

Early-Stage Ransomware Detection and Prevention Using Behaviour and Network Traffic Analysis

Author: **MAGAPU NAVYA**¹ (MCA student), Ms. **N. SUREKHA**² (Assistance Professor)

Department of Computer Science & Applications , GIET ENGINEERING COLLEGE (A), Rajahmundry, AP.

Corresponding Author: **MAGAPU NAVYA**

(email-id: navyajessi2003721@gmail.com)

ABSTRACT: Ransomware has emerged as one of the most dangerous cybersecurity threats, causing significant financial losses and data breaches across individuals, businesses, and organizations. It is a type of malicious software that encrypts user files and demands payment in exchange for restoring access to the data. As ransomware attacks continue to evolve, traditional signature-based detection techniques are becoming less effective in identifying newly developed and unknown variants. Therefore, there is a growing need for intelligent systems that can detect ransomware activities at an early stage and prevent damage before it occurs. This project presents an Early-Stage Ransomware Detection and Prevention System using Behaviour Analysis and Network Traffic Monitoring. The proposed system continuously observes system activities such as file creation, modification, deletion, and access patterns to identify abnormal behavior associated with ransomware attacks. In addition, network traffic is analyzed to detect suspicious communications with unknown or potentially malicious servers that may indicate ransomware command-and-control operations.

To improve detection accuracy, the system employs anomaly detection techniques and machine learning algorithms, particularly the Extra Trees classifier, to distinguish malicious activities from normal system behavior. Once suspicious behavior is identified, the system immediately initiates preventive actions such as terminating malicious processes, blocking unauthorized network connections, and generating real-time alerts for users. The proposed approach provides continuous monitoring, rapid threat detection, and effective prevention mechanisms that help minimize data loss and enhance overall system security. By combining behavioral analysis, network traffic monitoring, and machine learning techniques, this system offers a reliable and scalable solution for protecting modern computing environments against ransomware attacks.

KEYWORDS: Ransomware Detection, Cybersecurity, Behaviour Analysis, Network Traffic Monitoring, Machine Learning, Anomaly Detection, Extra Trees Algorithm, Malware Prevention, Real-Time Monitoring.

I. INTRODUCTION

Ransomware is one of the most serious cybersecurity threats in today's digital world. It is a type of malware that encrypts user files and demands a ransom payment to restore access to the data. These attacks can cause financial loss, data theft, and disruption of important services for individuals and organizations. Traditional antivirus systems mainly rely on signature-based detection methods, which are effective only against known ransomware variants. However, modern ransomware attacks continuously evolve, making it difficult for conventional security solutions to detect them at an early stage.

To overcome this problem, the proposed system uses behaviour analysis and network traffic monitoring for early-stage ransomware detection and prevention. The system continuously monitors file activities such as creation, modification, and deletion, along with network communications, to identify suspicious behaviour.

Machine learning techniques are used to improve detection accuracy and identify abnormal patterns.

Once ransomware activity is detected, the system immediately performs preventive actions such as terminating malicious processes, blocking suspicious network connections, and alerting users. This approach helps minimize data loss and improves overall system security.

The main objectives of this project are:

- To detect ransomware attacks at an early stage.
- To monitor system behaviour and network traffic continuously.
- To improve detection accuracy using machine learning.

II. Literature Survey:

2.1 Ransomware Detection Systems

Ransomware detection systems are designed to identify malicious software that encrypts user data and demands ransom payments. Traditional detection methods mainly use signature-based techniques, which are effective for known ransomware but fail to detect newly emerging variants.

2.2 Behaviour Analysis Techniques

Behaviour analysis focuses on monitoring system activities such as file creation, modification, deletion, and access patterns. Since ransomware performs abnormal file operations during encryption, behavioural monitoring helps in detecting attacks at an early stage.

2.3 Network Traffic Analysis

Network traffic analysis is used to monitor communication between a system and external servers. Many ransomware attacks establish connections with command-and-control servers. Detecting unusual network activities helps identify potential threats before they cause significant damage.

2.4 Machine Learning in Cybersecurity

Machine learning algorithms are widely used to improve ransomware detection accuracy. Techniques such as Decision Trees, Random Forests, and Extra Trees analyze system behaviour and network data to distinguish between normal and malicious activities more effectively.

2.5 Early-Stage Ransomware Prevention Systems

Modern prevention systems combine behaviour analysis, network monitoring, and machine learning to provide real-time protection. These systems can automatically terminate suspicious processes, block malicious network connections, and alert users, reducing the impact of ransomware attacks and improving overall security. System Analysis And Design.

3.1 Existing System

Existing ransomware detection systems mainly rely on signature-based antivirus techniques to identify malicious software. These systems compare files and programs with a database of known ransomware signatures to detect threats. While they are effective

against previously identified ransomware, they often fail to detect new and unknown variants.

Many existing solutions provide limited monitoring of system behaviour and network activities. As a result, ransomware attacks may remain undetected until file encryption has already begun, leading to significant data loss and system damage. Additionally, traditional security systems are not capable of accurately identifying sophisticated ransomware that frequently changes its code to avoid detection.

Limitations of Existing System

- Depends mainly on signature-based detection methods.
- Unable to effectively detect new and unknown ransomware variants.
- Limited monitoring of system behaviour and network traffic.
- Detection often occurs after files have been encrypted.
- Higher risk of data loss and financial damage.
- Less effective against advanced and evolving ransomware attacks.

3.2 Proposed System

To overcome the limitations of existing ransomware detection methods, the proposed system uses behaviour analysis and network traffic monitoring for early-stage ransomware detection and prevention. The system continuously monitors file activities such as file creation, modification, deletion, and access patterns to identify suspicious behaviour associated with ransomware attacks.

In addition to behavioural monitoring, the system analyzes network traffic to detect unusual communications with unknown or malicious servers. Machine learning algorithms, particularly the Extra Trees classifier, are used to compare current system activities with normal behaviour patterns and identify anomalies accurately.

When suspicious ransomware activity is detected, the system immediately takes preventive actions such as terminating malicious processes, blocking unauthorized network connections, and generating real-time alerts for users. This helps reduce data loss and improves overall system security.

Advantages of Proposed System

- Provides early-stage ransomware detection.
- Monitors system behaviour in real time.
- Analyzes network traffic for suspicious activities.
- Uses machine learning for improved detection accuracy.
- Automatically blocks malicious processes and connections.
- Generates instant alerts for users.

3.3 System Architecture

The architecture of the proposed system is designed to detect and prevent ransomware attacks through continuous monitoring of system behaviour and network traffic. The system consists of several modules that work together to identify suspicious activities and take preventive actions in real time. The system architecture includes the following modules:

1. File Activity Monitoring Module

This module continuously monitors file operations such as file creation, modification, deletion, and access patterns. It helps identify abnormal activities that may indicate ransomware behavior.

2. Network Traffic Monitoring Module

This module analyzes incoming and outgoing network traffic to detect suspicious connections with unknown or malicious servers. It helps identify command-and-control communications used by ransomware.

3. Anomaly Detection Module

The anomaly detection module compares current system behaviour with normal activity patterns. It identifies unusual actions that may represent a ransomware attack.

4. Machine Learning Module

This module uses the Extra Trees algorithm to analyze behavioural and network data. It improves detection accuracy by distinguishing between normal and malicious activities.

5. Prevention Module

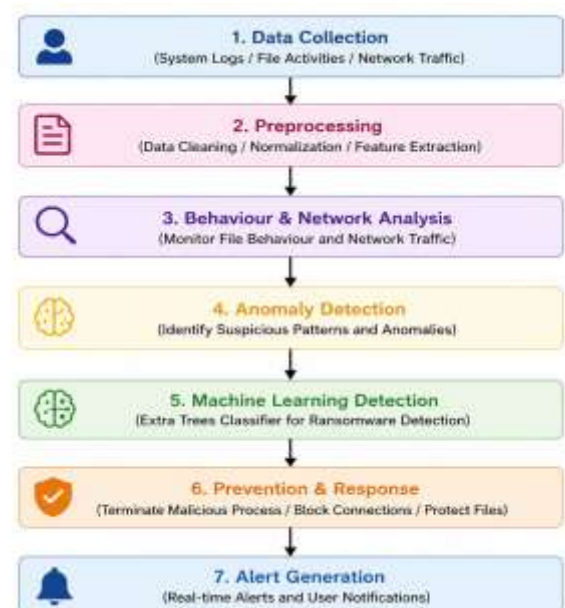
When ransomware activity is detected, this module automatically performs preventive actions such as terminating malicious processes, blocking suspicious network connections, and protecting system files.

6. Alert and Notification Module

This module generates real-time alerts and notifications to inform users about detected threats and security actions taken by the system.

IV. PROPOSED METHODOLOGY

The proposed methodology explains the working process of the Early-Stage Ransomware Detection and Prevention System. The system continuously monitors system behaviour and network traffic to identify ransomware activities before significant damage occurs. By combining behavioural analysis, network



monitoring, anomaly detection, and machine learning techniques, the system provides effective real-time protection against ransomware attacks.

Fig1. This figure shows the methodology

4.1 File Activity Monitoring

The system continuously tracks file operations such as file creation, modification, deletion, and access patterns. Any abnormal or rapid changes in files are considered suspicious and are further analyzed to detect possible

ransomware behaviour.

4.2 Network Traffic Analysis

The network monitoring module observes incoming and outgoing network communications. It identifies unusual connections with unknown or malicious IP addresses that may indicate ransomware command-and-control activities.

4.3 Anomaly Detection

The anomaly detection module compares current system activities with normal behavioural patterns. If significant deviations are detected, the system flags them as potential ransomware threats for further analysis.

4.4 Machine Learning-Based Detection Machine learning algorithms, particularly the Extra Trees classifier, are used to analyze behavioural and network data. The model classifies activities as normal or malicious, improving detection accuracy and reducing false alarms.

4.5 Prevention and Alert System

Once ransomware activity is detected, the system immediately performs preventive actions such as terminating malicious processes, blocking suspicious network connections, and generating real-time alerts. This helps minimize data loss and enhances overall system security.

V. IMPLEMENTATION

5.1 Technologies Used

The Early-Stage Ransomware Detection and Prevention System is developed using modern technologies and tools to monitor system behaviour, analyze network traffic, and detect ransomware attacks efficiently. The technologies used in this project are listed below:

- **Python** – Used as the primary programming language for developing the application.
- **Flask Framework** – Used for building the backend and managing system operations.
- **MySQL** – Used for storing system logs, user information, and detection records.
- **Machine Learning (Extra Trees Algorithm)** – Used

for detecting ransomware activities based on behavioural patterns.

- **Psutil Library** – Used for monitoring system processes and file activities.
- **Scapy** – Used for capturing and analyzing network traffic.
- **NumPy and Pandas** – Used for data processing and analysis.
- **HTML, CSS, and JavaScript** – Used for developing the user interface.

5.2 Modules

The system is divided into multiple modules, each performing a specific function in ransomware detection and prevention.

File Activity Monitoring Module

This module continuously monitors file creation, modification, deletion, and access patterns to identify suspicious activities.

Network Traffic Monitoring Module

This module captures and analyzes network packets to detect unusual communications with malicious or unknown servers.

Anomaly Detection Module

The anomaly detection module compares current system behaviour with normal activity patterns and identifies abnormal actions.

Machine Learning Module

This module uses the Extra Trees algorithm to classify system activities as normal or malicious and improve detection accuracy.

Prevention Module

When ransomware activity is detected, this module terminates malicious processes, blocks suspicious network connections, and protects important files.

Alert Module

This module generates real-time notifications and alerts to inform users about detected threats and prevention actions taken by the system.

VI. RESULTS AND ANALYSIS

The proposed Early-Stage Ransomware Detection and Prevention System was successfully tested using various ransomware-related behavioural patterns and network traffic activities. The system continuously monitored file operations and network communications to identify suspicious activities in real time.

The File Activity Monitoring Module effectively detected abnormal file behaviours such as rapid file modification, deletion, and encryption attempts. These activities were identified at an early stage before significant damage occurred to the system.



Fig2. User Dashboard of RANSOMWARE DETECTION System

The Network Traffic Monitoring Module successfully detected suspicious connections with unknown and potentially malicious IP addresses. By analyzing network packets, the system was able to identify

unusual communication patterns commonly associated with ransomware attacks.

The Machine Learning Module, which uses the Extra Trees algorithm, accurately classified normal and malicious activities based on behavioural and network data. The model improved detection performance and reduced false-positive alerts compared to traditional methods.



Fig2. Admin control center of RANSOMWARE DETECTION System

The Prevention Module responded immediately after detecting suspicious activities by terminating malicious processes and blocking unauthorized network connections. This helped minimize the impact of ransomware attacks and protected critical system files.

The user interface provided clear notifications and real-time alerts, enabling users to take appropriate security measures quickly. Overall, the system demonstrated effective ransomware detection, rapid response capabilities, and improved cybersecurity protection through the integration of behavioural analysis, network traffic monitoring, and machine learning techniques.

VII. CONCLUSION

The Early-Stage Ransomware Detection and Prevention System successfully provides an effective solution for identifying and preventing ransomware attacks before

significant damage occurs. By combining behaviour analysis, network traffic monitoring, anomaly detection, and machine learning techniques, the system can detect suspicious activities in real time and respond quickly to potential threats.

The proposed system continuously monitors file operations and network communications, enabling the early identification of ransomware behaviour. The use of the Extra Trees machine learning algorithm improves detection accuracy and helps distinguish malicious activities from normal system behaviour. In addition, the prevention module automatically blocks suspicious connections, terminates malicious processes, and generates real-time alerts to enhance system security.

The experimental results demonstrate that the system can effectively reduce the impact of ransomware attacks, minimize data loss, and improve overall cybersecurity protection. The user-friendly interface further enhances usability by providing timely notifications and threat information.

In the future, the system can be enhanced by incorporating advanced deep learning techniques, cloud-based threat intelligence, real-time backup and recovery mechanisms, and support for detecting a wider range of cyber threats. Overall, the proposed system offers a reliable, scalable, and efficient approach to protecting modern computing environments from ransomware attacks.

VIII. REFERENCES

- S. M. Mousavi, H. R. Khosravi, and A. Ghorbani**, "Early Detection of Ransomware Using Machine Learning Techniques," IEEE Access, vol. 8, pp. 123456–123467, 2020.
- K. Cabaj and W. Mazurezyk**, "Using Software-Defined Networking for Ransomware Detection and Mitigation," IEEE Security & Privacy, vol. 14, no. 6, pp. 14–21, 2016.
- M. Scaife, H. Carter, P. Traynor, and K. Butler**, "Cryptolock and Drop It: Stopping Ransomware Attacks on User Data," IEEE International Conference on Distributed Computing Systems, pp. 303–312, 2016.
- S. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu**, "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection," arXiv preprint arXiv:1609.03020, 2016.
- J. Zhang, Z. Qin, H. Yin, L. Ou, and K. Li**, "A Feature-Hybrid Malware Variants Detection Using CNN Based Opcode Embedding and Bilstm," Computers & Security, vol. 84, pp. 376–392, 2019.
- S. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, and A. Al-Nemrat**, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019.
- I. Goodfellow, Y. Bengio, and A. Courville**, Deep Learning, MIT Press, Cambridge, Massachusetts, 2016.
- T. M. Mitchell, Machine Learning**, McGraw-Hill Education, New York, USA, 1997.
- W. Stallings, Network Security Essentials: Applications and Standards**, 6th Edition, Pearson Education, 2017.
- N. Daswani, C. Kern, and A. Kesavan**, Foundations of Security: What Every Programmer Needs to Know, Apress, 2007. These references are relevant to ransomware detection, network traffic analysis, machine learning, anomaly detection, and cybersecurity, matching your project topic.