Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 02 | Feb-2026
ISSN (O) 3107-6696

A Survey on Dynamic Ransomware Simulation and Detection System for Endpoint Security

[1]Devi priya T, [2]Nagarani M

[1]Student, Department of Computer Science with Cybersecurity, Dr. N.G.P Arts and Science College, Coimbatore, devipriyavns54@gmail.com

2Professor, Department of Computer Science with Cybersecurity, Dr. N.G.P Arts and Science College, Coimbatore, nagarani.m@drngpasc.ac.in

---

Abstract - Ransomware attacks have become one of the most serious threats to endpoint devices such as personal computers and laptops. These attacks encrypt important user files and demand a ransom for recovery, causing financial loss and data unavailability. Traditional antivirus solutions mainly rely on signature-based detection, which often fails to identify new or unknown ransomware variants. To overcome this limitation, this project proposes a Dynamic Ransomware Simulation and Detection System for Endpoint Security that monitors real-time system behavior such as file access, file modifications, and suspicious process activities. A controlled ransomware simulation is used to analyze attack patterns safely and improve detection accuracy. When malicious behavior is detected,the system generates alerts and can take preventive actions to minimize file damage, thereby enhancing endpoint security against modern ransomware attacks.

Keywords: Ransomware,endpoint security, dynamic analysis, behavior-based detection, ransomware simulation, real-time monitoring, file system monitoring, malware detection, cybersecurity,intrusion detection.

1. INTRODUCTION

Ransomware attacks are increasing rapidly as technology becomes more integrated into everyday life making endpoint devices an easy target for cybercriminals. Users often store valuable documents,images,and sensitive information on their computers, which makes these devices highly attractive to attackers. Ransomware silently enters systems through phishing emails, unsafe downloads or infected websites and begins spreading before the user in even aware of the attack. Once activated, it disrupt normal system operations and limits access to data, creating stress and uncertainty for users.Existing security solutions mainly focus on identifying malware after it is already known, leaving systems exposed to newly created or cleverly cleverly modified ransomware. This growing gap between attackers and traditional defense methods highlight the need for smarter security approaches. A dynamic ransomware detection system that observes real time activities and system behavior offers a more reliable way to identify threats early.by focusing on how a system behaves rather than what a program looks like, endpoint security can be strengthened to respond effectively to modern ransomware challenges.

2. LITERATURE SURVEY

Ransomware attacks have increased significantly with the widespread use of endpoint devices, making them prime targets for cybercriminals Kharraz et al.analyzed the internal behavior of ransomware and highlighted that such attacks often infiltrate systems silently through phishing emails, malicious downloads, and compromised websites, remaining undetected until damage occurs[1].Scaife at al.emphasized that traditional signature based antivirus solutions are ineffective against modern ransomware variants due to techniques such as encryption, obfuscation and polymorphism which allow malware to evade detection[2].further studies by Scaife and Traynor demonstrated that ransomware typically causes abnormal system behavior, including rapid file modifications and high resource consumption, suggesting that behavior based monitoring is more effective for early detection[3].

Industry research by Symantec also supports the need for dynamic detection techniques,stating that reliance on frequent signature updates limits protection against newly emerging threats[4].Additional research by Demontis et al.explored machine learning based detection models,which leverage both static and dynamic feature of software to identify malicious behavior,showing improved accuracy against unknown ransomware variants[5].Liao et al.proposed real time file monitoring systems that tract abnormal read/write operations and process activities,demonstrating that continuous monitoring can significantly reduce the to detect ransomware attacks[6].patel et al.highlighted the importance of heuristic rules combined with system level metrics,emphasizing that adaptive behavior based techniques can provide proactive protection while minimizing false positives[7].collectively,these studies underscore the shift from

reactive,signature based approaches toward dynamic,behavior driven detection strategies,which are essential for strengthening endpoint security in modern computing environments.

Literature Survey on Ransomware Detection Techniques

S.No	Author & Year	Title of the Paper / Work	Technique Used	Key Contribution / Findings	Limitation
1	A. Kharraz et al. (2015)	Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks	Behavioral Analysis	Studied ransomware attack behavior and infection life cycle	No real-time prevention mechanism
2	A. Scaife et al. (2016)	Cryptolock (and Drop It): Stopping Ransomware Attacks on User Data	Behavior-Based Detection	Highlighted limitations of signature-based antivirus and proposed behavioral detection	Focused mainly on file system level
3	N. Scaife & P. Traynor (2016)	Understanding the Impact of Ransomware on Endpoint Systems	Endpoint Behavior Monitoring	Analyzed ransomware impact on endpoints and system resources	Limited simulation environment
4	M. Continella et al. (2016)	ShieldFS: A Self-Healing Ransomware-Aware File System	Ransomware-Aware File System	Proposed self-healing mechanism for ransomware protection	File-system dependent solution
5	S. Cabaj et al. (2016)	SDN-Based Crypto Ransomware Detection	Network Behavior Analysis	Detected ransomware using traffic behavior patterns	Network-level focus only
6	Y. Zhang et al. (2019)	Behavior-Based Ransomware Detection on Endpoint Systems	Behavior-Based Monitoring	Improved detection of unknown ransomware variants	Threshold tuning required
7	Symantec Security Team (2018)	Internet Security Threat Report	Industry Analysis	Reported rise in ransomware via phishing and unsafe downloads	Commercial and survey-based data

3. BACKGROUND STUDY

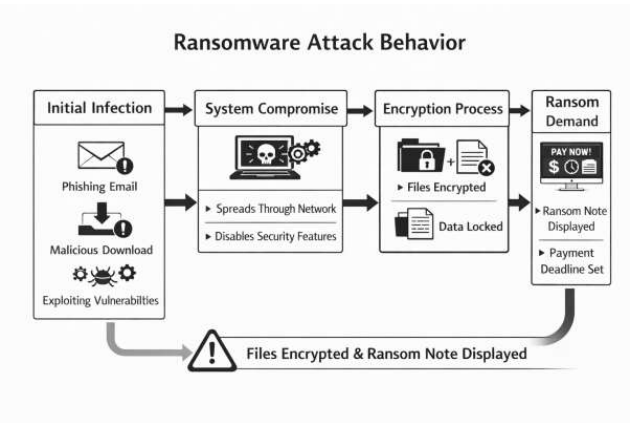
With the rapid growth of digital technology,endpoint devices such as personal computers and laptops have become essential for communication,education and business operations.these devices store large volumes of sensitive data,making them attentive targets for cyber attacker[1].ransomware a malicious form of malware that encrypt user files and demands ransom payments,has emerged as one of the most damaging cyber threats,leading to severe data loss and financial impact[2].traditional antivirus solutions rely heavily on signature based detection mechanisms,which are ineffective against newly developed or modified ransomware variants that employ encryption,obfuscation and polymorphism techniques[3].as a result,endpoint system remain vulnerable to zero-day ransomware attacks.To overcome these limitations,recent cybersecurity research has shifted toward dynamic and behavior based detection approaches[4].these methods focus on monitoring real time system activities such as file access behavior,process execution patterns,and abnormal encryption activity to detect ransomware at an early stages[5].controlled ransomware simulation environment are also widely used to safely analyze ransomware behavior and evaluate detection mechanism without deploying real malware[6].studies have shown that combining real time behavioral monitoring with simulation based testing significantly improves detection accuracy against both development of the proposed dynamic ransomware simulation and detection system for endpoint security.

4. SOFTWARE ATTACK BEHAVIOR

Ransomware attack behavior refers to the sequence of actions through which ransomware infiltrates an endpoint system, operates within it, and ultimately damages user data.In most cases, ransomware enters endpoint devices through phishing emails, malicious attachments, unsafe software downloads, or compromised websites, where users unknowingly activate the malware.Once executed, the ransomware installs itself silently and runs in the background, allowing it to evade early detection by traditional security solutions.After successful infiltration, ransomware scans the system to locate valuable files such as documents, images, videos, and database files.It mainly targets frequently accessed directories and connected storage drives to maximize the impact of the attack.

The ransomware then encrypts the identified files using strong cryptographic algorithms, making them inaccessible to the user.During the encryption process, ransomware may disable security services, terminate backup processes, or block system recovery mechanisms to prevent easy data restoration.In the final stage of the attack, ransomware displays a ransom note demanding payment in exchange for the decryption key.These ransom messages often use fear tactics, deadlines, and threats of permanent data loss to pressure victims into paying the ransom.Advanced ransomware variants may communicate with remote command-and-control servers, spread laterally across networks, or dynamically alter their behavior to evade detection.Understanding ransomware attack behavior is essential for developing effective detection and prevention mechanisms.

Behavior-based security solutions can identify ransomware activity at an early stage and significantly reduce potential damage to endpoint devices.



5. ENDPOINT SECURITY MECHANISM

Endpoint security refers to the methods and technologies used to protect endpoint devices such as personal computers, laptops, and mobile devices from cyber threats.These endpoint devices are common targets for malware and ransomware attacks because they store sensitive personal and organizational data and interact directly with users and external networks.Effective endpoint security is essential to prevent data breaches, financial losses, and disruption of system operations.Traditional endpoint security mechanisms mainly rely on antivirus and anti-malware software that use signature-based detection techniques.While signature-based methods are effective against known threats, they fail to detect newly developed or modified ransomware variants.To overcome this limitation, modern endpoint security systems adopt behavior-based monitoring approaches that analyze real-time system activities.These activities include file access patterns, process execution behavior, and abnormal system modifications that may indicate malicious intent.

Additional endpoint security mechanisms include firewalls and intrusion detection systems, which help monitor and control network traffic.Encryption techniques are used to protect sensitive data even if an endpoint device is compromised or stolen.Regular system updates and patch management reduce vulnerabilities that attackers could exploit.Backup and recovery solutions ensure that critical data can be restored in the event of a ransomware attack.By integrating multiple layers of security, endpoint protection mechanisms can effectively detect, prevent, and respond to ransomware threats.This layered approach significantly enhances the resilience of endpoint systems against evolving cyberattacks.

6. TRADITIONAL RANSOMWARE DETECTION TECHNIQUES

Traditional ransomware detection techniques are designed to identify malicious software using predefined patterns or signatures. These techniques are commonly implemented in conventional antivirus and anti-malware solutions. The primary principle behind traditional detection is to compare files and programs against a database of known malware signatures. If a match is found, the file or process is immediately classified as malicious and blocked. One widely used technique is signature-based detection, which relies on identifying unique byte patterns associated with known ransomware variants. Heuristic analysis is another method that examines suspicious code structures or behavior patterns to detect potentially malicious programs.

File scanning techniques monitor files for unusual changes, such as sudden encryption or rapid modification of multiple files.Sandboxing, also known as static analysis, executes programs in a controlled environment to observe their behavior without affecting the actual system.Although these traditional techniques are effective against previously identified ransomware, they have significant limitations. Modern ransomware often uses encryption, obfuscation, polymorphism, and fileless execution techniques to evade signature-based detection.As a result, traditional detection methods struggle to identify zero-day and newly evolved ransomware attacks. These limitations have led to the development of dynamic and behavior-based ransomware detection approaches that provide improved protection against modern threats.

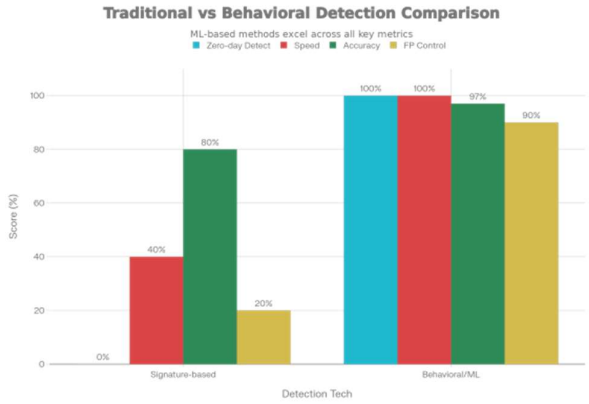


Fig 2:Comparison of signature-based (traditional) vs behavioral detection for ransomware

7. DYNAMIC RANSOMWARE DETECTION APPROACH

Dynamic ransomware detection is an advanced security approach that identifies ransomware based on its behavior rather than relying on predefined signatures. Unlike traditional detection methods, this approach continuously monitors real-time activities occurring on endpoint devices. These activities include file access operations, file modifications, process creation, and abnormal system behavior. By observing how applications behave during execution, dynamic detection systems can identify both known and unknown ransomware variants.

One of the key features of this approach is real-time monitoring, which allows early detection of suspicious activities before extensive damage occurs.Behavioral analysis

is used to recognize abnormal actions such as rapid encryption of multiple files or unauthorized changes to system directories.

When malicious behavior is detected, the system generates alerts and can automatically block or terminate the suspicious process.This immediate response helps prevent ransomware from spreading and reduces potential data loss. Dynamic ransomware detection is particularly effective against modern ransomware techniques such as polymorphism, code obfuscation, and fileless execution. By focusing on behavioural patterns instead of static signatures, this approach significantly improves endpoint security.

Overall, dynamic ransomware detection provides a proactive and reliable solution for protecting systems against evolving ransomware threats.

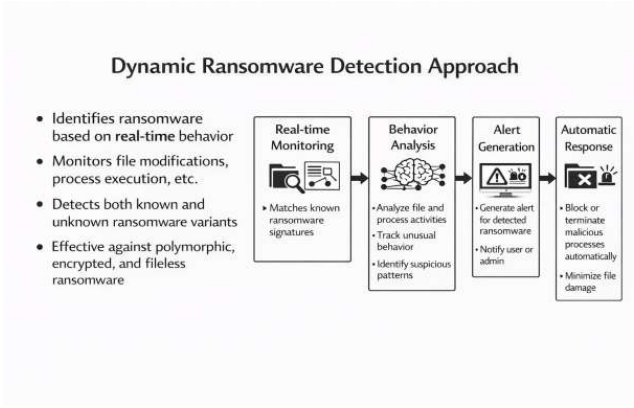


Fig 3:Dynamic Ransomware Detection Approach

8. RANSOMWARE SIMULATION ENVIRONMENT

A ransomware simulation environment is a controlled, isolated, and secure framework designed to safely replicate ransomware attacks without causing harm to real systems or data. This environment allows security researchers and detection systems

to closely observe ransomware behavior, including infection methods, file discovery processes, encryption techniques, privilege escalation attempts, and interactions with system resources. Typically implemented using Sandboxing or virtual machine–based setups, the simulation environment ensures complete isolation from production systems while maintaining realistic execution conditions. Advanced monitoring components continuously track file system activities, process creation and termination, CPU and memory usage, registry changes, and network communications to identify abnormal patterns associated with ransomware. The environment enables repeated and controlled experiments, making it possible to analyze both known and unknown ransomware variants and evaluate the effectiveness of dynamic detection algorithms. By simulating real-world attack scenarios, the system helps refine behavioral rules, improve detection accuracy, and reduce false positives. Furthermore, ransomware simulation supports proactive security testing by allowing early identification of weaknesses in detection mechanisms.Overall, the ransomware simulation environment plays a critical role in strengthening endpoint security by supporting the development, testing, and validation of advanced behavior-based ransomware detection and prevention systems.

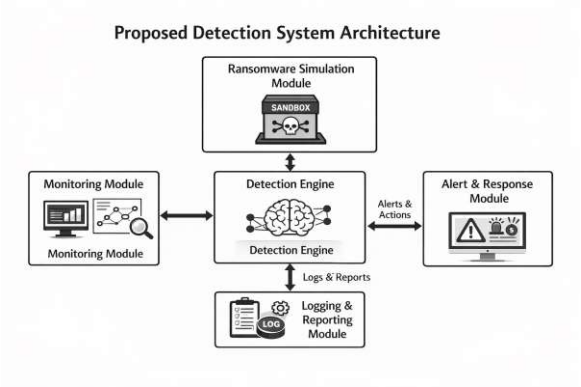


Fig.4:Proposed Detection System Architecture

9. CONCLUSION

Ransomware attacks have become one of the most serious threats to endpoint devices, causing data loss, financial damage, and disruption of normal system operations. Traditional signature-based ransomware detection techniques are no longer sufficient to defend against modern ransomware that uses advanced evasion techniques. This project presented a Dynamic Ransomware Simulation and Detection System for Endpoint Security that combines real-time behavior monitoring with a controlled ransomware simulation environment.By analysing file access patterns, process behavior, and abnormal system activities, the system is capable of detecting both known and unknown ransomware variants at an early stage. The use of ransomware simulation enables safe analysis of attack behaviour and improves the accuracy and reliability of detection mechanisms. When suspicious activity is detected, the system can generate alerts and take preventive actions to minimize file damage. Overall, the proposed approach enhances endpoint security by providing proactive, behaviour-based protection against evolving ransomware threats. This system demonstrates that dynamic detection methods offer a more effective and reliable solution for mitigating ransomware attacks in modern computing environments.

10. REFERENCES

[1] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda,
"Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks,"
in *Proceedings of the 12th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, Milan, Italy, 2015, pp. 3–24.

[2] A. Scaife, P. Traynor, and K. R. B. Butler,
"Cryptolock (and Drop It): Stopping Ransomware Attacks on User Data,"
in *Proceedings of the IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, Nara, Japan, 2016, pp. 303–312.

[3] N. Scaife, K. R. B. Butler, and P. Traynor,
"Understanding the Impact of Ransomware on Endpoint Systems,"
IEEE Security & Privacy, vol. 14, no. 5, pp. 48–56, Sept.–Oct. 2016.

[4] Symantec Security Response,
"Ransomware: Evolution, Trends, and Prevention Techniques,"
Symantec Corporation, White Paper, 2017.

[5] Y. Zhang, Q. Li, and Y. Guo,
"Behaviour-Based Ransomware Detection on Endpoint Systems,"
in *Proceedings of the IEEE TrustCom*, 2019.

[6] R. Sommer and V. Paxson,
"Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,"
in *Proceedings of the IEEE Symposium on Security and Privacy*, 2010.

[7] Symantec Security Response,
"Internet Security Threat Report,"
Symantec Corporation, 2018.