Cureus Journal of Computer Science

Open Access Original Article

Enhancing Ransomware Protection Through Moving Target Defense Technique

Sanika S. Shinde [1] , Snehal Ghoparkar [1] , Rashmi K. Patil [1] , Sanika B. Patil [1]

[1]. Computer Engineering, Pillai HOC College of Engineering and Technology, Rasayani, IND

Corresponding author: Sanika S. Shinde, shinde.sanika02@gmail.com

Received 03/04/2025
Review began 03/10/2025
Review ended 04/24/2025
Published 04/28/2025

DOI: https://doi.org/10.7759/s44389-025-03546-z

Abstract

Ransomware is a major cybersecurity threat that locks systems or encrypts files, demanding ransom for decryption or access. Evolving, statically defined defenses are incapable of dealing with modern ransomware techniques, making advanced detection systems imperative. This research proposes a hybrid technique that combines moving target defense (MTD) with both static and dynamic system analysis to improve system and network security. Under MTD, blockades to system exploitation are achieved through randomization, diversification, and continuous system optimization, which dynamically manipulate the system's attack surface. Changes in behavioral analysis and real-time modifications enhance the accuracy of detection, reduce the identification of incorrect targets, and minimize operational interruptions during system functionality. Ransomware is disseminated through phishing emails, other malicious downloads, or exploits within software. The two most commonly encountered types of ransomware are para-cryptor ransomware, which encrypts files, and locker ransomware, which denies access to the entire system. Modern ransomware can change its shape using polymorphic and metamorphic techniques to avoid detection, making signature-based defenses insufficient. To mitigate these threats, this research integrates static and heuristic analysis with dynamic behavior observation, thereby increasing adaptability for identifying ransomware activities. Cuckoo Sandbox, an automated malware analysis tool, forms the foundation of this approach.

Categories: Network Security, Software Security, Machine Learning (ML)
Keywords: cuckoo sandbox, moving target defense ransomware, behavioral analysis, attack surface randomization, threat mitigation, static analysis, dynamic analysis

Introduction

Cybersecurity [1] is more or less keeping the systems, networks, and programs secure from destructive digital attacks. These attacks could access sensitive information, change it, or delete it, mess with operations, or even extort money. Important areas to concentrate on include network security, application security, information security [2], operational security, disaster recovery, and user education on safety. All of this keeps our data safe and our systems running, but there are a few pretty tough challenges: changing threats, not enough resources, and clever attackers can really create some big problems. Ransomware [3-4] is the biggest threat. It is a type of malicious software that locks up someone's data and asks for money, usually in cryptocurrency, to unlock it. Ransomware was noticed as a spread that had its entry point in the form of phishing emails, unsafe websites, or an exploited weak spot of any system. Further types include crypto [5] ransomware, locker ransomware, double extortion ransomware, and ransomware-as-a-service. These demonstrate major cases and have left enormous footprints when companies' monetary loss was measured to have created immense problems through massive operational hindrance, affecting reputations too. The key measures in countering such risks are data backups on a regular basis, employee training, endpoint security, managing updates, and controlling access. The constant growth of both frequency and sophistication in ransomware attacks makes strong cybersecurity practices very necessary. Such cybersecurity practice has to stay one step ahead of emerging threats by engaging the triad of government, organization, and individual together for protecting critical systems and sensitive data.

How to cite this article
Shinde S S, Ghoparkar S, Patil R K, et al. (April 28, 2025) Enhancing Ransomware Protection Through Moving Target Defense Technique . Cureus J Comput Sci 2 : es44389-025-03546-z. DOI https://doi.org/10.7759/s44389-025-03546-z

FIGURE 1: Ransomware Attack

Figure 1 illustrates ransomware attack. The graphic captures the essential components of a ransomware attack such as file encryption, ransom extraction, and cybersecurity responses. It underscores the notion of moving target defense (MTD) as one means to mitigate the attack by illustrating how changes in the system can interfere with the execution and recruitment processes of the ransomware.

Ransomware has grown to be one of the most widespread and damaging cybersecurity threats, with the ability to encrypt sensitive data and require ransom payments to regain access. As the variants of ransomware become more sophisticated, such as polymorphic, metamorphic, and file less methods, conventional [6] security controls like signature-based detection, static analysis, and heuristic-based mechanisms are no longer proving effective. Threat agents are constantly advancing their attack processes to evade established defense mechanisms by utilizing sophisticated evasive techniques such as process hollowing, code obfuscation, and sandbox detection. Inability of standard security architectures to dynamically evolve towards countering such dynamic threats places emphasis on emerging and proactive methods of defense. MTD is an insurgent practice nowadays in the domain of cybersecurity that countermands the deficiency of fixed defenses via incessant revision of system settings, assault surfaces, and network landscapes. MTD finds its power rooted in the dogma of uncertainty, for making it cumbersome and costly to commit successful assaults by the invaders. Through dynamic modification of parameters such as memory allocation, file system structure, application programming interface calls, and network routing tables, MTD disrupts execution patterns of ransomware, preventing malware from attaining persistence or having the potential to encrypt data. MTD's randomness imposes additional layers of protection [7], lessening the efficiency of the attack while making the system more resistant simultaneously. This paper describes an MTD-informed ransomware prevention and detection system integrating dynamic system adaptation, runtime behavior monitoring, and deception-based countermeasures. The system uses layered defenses like attack surface randomization [8], process relocation, system polymorphism, and decoy-based honeypots to identify and disable ransomware before it can cause harm. Together with AI-powered anomaly detection and adversarial analysis, the approach supports improved real-time threat detection and response. The intended strategy is deeply analyzed across different families of ransomware in order to get a better grasp of its effectiveness in preventing encryption attempts, process injection, and stealth-based dissemination. Comparative assessment against the present detection strategies directs towards the capability of MTD in increasing cyber resilience and the diminishment of ransomware attacks. With the incorporation of this principles with advanced threat intelligence and live monitoring, the new framework will transform ransomware defense strategy with a robust and adaptive response to modern cyber attacks.

Materials And Methods

The system is based on combining MTD [9] strategies and building holistic frameworks for ransomware detection and prevention. It employs changing of certain system parameters, for example, shifting of IP addresses, changing of file trees, or alterations in system configurations in order to create uncertainty for the potential ransomware attackers. In the case where ransomware-like activity is detected, the system employs lockdown of network [10] elements that contain the ransomware. To further fortify these features of automated machine response, the system applies normal working protocols for protecting data, employing other proactive defense mechanisms such as passive deception with honey files [11] boarding up sensitive files to be used as bait for some attackers. Within the implementations, the random forest algorithm is employed because it can accurately identify and classify ransomware based on a feature set. Random forest is a supervised machine learning algorithm, which means that it builds a multitude of decision trees at training and merges their predictions at the end to provide stronger estimates. In this case, there are features such as file access patterns, rates of encryption, system calls, and changes in file structure that are present in the scanned files and are extracted. The algorithm employs these features to recognize behavior that is typically associated with ransomware. The algorithm is trained on labeled datasets where normal files and files with various forms of ransomware are present to enhance its ability to classify unseen data. Random forests make predictions using the average output of many decision trees, which reduces the risk of overfitting as well as boosts detection accuracy. With these abilities, the systems will be able to greatly distinguish between malicious and normal behavior, which is crucial in this stage of the detection and classification in the prevention framework of the ransomware.

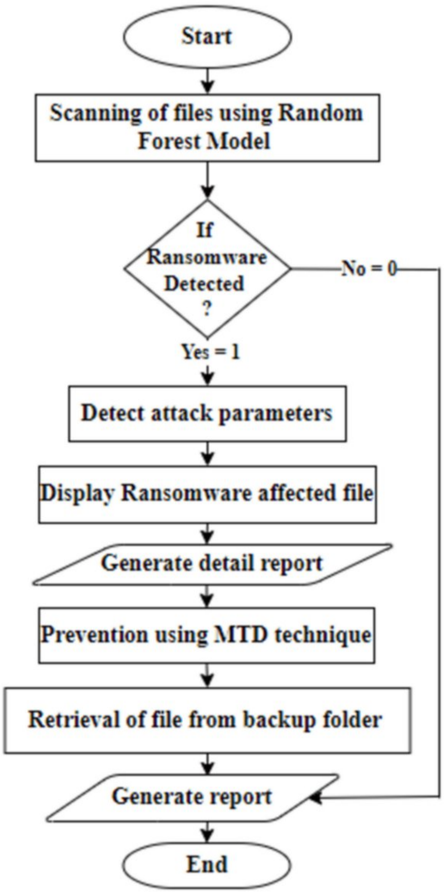

Start
Scanning of files using Random Forest Model
If Ransomware Detected ?
No = 0
Yes = 1
Detect attack parameters
Display Ransomware affected file
Generate detail report
Prevention using MTD technique
Retrieval of file from backup folder
Generate report
End

FIGURE 2: Ransomware Detection and Prevention Framework

MTD, Moving Target Defense

Figure 2 illustrates methodology of ransomware detection and prevention. The steps are as follows:

1. Start: This marks the beginning of the ransomware detection and prevention process. It initiates the system's monitoring and scanning functionality.

2. Scanning of Files Using Random Forest Model: In this step, files are scanned using a random forest

machine learning model. The model is trained to analyze file features and behavior to detect suspicious patterns indicative of ransomware. Random forest is chosen for its robustness in handling large datasets and its ability to make accurate predictions by averaging the results of multiple decision trees.

3. Is Ransomware Detected? (Decision Point): This is a decision point in the process flow. The model determines whether ransomware is present in the scanned files.

If No (0) ransomware is detected, the process ends, meaning no action is needed.

If Yes (1) ransomware is detected, the process proceeds to the next steps aimed at mitigating the threat.

4. Detect Attack Parameters: Once ransomware is detected, the system identifies and extracts important parameters related to the attack. These could include the type of ransomware, the encryption method being used, the affected files, and any other critical information about the attack.

5. Display Ransomware Affected File: The system displays the files that have been affected by the ransomware. This helps the user or administrator understand which files are compromised or at risk and enables them to take further action.

6. Generate Detail Report: A detailed report is generated, logging important information about the detected ransomware attack. This report includes specifics such as the nature of the attack, affected files, and potential methods of recovery or prevention applied. It can be used for forensic analysis or further investigation.

7. Prevention Using MTD Technique: Moving Target Defense (MTD) techniques are applied to prevent ransomware from further encrypting files or spreading to other parts of the system. MTD works by dynamically altering the system's attack surface, making it difficult for the ransomware to proceed with its intended actions.

8. Retrieval of File From Backup Folder: In this step, the system retrieves any files that have been compromised by the ransomware from a secure backup. This ensures that the affected files can be restored, mitigating the damage caused by the attack.

9. Generate Report: A final report is generated, summarizing the entire ransomware detection and prevention process. This report will include details of the detected ransomware, the preventive actions taken, and the files recovered from the backup.

10. End: This marks the completion of the ransomware detection and prevention cycle. The system either successfully prevents the ransomware attack or continues monitoring if no threat is detected.

The software and hardware requirements for ransomware detection and prevention [12] via MTD include both software and hardware components. The software requirements include Visual Studio Code as the primary development environment, Python 3.11.0, and the Python Interpreter to execute scripts and deploy machine learning models [13]. Python libraries are also utilized during data preprocessing, feature extraction, classification, and system automation. The hardware requirement includes a 64-bit operating system that incorporates an x64-based processor, i.e., an AMD Ryzen 5 5500U with Radeon Graphics (2.10 GHz). The setup provides the necessary computational power to execute ransomware detection software, simulations, and dynamic system settings. In addition, the system needs ample RAM and disk space to run malware analysis software, like Cuckoo Sandbox, that observes file activities and backup storage space for restoring clean file copies during an attack. The process includes four primary phases: file scanning and data harvesting, detection and categorization, prevention, and report generation. File scanning phase continuously keeps an eye on files and system activity to identify suspicious [14] activity such as unauthorized encryption, file alteration, or unusual access patterns. Data extraction is the subsequent step where files are classified as infected or benign depending upon their activity and primary characteristics such as frequency of access of files, encryption patterns, and network communication patterns are determined. In the detection and classification phase, machine learning models, in this case, random forest [15] classifiers, are employed to detect ransomware from normal files. Malware [16] detection techniques continue to evolve as attackers develop more sophisticated evasion methods. Feature selection algorithms are utilized to narrow down this process through the detection of the most discriminatory features for effective classification. MTD methods are deployed at the prevention phase, and these continuously alter the system attack surface such that it becomes difficult for ransomware to attack files. Methods such as file location randomization, honeypots, decoys, and permission changes for accessing files are employed to mislead attackers. In case of ransomware detection, the system initiates automatic recovery of files from secure backup folders to prevent harm. Finally, the reporting stage produces a comprehensive report of threats detected, preventive measures taken, and system reactions, providing useful information for enhancing cybersecurity and preventing threats in the future.

Results

To enhance ransomware detection, machine learning-based techniques, particularly hybrid models combining static and dynamic analysis, can be integrated into the DOLOS framework. High-performing models, such as random forest classifiers and support vector machines with dynamic behavioral analysis, excel at detecting both known and zero-day ransomware. Dynamic analysis in sandbox environments, paired with feature extraction (e.g., opcode frequency, entropy, system call patterns), ensures precision while mitigating evasion tactics like obfuscation. This hybrid approach forms a multi-layered defense: DOLOS disrupts and delays attackers with dynamic deception, while machine learning ensures accurate ransomware detection. Together, they provide a resilient system with rapid threat identification, reduced time-to-compromise, and effective ransomware mitigation in evolving threat landscapes.

Hardware components

1. The system operates on a 64-bit operating system with an x64-based processor.

2. A recommended processor is AMD Ryzen 5 5500U with Radeon Graphics (2.10 GHz), which provides sufficient computational power for executing ransomware detection algorithms, running simulations, and dynamically adjusting system settings.

3. The system also requires ample RAM and disk space for running malware analysis software such as Cuckoo Sandbox, which observes file behavior. Additionally, backup storage space is needed for restoring clean copies of files in case of an attack.

Comparison of the proposed system with existing system

Table *1* illustrates the comparison of existing and proposed systems.

Features	Existing System	Proposed System
Detection	ML-based (static and dynamic)	MTD with ML
Data Analysis	Static and dynamic	Integrated approach
Resilience	Limited against evasion	Randomization-based security
Accuracy	97.4% -99.1%	95% (known), 91% (zero- day)
Real-Time Protection	Post-attack recovery	Prevents encryption
File Recovery	Uses backups	Instant recovery
Performance	Moderate to high overhead	Optimize for efficient

TABLE 1: Comparison of Existing and Proposed System

ML, Machine Learning; MTD, Moving Target Defense

Experimental setup

Figure *3* illustrates user interface for a system. It features "Start Detection", "Start Prevention", and "Generate Report" buttons, indicating the software is designed to initiate ransomware detection and prevention process.

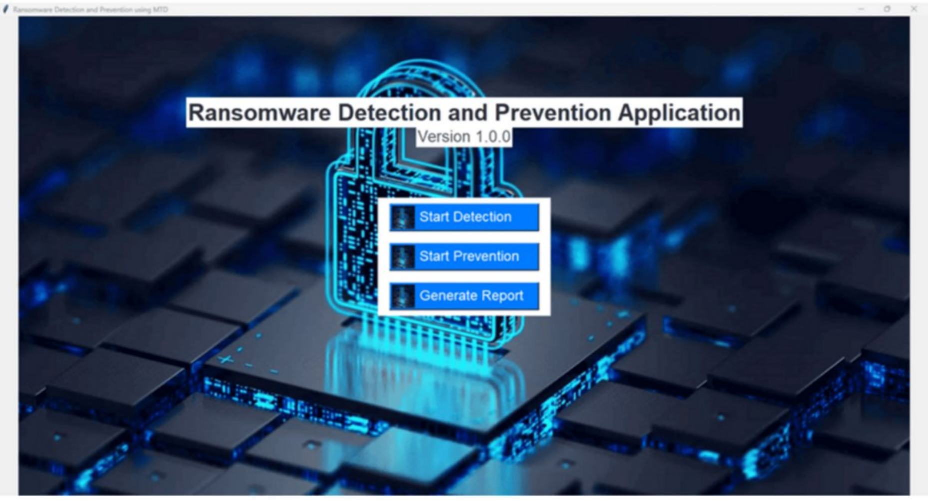
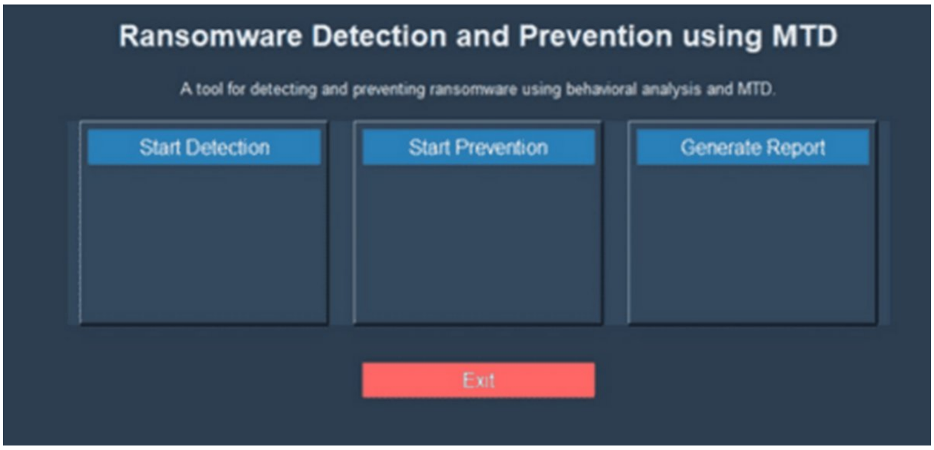

Ransomware Detection and Prevention using MTD
Ransomware Detection and Prevention Application
Version 1.0.0
Start Detection
Start Prevention
Generate Report

FIGURE 3: User Interface

Figure 4 illustrates a software interface featuring buttons: "Start Detection" for initiating ransomware scans. "Exit" to close the application. "Start Prevention" for initiating ransomware prevention. "Generate Report" for generating overall report of scanning.

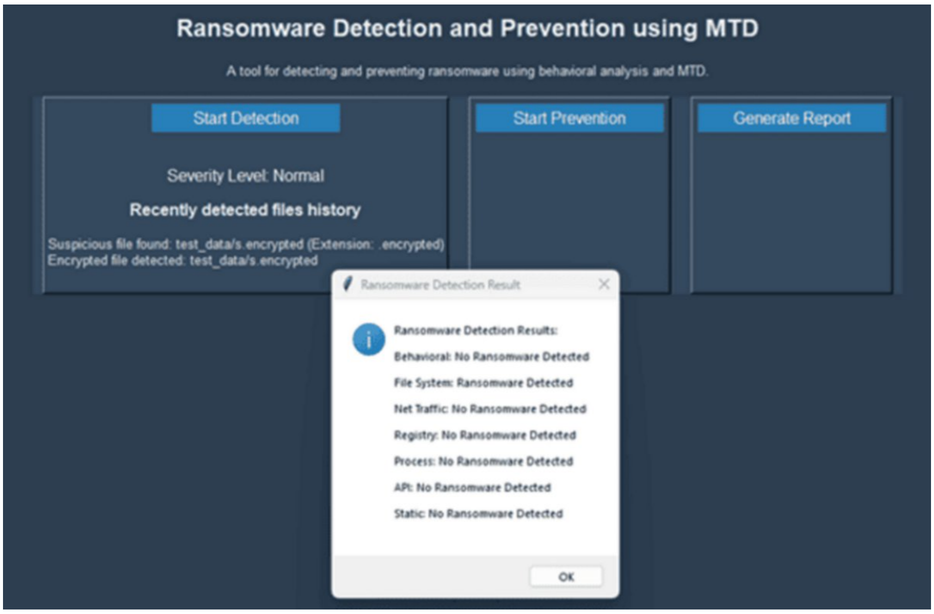


A tool for detecting and preventing ransomware using behavioral analysis and MTD.

FIGURE 4: Detection Window

MTD, Moving Target Defense

Figure 5 illustrates a pop-up window, indicating the detection results across various system parameters, showing the ransomware result.


Ransomware Detection and Prevention using MTD
A tool for detecting and preventing ransomware using behavioral analysis and MTD.
Start Detection
Start Prevention
Generate Report
Ransomware Detection Result
OK

Severity Level: Normal

Recently detected files history

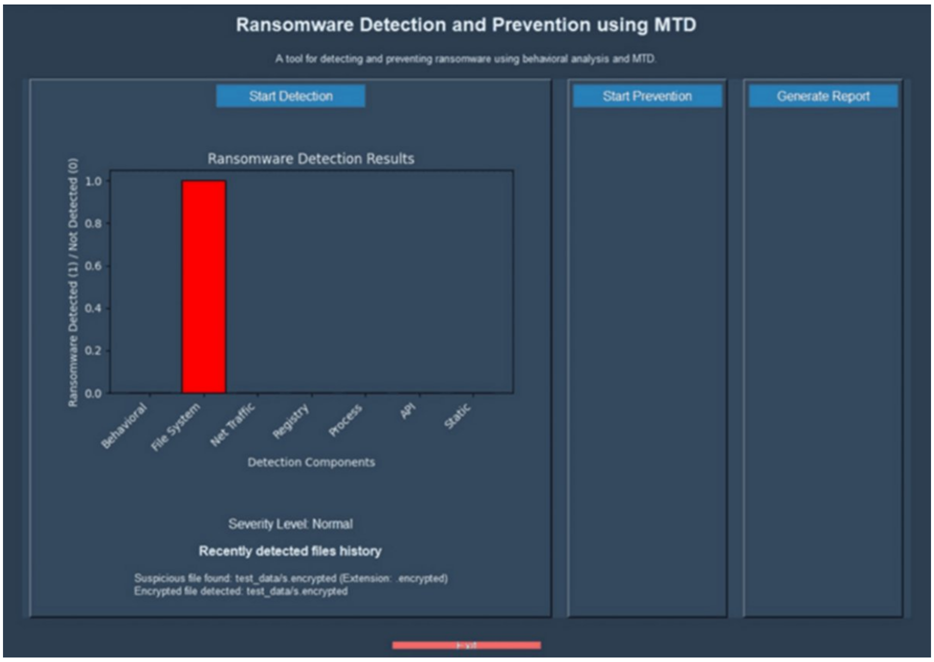
Suspicious file found: test_data/s.encrypted (Extension: .encrypted)
Encrypted file detected: test_data/s.encrypted

Ransomware Detection Results:
Behavioral: No Ransomware Detected
File System: Ransomware Detected
Net Traffic: No Ransomware Detected
Registry: No Ransomware Detected
Process: No Ransomware Detected
API: No Ransomware Detected
Static: No Ransomware Detected

FIGURE 5: Detection Pop-up

MTD, Moving Target Defense

Figure 6 illustrates the graphical results, showing that ransomware has been detected in the file system component.


Ransomware Detection and Prevention using MTD
A tool for detecting and preventing ransomware using behavioral analysis and MTD.
Start Detection
Start Prevention
Generate Report
Ransomware Detection Results
Ransomware Detected (1) / Not Detected (0)
1.0
0.8
0.6
0.4
0.2
0.0
Behavioral
File System
Net Traffic
Registry
Process
API
Static
Detection Components

Severity Level: Normal

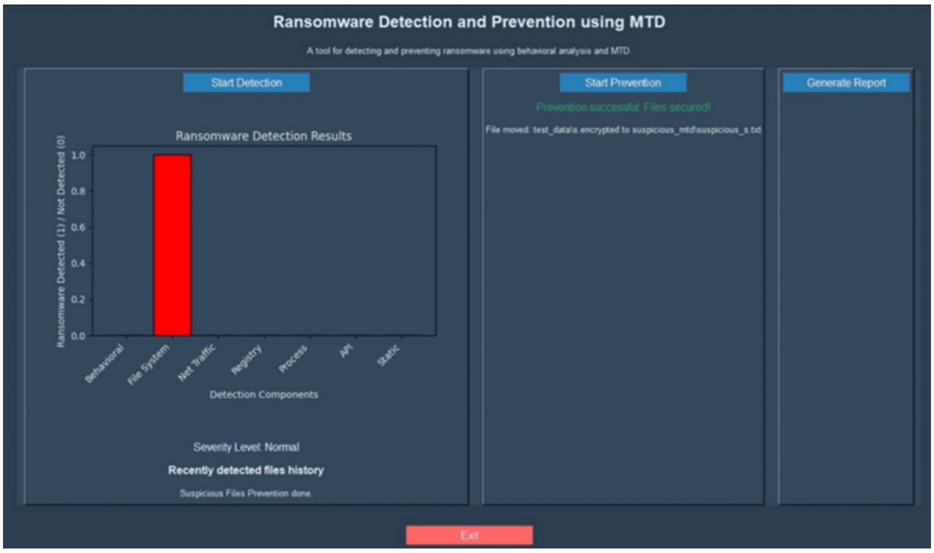
Recently detected files history

Suspicious file found: test_data/s.encrypted (Extension: .encrypted)
Encrypted file detected: test_data/s.encrypted

FIGURE 6: Graphical Representation

MTD, Moving Target Defense

Figure 7 illustrates the successful prevention of ransomware.


Ransomware Detection and Prevention using MTD
A tool for detecting and preventing ransomware using behavioral analysis and MTD.
Start Detection
Start Prevention
Generate Report
Ransomware Detection Results
Ransomware Detected (1) / Not Detected (0)
1.0
0.8
0.6
0.4
0.2
0.0
Behavioral
File System
Net Traffic
Registry
Process
API
Static
Detection Components
Exit

Prevention successful: Files secured!

File moved: test_data\s.encrypted to suspicious_mtd\suspicious_s.txt

Severity Level: Normal

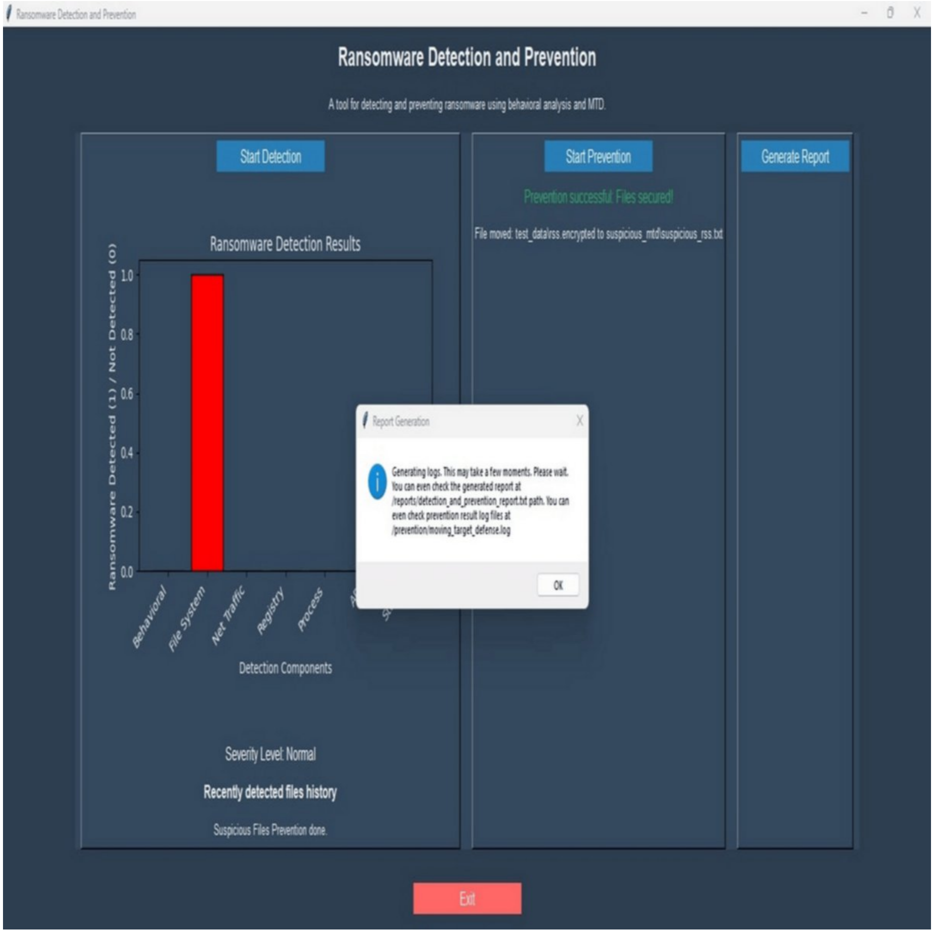
Recently detected files history

Suspicious Files Prevention done.

FIGURE 7: Prevention of Ransomware

MTD, Moving Target Defense

Figure 8 illustrates the pop-up of generating logs.


Ransomware Detection and Prevention
Ransomware Detection and Prevention
A tool for detecting and preventing ransomware using behavioral analysis and MTD.
Start Detection
Start Prevention
Generate Report
Ransomware Detection Results
Ransomware Detected (1) / Not Detected (0)
1.0
0.8
0.6
0.4
0.2
0.0
Behavioral
File System
Net Traffic
Registry
Process
Detection Components
Report Generation
OK
Exit

Prevention successful: Files secured!

File moved: test_data\rss.encrypted to suspicious_mtd\suspicious_rss.txt

Generating logs. This may take a few moments. Please wait. You can even check the generated report at /reports/detection_and_prevention_report.txt path. You can even check prevention result log files at /prevention/moving_target_defense.log

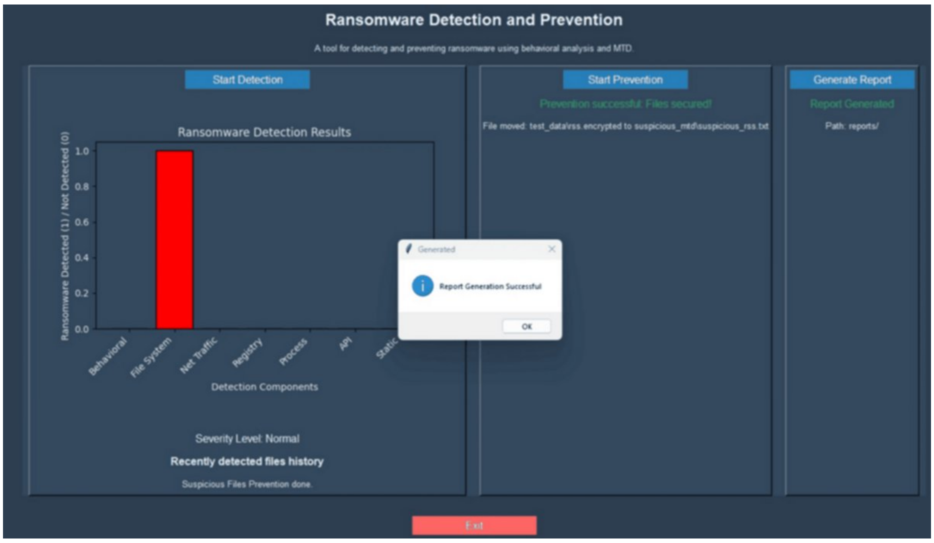
Severity Level: Normal

Recently detected files history

Suspicious Files Prevention done.

FIGURE 8: Pop-up of Generating Logs

Figure 9 illustrates the successful generation of report.



Ransomware Detection and Prevention

A tool for detecting and preventing ransomware using behavioral analysis and MTD.

Prevention successful: Files secured!

File moved: test_data\rss.encrypted to suspicious_mtd\suspicious_rss.txt

Report Generated

Path: reports/

Report Generation Successful

Severity Level: Normal

Recently detected files history

Suspicious Files Prevention done.

FIGURE 9: Report Generation Successful

Performance metrics

Accuracy Graph

Figure 10 illustrates the detection accuracy across three scenarios: Known Ransomware, Zero-Day Ransomware, and Evolving Variants. The system achieved the highest accuracy (95%) for known ransomware and maintained.

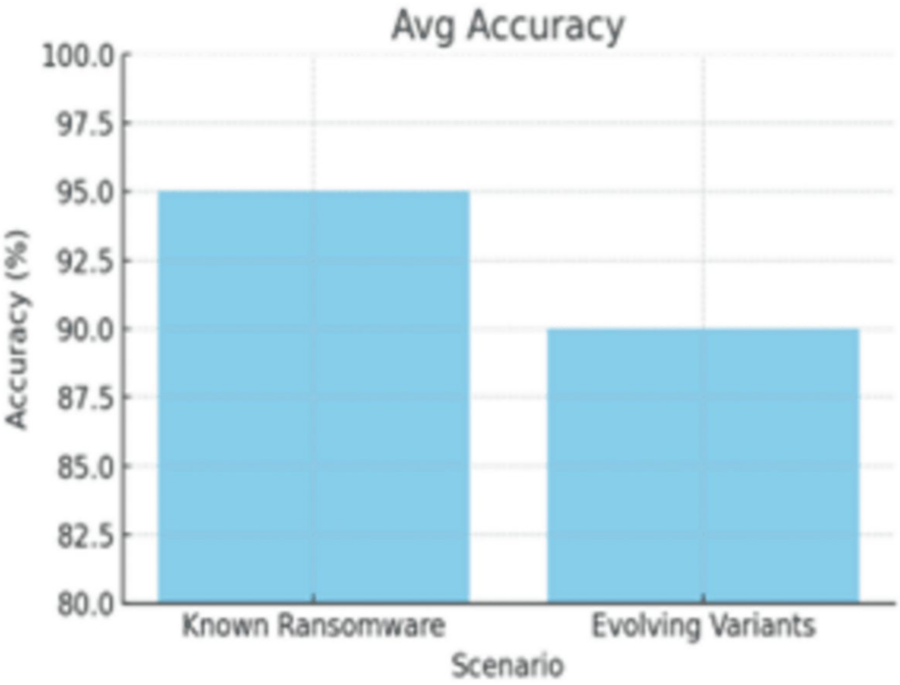


FIGURE 10: Average Accuracy of Detection for Known Ransomware and Evolving Variants

F1-Score Across Attack Scenarios

Figure 11 illustrates the F1-scores for detecting ransomware in different scenarios. The F1-score is highest (0.96) for known variants, slightly lower for zero-day attacks (0.91), and lowest for evolving variants (0.89), reflecting the challenges of detecting newer threats.

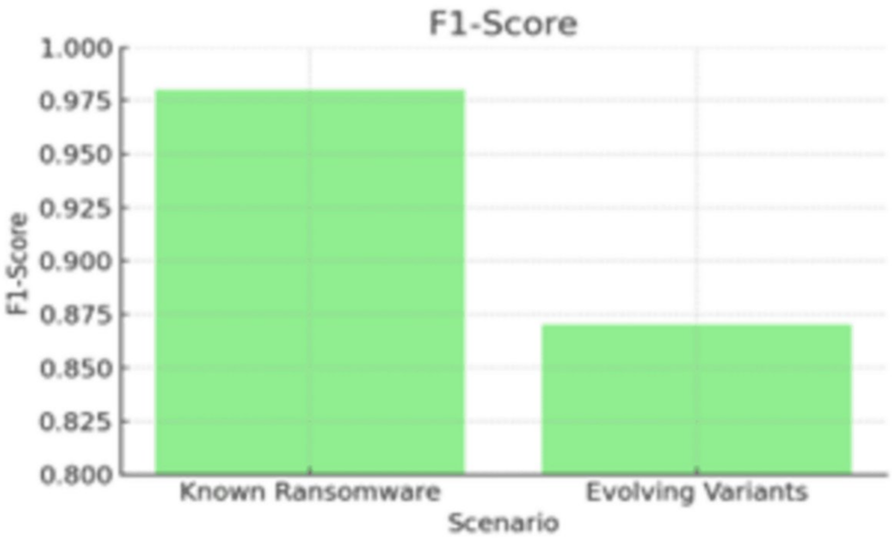


FIGURE 11: F1-Score for Detection of Known Ransomware and Evolving Variants

Line Graph

Figure 12 illustrates comparison of accuracy (blue line) and F1-score (red line) for Known Ransomware (95%, 0.98) and evolving variants (90%, 0.90), showing a drop in performance for evolving threats. It highlights the challenge of detecting newer ransomware variants effectively.

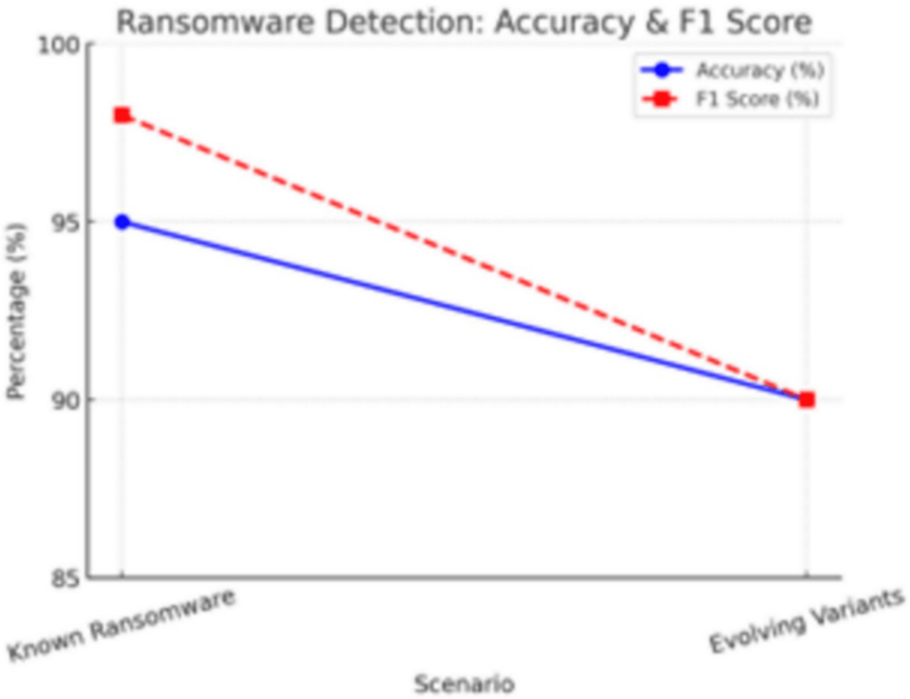


FIGURE 12: Comparison of Accuracy and F1-Score for Ransomware Detection

Table 2 illustrates comparison of accuracy and F1-score for ransomware detection.

Scenario	Accuracy(%)	F1-Score
Known Ransomware	95.0	0.98
Evolving Variants	90.0	0.87

TABLE 2: Accuracy and F1-Score Comparison

Throughput Comparison

Figure *13* illustrates comparison of throughput (samples processed per second) between traditional static analysis methods and the MTD system. The MTD system processed significantly more samples per second, indicating better efficiency.

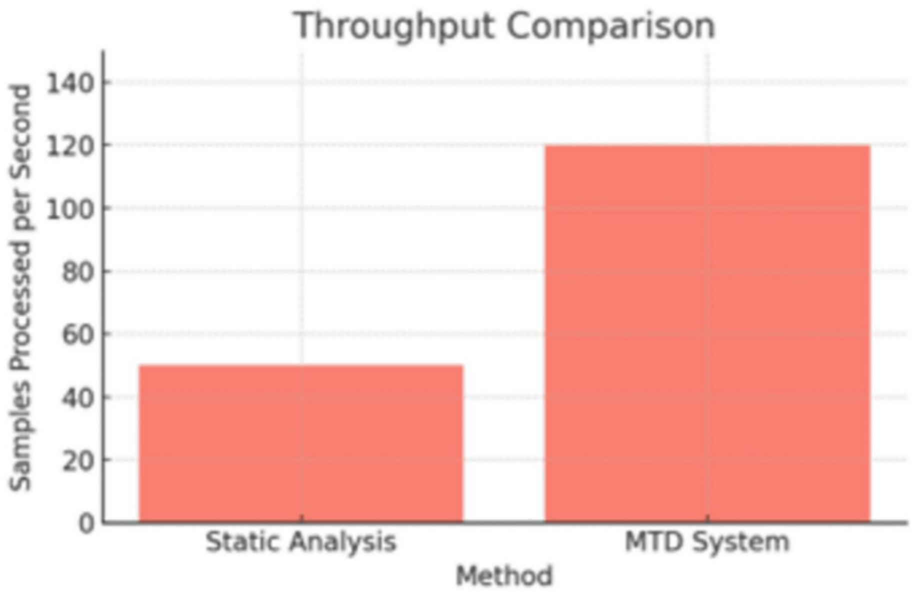


FIGURE 13: Throughput Comparison Between Static Analysis and MTD System

MTD, Moving Target Defense

Discussion

The deployment of MTD brings forth an active security model that dynamically adjusts system parameters to interfere with ransomware exploitation tactics. Through the use of attack surface randomization, API call obfuscation, and dynamic resource allocation, MTD greatly hinders adversary reconnaissance and payload execution. Combining static signature-based detection with dynamic behavioral analysis through tools such as Cuckoo Sandbox improves detection against known and emerging ransomware variants. Yet, MTD imposes computational overhead, requiring real-time optimization mechanisms to ensure system performance. Future developments need to address AI-based adaptive security models that automatically optimize MTD practices, providing immunity against the evolving polymorphic and metamorphic ransomware while limiting false positives and performance losses.

Conclusions

Ransomware detection and prevention using MTD offers a dynamic and adaptive approach to cybersecurity by continually altering the system's attack surface, making it difficult for attackers to exploit vulnerabilities or execute predictable strategies. This method enhances system resilience by preventing static attacks, promoting early detection, and enabling rapid response to ransomware actions, thereby limiting execution and spread. MTD, when combined with real-time detection techniques and multi-layered security measures, provides robust protection against evolving ransomware threats. In the future, MTD can be advanced by integrating machine learning and AI for predictive analysis blockchain for tamper-proof threat monitoring, and collaborative defense frameworks for shared threat intelligence. Research should also focus on optimizing MTD’s computational efficiency to ensure applicability in resource-constrained environments like Internet of Things and edge computing. With continuous innovation, MTD stands as a scalable and comprehensive solution to counter the ever-evolving ransomware landscape.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Sanika S. Shinde, Snehal Ghoparkar, Rashmi K. Patil, Sanika B. Patil

Acquisition, analysis, or interpretation of data: Sanika S. Shinde, Snehal Ghoparkar, Rashmi K. Patil, Sanika B. Patil

Drafting of the manuscript: Sanika S. Shinde, Snehal Ghoparkar, Rashmi K. Patil, Sanika B. Patil

Critical review of the manuscript for important intellectual content: Sanika S. Shinde, Snehal Ghoparkar, Rashmi K. Patil, Sanika B. Patil

Supervision: Snehal Ghoparkar

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue. **Animal subjects:** All authors have confirmed that this study did not involve animal subjects or tissue. **Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

References

1. Abu Elkhail A, Lachtar N, Ibdah D, Aslam R, Khan H, Bacha A: Seamlessly safeguarding data against ransomware attacks. IEEE Transactions on Dependable and Secure Computing. 2023, 20:1-16. 10.1109/tdsc.2022.3214781
2. Ahmad S, Zulkifli Z, Nasarudin NH, Imran M, Ariff M: A recent systematic review of ransomware attack detection in machine learning techniques. 2023 4th International Conference on Artificial Intelligence and Data Sciences (AiDAS). 2023, 349-354. 10.1109/AiDAS60501.2023.10284709
3. Duraibi S, Kaur C, Pawar AB: Cyber extortion unveiled: The evolution, tactics, challenges, and future of ransomware. 2023 International Conference on Computational Science and Computational Intelligence (CSCI). 2023, 861-867. 10.1109/CSCI62032.2023.00144
4. Khurana S: Ransomware threat detection and mitigation using machine learning models. 2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG). 2023, 1-6. 10.1109/ICTBIG59752.2023.10456343
5. Fujinoki H, Manukonda L: Proactive damage prevention from zero-day ransomwares. 2023 5th International Conference on Computer Communication and the Internet (ICCCI). 2023, 133-141. 10.1109/ICCCI59363.2023.10210183
6. Kunku K, Zaman AN, Roy K: Ransomware detection and classification using machine learning. IEEE Symposium Series on Computational Intelligence (SSCI). 2023, 862-866. 10.1109/SSCI52147.2023.10371924
7. Pagnotta G, De Gaspari F, Hitaj D, Andreolini M, Colajanni M, Mancin LV: DOLOS: A novel architecture for moving target defense. IEEE Transactions on Information Forensics and Security. 2023, 18:5890-5905. 10.1109/tifs.2023.3318964
8. Inoue K, Koide H: Detection and isolation of malware by dynamic routing moving target defense with proxies. 2022 International Conference on Computational Science and Computational Intelligence (CSCI). 2022, 1071-1075. 10.1109/CSCI58124.2022.00189
9. von der Assen J, Huertas Celdran A, Sánchez Sanchez PM, Cedeño J, Bovet G, Martínez Pérez G: A lightweight moving target defense framework for multi-purpose malware affecting IoT devices. ICC 2023 - IEEE International Conference on Communications. 2023, 6010-6015. 10.1109/ICC45041.2023.10278951
10. Kim DY, Choi GY, Lee JH: White list-based ransomware real-time detection and prevention for user device protection. 2018 IEEE International Conference on Consumer Electronics (ICCE). 2018, 1-5. 10.1109/ICCE.2018.8326119
11. Ozer M, Varlioglu S, Gonen B, Bastug M: A prevention and traction system for ransomware attacks. 2019 International Conference on Computational Science and Computational Intelligence (CSCI). 2019, 150-154. 10.1109/CSCI49370.2019.00032
12. Aldaraani N, Begum Z: Understanding the impact of ransomware: A survey on its evolution, mitigation, and prevention techniques. 2018 21st Saudi Computer Society National Computer Conference (NCC). 2018, 1-5.

10.1109/NCG.2018.8593029

13. Hirano M, Kobayashi R: Machine learning-based ransomware detection using storage access patterns obtained from live-forensic hypervisor. 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS). 2019, 1-6. 10.1109/IOTSMS48152.2019.8939214
14. Alexandrov B, Gotsev L, Petkova MV, Vladimirova Petkova V: Heuristic approach to ransomware detection and prevention at software or hardware level. 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). 2023, 1-6. 10.1109/ICECCME57830.2023.10252341
15. Ispahany J, Islam MR, Islam MV, Khan MA: Ransomware detection using machine learning: A review, research limitations and future directions. IEEE Access. 2024, 12:68785-68813. 10.1109/access.2024.3397921
16. The Digital Object Identifier (DOI) for the Ransomware Dataset . 2024:10.5281/zenodo.13890887