ISSN 2277-2685
IJESR/April-June. 2025/ Vol-15/Issue-2s/1164-1176
T Sai Sushmitha *et. al.,* / International Journal of Engineering & Science Research

Ransomware Detection Using Machine Learning

Dr P Sumalatha, T Sai Sushmitha, A Saileela

[1] Associate Professor, Department of CSE, Bhoj Reddy Engineering College for Women, India.

[2,3]B. Tech Students, Department of CSE, Bhoj Reddy Engineering College for Women, India.

ABSTRACT

Ransomware has emerged as one of the most disruptive and financially damaging forms of cybercrime, capable of paralyzing individuals, organizations, and critical infrastructure by encrypting sensitive data and demanding ransom payments. This seminar report explores the evolving landscape of ransomware attacks, focusing on the rise of Ransomware-as-a-Service (RaaS), double extortion tactics, and advanced evasion techniques. Traditional detection methods, primarily signature-based, are increasingly ineffective against modern, polymorphic ransomware variants. In response, the integration of machine learning (ML) techniques offers a promising direction for enhancing ransomware detection capabilities. This study investigates various ML models—supervised, unsupervised, and deep learning—and their applications in detecting ransomware during different stages of its lifecycle, including delivery, execution, and command-and-control communication. Emphasis is placed on feature engineering, real-time detection challenges, and the need for high-quality, standardized datasets. The report also outlines research limitations and future directions, advocating for scalable, interpretable, and proactive ML-based defense mechanisms. Through a comprehensive analysis, this work highlights the potential of machine learning to revolutionize ransomware detection and fortify cyber resilience.

1. INTRODUCTION

Ransomware is a type of malicious software (malware) designed to extort money from its victims. It achieves this by encrypting sensitive data and demanding a ransom payment in exchange for the decryption key. Over the years, ransomware has evolved into one of the most significant threats in cybersecurity. Unlike traditional malware, which often aims to disrupt operations or steal data covertly, ransomware openly locks victims out of their own files, creating urgency and fear to compel payment.

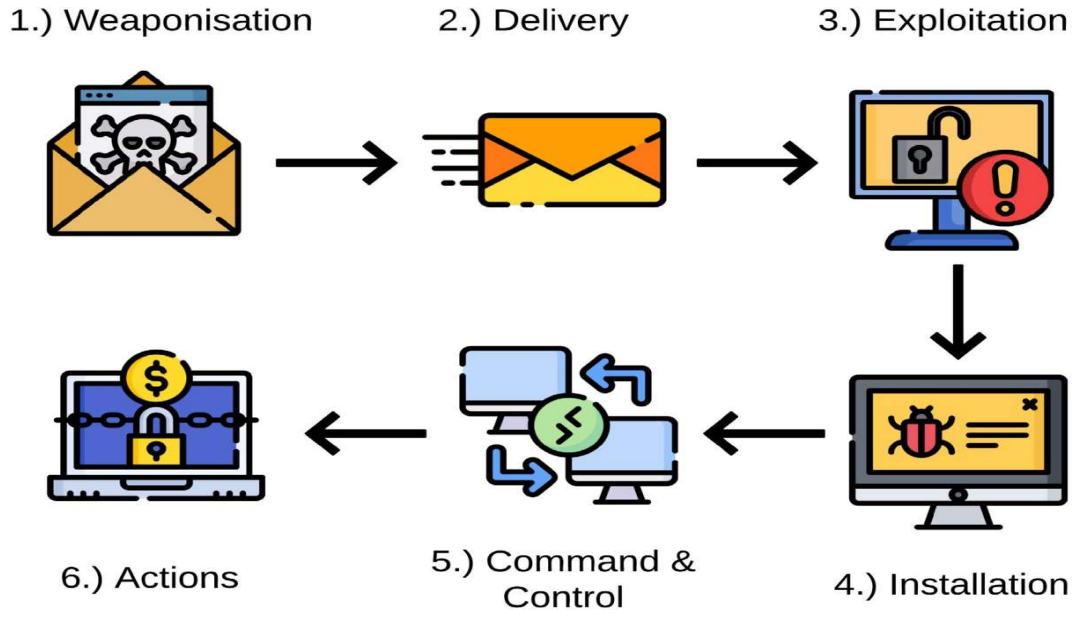
The financial and operational impact of ransomware attacks is immense, with global losses running into billions of dollars annually. Organizations face not only the direct costs of ransom payments but also indirect costs such as downtime, reputational damage, and legal repercussions. High-profile incidents, such as the Colonial Pipeline attack, demonstrate how ransomware can disrupt critical services, inflate costs, and compromise sensitive data. Furthermore, ransomware attacks can undermine public trust, particularly when critical infrastructure or essential services are affected. Such attacks highlight the urgent need for robust defensive strategies and policies to mitigate these risks.

2. RANSOMWARE ATTACKS AND TRENDS

Key Ransomware Families and Incidents

Ransomware attacks have evolved significantly over the years, with various families of ransomware emerging to target specific industries, regions, or systems. Notable ransomware families such as **LockBit**, **REvil**, **Darkside**, and **Conti** have been responsible for some of the most devastating attacks.

For instance, the 2021 Colonial Pipeline attack conducted by the
Darkside group disrupted fuel supply across the U.S. East Coast, leading to widespread panic and economic losses. Similarly, the Costa Rican government was crippled by a Conti ransomware attack, which infected over 1,500 systems and attacks even more lucrative and difficult to counter. forced the declaration of a national emergency. These incidents highlight not only the financial impact of ransomware but also its ability to cause societal and governmental disruptions. Modern ransomware groups employ advanced tactics like data exfiltration and double extortion, making their



Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service (RaaS) has revolutionized the ransomware landscape, making it accessible even to less technically skilled cybercriminals. This model allows ransomware developers to create sophisticated malware and offer it to affiliates who distribute it in exchange for a share of the profits. Affiliates handle tasks such as phishing campaigns or
exploiting vulnerabilities, while developers provide updates, customer support, and payment infrastructure. Groups like **LockBit** and **REvil** have embraced this model, earning millions of dollars in ransom payments. The RaaS model mirrors legitimate software businesses in its structure, offering subscription plans, feature updates, and even bug bounties to improve their malware. This professionalization has dramatically increased the scale and reach of ransomware campaigns globally.

Modular Nature and Evasion Techniques

Modern ransomware is modular, meaning it is designed to operate in stages, using various tools and techniques to achieve its goals. For example, ransomware might begin by exploiting a vulnerability to gain initial access, using tools like **Mimikatz** for credential harvesting or
Cobalt Strike for lateral movement within the network. Once inside, the ransomware might use legitimate system tools such as **PowerShell** or **Remote Desktop Protocol (RDP)** to avoid detection—a technique known as "living off the land." Advanced evasion tactics like process

injection, DLL sideloading, and fileless malware ensure that ransomware remains undetected during critical stages of the attack. These strategies make traditional signature- based detection systems less effective, emphasizing the need for behavior-based approaches.

3-RANSOMWARE DETECTION TECHNIQUES

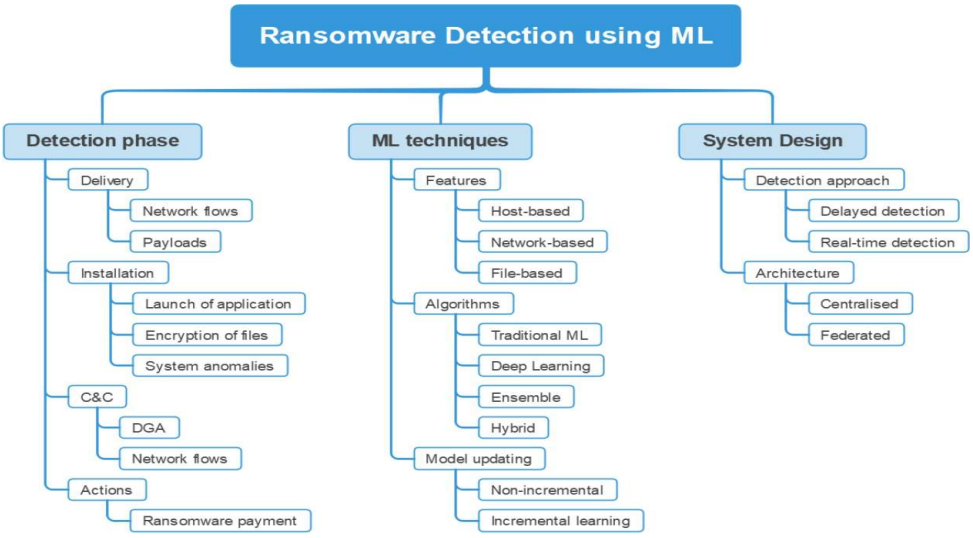
Signature-Based and Behavior-Based Detection

Ransomware detection techniques have evolved significantly over time, primarily categorized into signature-based and behavior-based methods. Signature-based methods rely on identifying known patterns or "signatures" of ransomware in files or processes. These signatures may include binary sequences, cryptographic hashes, or predefined rule sets. While effective for detecting known ransomware families, this approach struggles with polymorphic or metamorphic ransomware that can alter its code to evade detection. Figure 6 in the IEEE paper illustrates the stages of a ransomware attack, highlighting the phases where signature-based methods are less effective due to the modular nature of modern ransomware.

On the other hand, behavior-based detection examines the runtime activities of processes to identify malicious actions indicative of ransomware. This method monitors actions such as file access patterns, attempts to overwrite shadow copies, or suspicious encryption activity. For example, processes that initiate mass encryption or modify file permissions without user consent can be flagged as ransomware. Figure 7 from the paper provides a taxonomy of ransomware detection systems, emphasizing the shift towards behavior-based and machine- learning-driven models.

Detection During Delivery

The delivery phase of a ransomware attack, as shown in Figure 6, involves transmitting malicious payloads to the target. Detection at this stage focuses on analyzing network traffic and email attachments. Machine learning models, such as Bi-LSTM (Bidirectional Long Short- Term Memory), have been effectively used to monitor network communication patterns for anomalies. For instance, Liu and Patras (cited in the paper) detected ransomware spreading via the SMB protocol with a 99.97% accuracy rate. Similarly, network probes like those depicted in Figure 7 analyze file-sharing traffic, capturing features such as file reads, writes, and deletions, to train detection models.



Detection During Installation and Execution

The installation phase is critical for detecting ransomware as it begins interacting with the target system. Techniques during this phase include monitoring system logs, syscall traces, and API calls. For example, syscall-based detection provides low-level insights into ransomware behavior, such as attempts to delete shadow copies or disable security software. Dynamic analysis, where ransomware is executed in a sandbox environment, is commonly used to observe these behaviors. According to Figure 7, dynamic analysis forms a significant part of modern ransomware detection systems.

Tools like decoy files, also known as "honeypots," are placed within the system to trigger alerts if tampered with by ransomware. While effective, this approach works primarily as a confirmation method, as changes are detected post-encryption. Additionally, Figure 8 from the paper highlights features extracted during this phase, such as entropy changes in files and unusual CPU activity.

4-MACHINE LEARNING TECHNIQUES

Classification of ML Models Used in Ransomware Detection

Machine learning models used in ransomware detection can be broadly classified into supervised, unsupervised, and deep learning approaches:

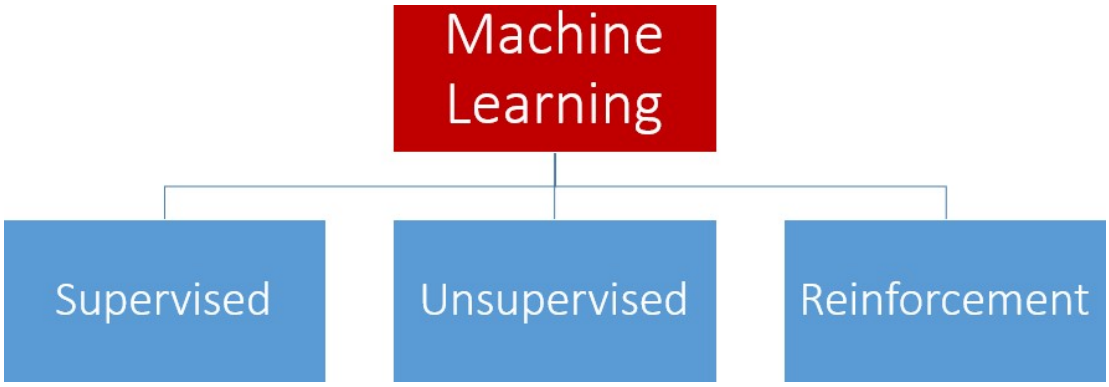


Fig 4.1 Machine Learning models

1. Supervised Learning

   Supervised learning models are trained on labeled datasets containing examples of both benign and ransomware-related activity. Algorithms like Random Forests,

   Decision Trees, and Logistic Regression are commonly used. For instance, a supervised model may classify files as malicious or benign based on extracted features such as opcode sequences or API call patterns.

2. Unsupervised Learning

   In scenarios where labeled data is scarce, unsupervised learning models like k-Means Clustering and One-Class SVMs are used for anomaly detection. These models

   identify deviations from normal system behavior, flagging potential ransomware activities.

3. Deep Learning

   Deep learning models, such as Convolutional Neural Networks (CNNs) and Long

Short-Term Memory (LSTM) networks, excel in handling complex, sequential, and high-dimensional data. LSTMs are particularly effective for analyzing time-series data, like system logs, to detect ransomware patterns over time. CNNs can process network traffic or file system snapshots to identify ransomware signatures.

Feature Engineering for Ransomware Detection

Feature engineering plays a critical role in machine learning-based ransomware detection. Features are typically categorized as **static** or **dynamic**:

- **Static Features**: These are extracted from files without executing them. Examples include file metadata, opcode sequences, and printable strings. While static features are computationally inexpensive to analyze, they are vulnerable to obfuscation techniques.
- **Dynamic Features**: These are observed during the execution of a file. System calls, API usage, and resource consumption patterns are common dynamic features. Dynamic analysis provides deeper insights into ransomware behavior but requires sandbox environments and incurs higher computational costs.

5-CONCLUSION

Ransomware continues to pose a severe threat to individuals, organizations, and governments worldwide. The increasing sophistication of ransomware tactics, including double extortion and advanced evasion techniques, underscores the need for innovative detection methods.

While traditional approaches like signature-based detection have proven inadequate against modern threats, machine learning offers a promising alternative by enabling adaptive and proactive defense mechanisms.

However, the effectiveness of machine learning-based ransomware detection depends on overcoming several challenges. High-quality datasets, standardized evaluation frameworks, and scalable system designs are critical to advancing the field. Real-time and early detection remain key priorities, as they provide the best chance of mitigating ransomware attacks before they cause significant damage.

Future research should focus on integrating advanced machine learning techniques with practical security tools, improving model interpretability, and fostering collaboration between academia, industry, and government agencies. By addressing these challenges, the cybersecurity community can develop robust solutions to combat ransomware and enhance global cyber resilience.

REFERENCES

1. J. Ispahany, M. R. Islam, M. Z. Islam, and M. A. Khan, "Ransomware Detection Using Machine Learning: A Review, Research Limitations and Future Directions," IEEE Access, vol. 12, pp. 68785-68796, 2024, doi: 10.1109/ACCESS.2024.3397921.
2. Liu and Patras, "Detecting ransomware using Bi-LSTM models: Network anomaly detection approach," Proceedings of the IEEE, 2024.
3. Almashhadani et al., "Identifying suspicious domains using machine learning for ransomware prevention," Cybersecurity and Infrastructure Protection Journal, vol. 23, no. 7, pp. 101–116, 2023.
4. Al-Haija and Alsulami, "Blockchain-based ransomware detection: A machine learning approach," Journal of Financial Security, vol. 17, no. 2, pp. 201–215, 2023.
5. Moussaileb et al., "Early detection of ransomware: Aligning detection phases with the Cyber-Kill-Chain," Expert Systems with Applications, vol. 42, no. 5, pp. 1231–1245, 2023.

6. Sumalatha Potteti Kanakandla Vasudha ,"A Machine Learning Approach for Network Intrusion Detection System," International Journal for Scientific Research & Development, vol. 8, no. 1, pp. 238–241, Mar. 2020.
7. Sumalatha Potteti, Namita Parati , "Intrusion Detection System Using Hybrid Fuzzy Genetic Algorithm," in Proceedings of the 2017 International Conference on Trends in Electronics and Informatics (ICEI), pp. 613–618, IEEE, May 2017.
8. G.S. Mahalakshmi P Sumalatha ,"Machine Learning Based Ensemble Classifier for Android Malware Detection," International Journal of Computer Networks & Communications (IJCNC), vol. 15, no. 4, pp. 111–128, Sept. 2023.