JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ASSESSING THE PERFORMANCE OF RANSOMSHIELD: A LAYERED APPROACH TO RANSOMWARE DETECTION AND DATA SECURITY

Swara Kalsekar[1], Sehar Khan[2]

MSc.CS Cybersecurity Student[1], Assistant Professor[2]

Nagindas Khandwala College

University of Mumbai, Maharashtra, India

1. Abstract: Ransomware has become one of the most serious problems in cybersecurity. Traditional defenses, such as antivirus software that uses signature-based detection, often fail to catch ransomware until files are already encrypted, leading to heavy data loss and financial damage. This paper introduces RansomShield, a multi-layered defense system designed to detect and stop ransomware at an early stage. It combines file system monitoring, process monitoring, and an adaptive machine learning model to identify unusual activity before encryption begins. Unlike existing fragmented tools, RansomShield provides a single desktop application with real-time alerts to help users take quick action. The paper discusses the methodology, objectives, and related research to show why RansomShield is an important and complete solution for defending against ransomware.

2. Index Terms: Ransomware, File System Monitoring, Process Monitoring, Machine Learning, RansomShield, Cybersecurity, Data Protection

3. Introduction:

Ransomware attacks are increasing in both number and complexity, causing serious damage to individuals, businesses, and governments. These attacks lock important files and demand payment for their release, resulting in major financial losses and loss of access to critical data. Attackers are constantly improving their methods, making traditional defenses less effective.

Most existing security tools are reactive. For example, antivirus software mainly uses signature-based detection, which works only for already known ransomware types. This means new or modified ransomware often goes undetected until the encryption has already started, leaving users with little chance of recovery.

To address these problems, proactive solutions are needed. Monitoring files and processes at an early stage can help detect suspicious behavior before damage occurs. RansomShield offers a layered strategy that combines file system monitoring, process monitoring, and the use of whitelists/blacklists for extensions. This integrated approach makes detection stronger and simpler by bringing different methods into one easy-to-use platform.

4. Literature Review:

1. GuardFS: A File System for Integrated Detection and Mitigation of Linux-based Ransomware (2024) [1]

This study explores GuardFS, a file system overlay designed to detect ransomware by monitoring file operations such as unusual entropy levels, rapid file changes, and suspicious extensions. The system also mitigates damage by halting encryption in progress.

Relevance: This work demonstrates the strength of file-level monitoring but also shows its limitations, as it does not address process behavior or adaptive threats, highlighting the need for multi-layered frameworks like RansomShield.

2. Automated Dynamic Analysis of Ransomware (2016) [2]

This research investigates the use of sandboxing and automated analysis to study ransomware behavior. By executing samples in controlled environments, the study identifies patterns in encryption activity and resource use.

Relevance: While effective in detecting unknown strains, sandboxing is resource-intensive and not suitable for real-time protection, emphasizing the value of lightweight, real-time monitoring in tools such as RansomShield.

3. Cryptographic Ransomware Encryption Detection: Survey (2023) [3]

This survey reviews cryptographic ransomware detection methods, focusing on encryption patterns, entropy, and file system anomalies. It highlights detection techniques and their challenges in handling polymorphic ransomware.

Relevance: The survey provides a comprehensive overview of ransomware detection but underscores the fragmentation of existing methods, reinforcing the need for integrated solutions.

4. Classification of Ransomware Variants Through Adaptive Pattern Recognition (2023) [4]:

The study proposes machine learning models that classify ransomware based on real-time behavioral patterns, entropy analysis,

and system activity. The authors emphasize adaptability to evolving ransomware variants.
Relevance: This work supports the machine learning layer in RansomShield, showing how adaptive models can enhance detection beyond static monitoring.
5. Ransomware Detection Based on File Entropy Analysis Using Machine Learning (2019) [5]:
This study applies entropy-based feature extraction combined with machine learning to detect ransomware encryption. It demonstrates high accuracy in early detection but is limited by dataset diversity.
Relevance: The findings validate the importance of combining entropy analysis with adaptive models, which RansomShield integrates alongside process monitoring.
6. Real-time System Call-based Ransomware Detection (2024) [6]:
The research presents a system call monitoring approach to identify malicious commands and file access behaviors. By analyzing system activity at the kernel level, the method provides rapid detection of suspicious processes.
Relevance: This study highlights the importance of process monitoring, which RansomShield incorporates to complement file system and ML-based detection.
7. SHIELD: Secure Host-Independent Extensible Logging for Tamper-Proof Detection (2024) [7]:
SHIELD leverages hardware-assisted monitoring to log and detect ransomware behavior securely, resistant to tampering by attackers. While robust, it requires specialized hardware not available to typical users.
Relevance: This approach shows strong resilience but lacks accessibility, reinforcing the practicality of a desktop-based solution like RansomShield.
8. Ransomware Prevention via Performance Counters (2018) [8]:
This study examines hardware performance counters to detect ransomware encryption attempts based on CPU usage patterns and I/O behavior.
Relevance: Although effective, this method is hardware-dependent, making it difficult to deploy widely. It highlights the need for software-based, flexible solutions such as RansomShield.

5. Theoretical Background

The theoretical foundation of this research is built on defense-in-depth strategies, anomaly detection mechanisms, and machine learning applications in cybersecurity. Key concepts include:

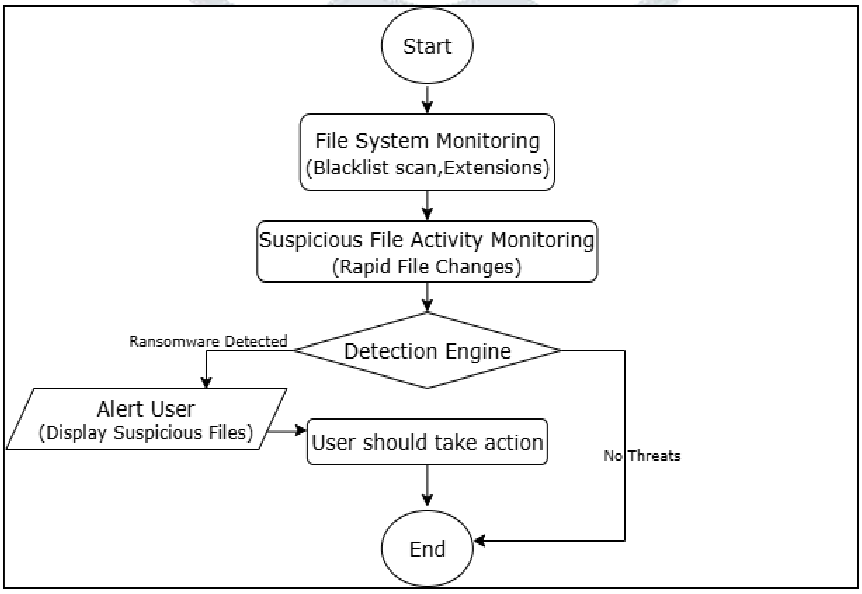
· File System Monitoring: Monitoring sudden file changes, entropy spikes, and abnormal extensions helps detect ransomware at the earliest stage. As highlighted in GuardFS: A File System for Integrated Detection and Mitigation of Linux-based Ransomware [1], file-level analysis can effectively identify ransomware encryption behavior, though it is insufficient alone.

· Defense-in-Depth: A layered security model integrates multiple protective techniques to minimize single points of failure. This principle is demonstrated in SHIELD: Secure Host-Independent Extensible Logging for Tamper-Proof Detection and Real-Time Mitigation of Ransomware Threats [7], which combines logging and monitoring to provide stronger resilience against tampering.

· Process Behavior Analysis: System call and process monitoring can expose malicious behavior such as rapid file access or encoded commands. This is supported by Real-Time System Call-Based Ransomware Detection [6], which shows how process activity can be used to identify threats beyond file-level changes.

· Machine Learning and Adaptive Models: Emerging technologies like AI and machine learning offer proactive detection against evolving ransomware. Classification of Ransomware Variants Through Adaptive Pattern Recognition in Real-Time Environments [4] demonstrates the potential of adaptive models to classify and detect new ransomware strains more accurately.

5.1. Working of the RansomShield Application:



6. Gaps in Current Research

1. Fragmented Approaches: Most studies focus on a single detection layer, such as file monitoring [1] or process analysis [6], without integrating them into a unified framework. This leaves systems vulnerable to ransomware that can bypass one layer of defense.

2. Limited Real-Time Evaluation: While surveys like Cryptographic Ransomware Encryption Detection: Survey [3] provide valuable insights, they often lack real-time deployment evaluations, reducing their practical effectiveness in live environments.
3. Hardware Dependence: Techniques such as those in Rapper: Ransomware Prevention via Performance Counters [8] and SHIELD [7] rely on specialized hardware features, which limit accessibility for general users. There is a gap in software-based, lightweight solutions.
4. Adaptability to New Variants: Although machine learning approaches (e.g., [4], [9]) show promise, many studies rely on limited datasets and may fail against novel or polymorphic ransomware. Broader evaluations are needed to improve robustness.
5. Unified User-Friendly Solutions: Existing research provides detection mechanisms but lacks integration into a single, practical application. Users often need to combine multiple tools manually, highlighting the need for unified frameworks such as RansomShield.

7. Ethical Implications

7.1. Maintaining User Privacy: The primary ethical concern in ransomware detection systems lies in maintaining user privacy. Tools like RansomShield monitor files and processes in real time, which, if mismanaged, can expose sensitive data. Ethical development requires that such monitoring be limited strictly to detecting malicious activity, without collecting or storing unnecessary user information. Transparent communication about the scope and purpose of monitoring ensures that ethical values of trust and autonomy are preserved.

7.2. Transparency and Accountability: Another ethical requirement is ensuring that the functioning of RansomShield remains transparent to users. A detection system that operates silently in the background without clear explanations risks creating suspicion and mistrust. Providing users with detailed logs of detected behavior, alerts, and justifications for actions taken (e.g., blocking a process) establishes accountability and aligns with ethical norms of openness.

7.3. Avoidance of Misuse: Cybersecurity tools can sometimes be repurposed for malicious use if not safeguarded. For instance, reverse engineering of detection mechanisms may allow attackers to design more sophisticated ransomware. Developers of RansomShield must therefore implement strong code protection, access controls, and responsible disclosure practices to prevent misuse of the system itself.

8. Legal Implications

8.1 Compliance with Cybersecurity Regulations: RansomShield, as a security application, must comply with national and international cybersecurity and data protection laws. Regulations such as the General Data Protection Regulation (GDPR) and the Indian Information Technology Act mandate strict limits on the collection, processing, and storage of user data. Ensuring compliance with these frameworks protects both developers and users from legal risks.

8.2.Liability and Responsibility: Legal accountability arises when detection systems fail or cause harm through false positives. For example, if legitimate files or processes are incorrectly flagged as ransomware and blocked, the user may suffer productivity or financial losses. Establishing clear terms of use and liability clauses ensures that responsibility is appropriately defined.

8.3.Intellectual Property and Ethical Use: RansomShield’s underlying models, detection methods, and software components fall under intellectual property protections. Proper licensing and respect for third-party software are essential to prevent legal disputes. Additionally, developers must ensure that the software is distributed in a controlled manner, preventing unauthorized adaptation for offensive purposes

9. Methodology

RansomShield employs a layered methodology combining file system monitoring, process analysis, machine learning, and real-time alerts. It monitors sudden file changes, abnormal extensions, and entropy spikes using lightweight hashing with whitelist/blacklist filtering to flag early encryption attempts. Simultaneously, active processes are examined for suspicious behavior such as rapid file access or malicious commands, while adaptive machine learning models analyze file activity, entropy patterns, and process behavior to detect evolving ransomware strains. These layers are unified into a single desktop application that delivers real-time alerts, enabling users to terminate threats before significant data loss occurs.

10. Justification for the Chosen Approach

The chosen methodology for RansomShield is justified for the following reasons:

1. Comprehensiveness:
   a. By combining file system monitoring, process monitoring, and machine learning, the framework covers multiple aspects of ransomware behavior. This ensures a broad and balanced approach to detection.
   b. Unlike single-layer methods, this integrated strategy minimizes the risk of overlooking advanced or polymorphic ransomware strains.
2. Rigorous and Reproducible:
   a. The design of RansomShield relies on established methods such as entropy analysis, system call monitoring, and adaptive classification models. These techniques can be consistently applied and replicated across different systems.
   b. Using standardized detection layers enhances the credibility of results and provides a reliable framework for future research and development.
3. Identification of Gaps:
   a. Existing literature highlights that most tools focus on only one detection method, such as GuardFS for file-level monitoring [1] or SHIELD for hardware-based logging [7].
   b. By integrating multiple approaches, RansomShield addresses this gap and demonstrates how layered monitoring can offer stronger protection.

4. Practical Relevance:
   a. The system is implemented as a single desktop application, reducing complexity for users who would otherwise need multiple tools.
   b. Real-time alerts and user-friendly controls ensure that the solution is practical for individuals and organizations alike.
5. Alignment with Review Research Objectives:
   a. The study's goal is to evaluate the effectiveness of a multi-layered ransomware defense framework rather than design a single-purpose tool.
   b. The chosen methodology directly supports this objective by integrating and analyzing multiple detection mechanisms within one system.

11. Results and Discussion

This section presents the findings from the evaluation of ransomware detection methods and compares them with the design and objectives of RansomShield.

11.1. Summary of Findings

1. File Monitoring:
   a. Findings: Research such as GuardFS: A File System for Integrated Detection and Mitigation of Linux-based Ransomware (ScienceDirect, 2024) [1] shows that monitoring file changes, entropy variations, and suspicious file extensions can effectively detect ransomware during its initial stages. GuardFS demonstrated that rapid file modifications and high-entropy outputs are strong indicators of encryption activity. This approach provides an early warning system that can prevent ransomware from spreading widely.
   b. Insight: Although effective in catching straightforward encryption attempts, file-only monitoring has limitations. Advanced ransomware often disguises its activity by hiding malicious behavior within legitimate processes or spreading encryption gradually. This means that depending solely on file-level monitoring may miss stealthy or process-driven ransomware, highlighting the need for additional detection layers.
2. Process Monitoring:
   a. Findings: Studies like Real-time System Call-Based Ransomware Detection (MDPI, 2024) [6] reveal that tracking system calls and process behavior is crucial for identifying ransomware that does not immediately alter files. By analyzing suspicious commands, encoded scripts, or abnormal access patterns, process-level monitoring captures hidden activities missed by file-based approaches. It can identify ransomware at the stage when it attempts to interact with system resources.
   b. Insight: Incorporating process monitoring into RansomShield significantly strengthens its defense. By combining file activity analysis with process behavior evaluation, the framework covers both visible and hidden ransomware operations. This layered strategy reduces blind spots and ensures broader protection against diverse attack techniques.
3. Machine Learning and Adaptive Models:
   a. Findings: Research such as Classification of Ransomware Variants Through Adaptive Pattern Recognition (ResearchSquare, 2023) [4] highlights the role of machine learning (ML) in identifying unknown or evolving ransomware strains. ML-based systems analyze file entropy, process patterns, and encryption speed, adapting over time to detect ransomware variants that bypass traditional defenses. These adaptive models improve accuracy in distinguishing between normal system activity and malicious encryption attempts.
   b. Insight: RansomShield integrates machine learning to address the weaknesses of static monitoring. The adaptive nature of ML ensures the framework evolves alongside ransomware threats, improving resilience against zero-day attacks and polymorphic ransomware. This makes RansomShield more future-proof compared to conventional detection systems.
4. Hardware and Advanced Methods:
   a. Findings: Advanced approaches such as SHIELD (ACM, 2024) [7] and Rapper: Ransomware Prevention via Performance Counters (arXiv, 2018) [9] demonstrate that hardware-assisted detection can provide strong tamper-proof monitoring. By leveraging performance counters and secure logging, these methods detect unusual system-level activity with high precision and are resistant to manipulation by attackers.
   b. Insight: Despite their strength, hardware-based methods are often impractical for everyday users due to the requirement of specialized hardware and high implementation costs. RansomShield addresses this limitation by offering a practical, software-based solution that integrates file, process, and ML-based detection without requiring additional hardware, making it more accessible to a wide range of users.

11.2. Comparison with Existing Literature

1. File Monitoring: GuardFS [1] supports the value of monitoring file changes. RansomShield builds on this by adding additional layers to address gaps.
2. Process Monitoring: Findings from MDPI (2024) [6] align with the inclusion of system call monitoring in RansomShield.
3. Machine Learning: ResearchSquare (2023) [4] emphasizes adaptive detection, which RansomShield integrates alongside monitoring.
4. Hardware Approaches: Studies like SHIELD [7] and Rapper [9] show the potential of hardware, but RansomShield provides accessibility without special hardware.

11.3. Gaps and Opportunities for Future Research

1. Unified Frameworks: Most existing studies address file and process detection individually. Future work should focus on testing integrated frameworks like RansomShield in real-world environments.
2. Real-Time Adaptability While ML models are promising, there is limited empirical testing of their performance against polymorphic ransomware in live systems. Further research is needed to refine adaptive detection.
3. Scalability: Studies have not fully explored how ransomware defenses can scale from individual desktops to enterprise networks. Expanding RansomShield for enterprise use is a key future direction.
4. Balancing Accuracy and Usability: Reducing false positives while maintaining usability remains a challenge. More work is needed to evaluate how user-friendly design can be balanced with strong detection capabilities.

12. Future Directions

The findings of this research highlight the need for further exploration of multi-layered ransomware defense systems and their application in real-world environments. Below are suggested areas for future research and key emerging trends that can guide the development of more effective ransomware protection frameworks.

12.1. Suggestions for Further Research

1. Advanced Behavioral Analysis
a. Research Focus: Future research should develop more sophisticated models that analyze not just files and processes but also user interaction patterns and system resource anomalies.
b. Expected Outcome: Early detection of stealthy ransomware that mimics normal system behavior.
2. Cross-Layer Correlation Studies
a. Research Focus: Explore methods that combine signals from multiple layers (file, process, and network activity) to reduce false positives.
b. Expected Outcome: More accurate detection results with fewer interruptions to normal system activity.
3. Automated Response Mechanisms
a. Research Focus: Investigate automated containment strategies, such as freezing suspicious processes or isolating affected files before full encryption occurs.
b. Expected Outcome: Faster mitigation that minimizes human intervention and data loss.
4. Usability and Human Factors
a. Research Focus: Study the balance between technical detection and user experience, including how alerts are delivered and how users respond.
b. Expected Outcome: Security tools that are not only effective but also easy to use, reducing the risk of users ignoring or disabling them.
a. Research Focus: Given the increasing use of multiple devices and platforms, future studies should investigate the development of cross-platform security frameworks that provide consistent protection across Android, iOS, and other operating systems.
b. Expected Outcome: A unified security framework that ensures seamless protection for users across all their devices and platforms.

12.2. Emerging Trends in the Field

1. Deception Technologies
a. Trend: Honeypots and decoy files are being deployed to lure ransomware and trigger alarms before real data is affected.
b. Implications: This proactive trickery can reduce damage by diverting ransomware away from critical assets.
2. Collaborative Threat Intelligence
a. Trend: Sharing ransomware signatures, behavioral patterns, and detection models across organizations and governments.
b. Implications: Collective intelligence improves the speed and accuracy of identifying new ransomware families.
3. Cloud-Native Security Tools
a. Trend: As more workloads move to the cloud, detection systems are being built directly into cloud platforms.
b. Implications: This ensures ransomware detection and response extends beyond desktops to virtualized and hybrid environments.
4. Continuous Learning Systems
a. Trend: Security tools are moving towards self-improving models that learn from every new attack attempt.
b. Implications: This dynamic learning enhances resilience against zero-day and polymorphic ransomware.
5. Integration with Backup and Recovery
a. Trend: Security frameworks are increasingly tied with automated backup and recovery systems to restore files immediately after an attack.
b. Implications: Even if ransomware bypasses detection, damage can be minimized through rapid restoration.

13. Conclusion

This research examined the growing challenge of ransomware and proposed RansomShield as a multi-layered defense mechanism to enhance ransomware detection and data protection. Traditional defenses, primarily signature-based detection, remain reactive and ineffective against evolving ransomware variants. By integrating file system monitoring, process analysis, and machine learning, RansomShield provides a proactive and unified approach to identifying ransomware before encryption begins.

The literature review highlighted existing solutions such as GuardFS, SHIELD, and machine learning-based methods, each offering valuable insights but often limited to a single detection layer. RansomShield addresses these limitations by combining multiple methods into one coherent framework, improving usability and effectiveness.

In conclusion, this paper contributes to the academic and practical understanding of ransomware defense by demonstrating the potential of layered detection. As ransomware attacks continue to evolve, future research should focus on scaling such frameworks, refining adaptive detection models, and ensuring regulatory compliance. Robust, user-friendly, and adaptive systems like RansomShield will be vital in safeguarding data and maintaining trust in an increasingly interconnected digital landscape.

14. References

[1]. GuardFS: A File System for Integrated Detection and Mitigation of Linux-based Ransomware (2024) https://www.sciencedirect.com/science/article/pii/S2214212625001152
[2]. Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection (2016) https://arxiv.org/abs/1609.03020
[3]. Cryptographic Ransomware Encryption Detection: Survey (2023) https://www.sciencedirect.com/science/article/pii/S0167404823002596
[4]. Classification of Ransomware Variants Through Adaptive Pattern Recognition in Real-Time Environments (2023) https://www.researchsquare.com/article/rs-5398213/v1

[5]. Ransomware Detection Based on File Entropy Analysis Using Machine Learning (2019) https://www.mdpi.com/2624-831X/1/2/30

[6]. Real-time system call-based ransomware detection (2024) https://www.mdpi.com/2624-831X/1/2/30

[7]. SHIELD: Secure Host-Independent Extensible Logging for Tamper-Proof Detection and Real-Time Mitigation of Ransomware Threats https://dl.acm.org/doi/abs/10.1145/3658644.3690269

[8]. Cryptographic Ransomware Encryption Detection: Survey (2023) https://www.sciencedirect.com/science/article/pii/S0167404823002596

[9]. Rapper: Ransomware Prevention via Performance Counters (2018) https://arxiv.org/abs/2004.01712

[10]. Digital DNA Sequencing Engine for Ransomware Detection Using ML (2020) https://ieeexplore.ieee.org/abstract/document/9121260

[11]. The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions https://ieeexplore.ieee.org/abstract/document/10105244