external systems.

Organizations implementing file monitoring systems must ensure compliance with security policies and privacy regulations. Proper access control mechanisms should also be implemented to ensure that monitoring data and generated reports are accessible only to authorized administrators.

VI. CONCLUSION

This research presented an Intelligent File Integrity Monitoring system designed to enhance host-based cybersecurity by detecting unauthorized file modifications and potential ransomware behavior. The proposed framework integrates real-time file monitoring with behavioral profiling, hybrid risk scoring, entropy-based encryption detection, directory traversal monitoring, and multi file-type access analysis.

The experimental evaluation demonstrated that the system effectively detects file system events such as file creation, modification, and deletion while analyzingbehavioral patterns to identify suspicious activity. The integration of entropy-based analysis enables the detection of potential ransomware encryption behavior, while the hybrid risk scoring mechanism provides an effective approach for classifying threat severity levels.

The system also includes automated response mechanisms such as email alerts and file quarantine, which help mitigate potential damage caused by malicious activities. In addition, the graphical monitoring dashboard and automated report generation module provide administrators with improved visibility into system security events and simplify forensic analysis.

Future work may focus on integrating machine learning based anomaly detection techniques, expanding monitoring capabilities to large-scale enterprise environments, and improving the accuracy of threat detection mechanisms. Overall, the proposed Intelligent File Integrity Monitoring system demonstrates the effectiveness of combining behavioral analysis with traditional file monitoring techniques to strengthen host-based cybersecurity protection.

VII. ACKNOWLEDGMENT

The authors would like to express sincere gratitude to our guide, *Mrs. M. Saranya*, *Department of Computer Science and Engineering – Cyber Security, J.J. College of Engineering and Technology (JJCET), Tiruchirappalli*, for her continuous

guidance and support throughout the development of this research work. Special thanks are extended to the project supervisor and faculty mentors for their valuable suggestions, encouragement, and technical guidance during the completion of this study.

The authors also extend their sincere thanks to the project supervisors and faculty members of the Cyber Security department for their valuable guidance, motivation, and support during the implementation and evaluation phases of the project. Their suggestions helped improve the quality and effectiveness of the proposed monitoring framework.

Finally, the authors acknowledge the open-source software community for providing essential libraries and development resources such as Python security tools and monitoring frameworks that supported the implementation of the Intelligent File Integrity Monitoring system. Appreciation is also extended to colleagues and peers for their constructive feedback and support during the testing and analysis stages of the project.

REFERENCES

[1] National Institute of Standards and Technology (NIST), "Guide to Intrusion Detection and Prevention Systems," 2024.
Available: https://nvlpubs.nist.gov

[2] M. Scaife, H. Carter, and P. Traynor, "Ransomware: Analysis and Defence Strategies," IEEE Security & Privacy, 2024.
Available: https://ieeexplore.ieee.org

[3] S. Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy," Journal of Network Security, 2025.
Available: https://www.sciencedirect.com

[4] Python Software Foundation, "Python Programming Language Documentation," 2025.
Available: https://www.python.org/doc/

[5] Watchdog Developers, "Python Watchdog File Monitoring Library Documentation," 2025.
Available: https://python-watchdog.readthedocs.io

[6] MITRE Corporation, "Common Vulnerabilities and Exposures (CVE) Database," 2025.
Available: https://cve.mitre.org

[7] National Vulnerability Database (NVD), "Cybersecurity Vulnerability Information Platform," 2026.
Available: https://nvd.nist.gov

[8] IEEE Cybersecurity Research Group, "Modern Approaches to Ransomware Detection and File System Monitoring," IEEE Journals, 2025.
Available: https://ieeexplore.ieee.org