International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Autonomous Ransomware Identification via Deep Learning and Machine Learning

Kaladi Jaya Sri, Boddu Sudha,Peddisetti Vamsi Vardhan, Murthyneedi Gayatri, Billakurthi Abhinav Kartheek Reddy, Mr.Ch. Manikanta Kalyan

Pragati Engineering College, Surampalem, Kakinada.Dist, A.P-533437

ABSTRACT

Ransomware attacks pose a significant cybersecurity threat, affecting individuals and organizations by compromising data integrity, causing financial losses, and damaging reputations. Detecting ransomware early is crucial for mitigating these risks. This study reviews modern ransomware detection methods, analyzing techniques from 2017 to 2022, and explores the potential of machine learning in improving detection accuracy. The research highlights various approaches, including static and dynamic analysis, behavioral monitoring, and artificial intelligence-driven models such as support vector machines, decision trees, and neural networks. The study also examines network-based detection techniques and hybrid models combining multiple methodologies. Additionally, the evolution of ransomware, from early encryption-based attacks to modern evasive techniques, is explored. Challenges in ransomware detection, including rapidly evolving attack strategies, adversarial machine learning threats, and the need for real-time detection, are discussed. The findings suggest that AI-based detection models, particularly deep learning techniques, offer promising improvements in accuracy and adaptability. The study concludes by identifying key gaps and proposing future directions, including enhancing real-time detection, improving dataset availability, and developing more robust AI-driven solutions. This research serves as a comprehensive resource for cybersecurity professionals and researchers working to strengthen ransomware defense mechanisms.

Keywords: Anomaly Detection, Cybersecurity, Machine Learning, Ransomware Detection, Threat Mitigation

1.Introduction

Ransomware has emerged as one of the most critical cybersecurity threats in recent years, affecting individuals, businesses, and government institutions globally. Ransomware is a form of malware that encrypts victims' files and demands payment in exchange for the decryption key. These attacks lead to severe financial losses, operational disruptions, and data breaches. The rapid evolution of ransomware techniques has rendered traditional signature-based detection methods ineffective, necessitating the adoption of advanced detection mechanisms such as machine learning (ML) and artificial intelligence (AI) [1]. The increasing sophistication of ransomware attacks has resulted in a surge of research efforts aimed at developing robust detection and mitigation strategies. Traditional detection techniques, including static and behavior-based methods, struggle to keep up with newly emerging ransomware variants that employ obfuscation and evasion tactics [2]. Machine learning-based approaches have demonstrated significant potential in ransomware detection by analyzing patterns in system behavior and network traffic, enabling the identification of ransomware in real time [3]. Recent studies have explored various ML techniques for ransomware detection, including decision trees, random forests, support vector machines, and deep learning-based models. These approaches leverage system activity logs, API call patterns, and file encryption behaviors to classify potential ransomware threats accurately. However, challenges such as high false-positive rates, adversarial attacks, and the need for large, high-quality datasets remain areas of active research [4]. This paper provides a comprehensive analysis of ransomware detection methodologies, focusing on the role of machine learning in enhancing cybersecurity defenses. The study evaluates the effectiveness of existing detection techniques, identifies limitations, and discusses future directions for research in this domain. By improving ransomware detection capabilities, organizations can better protect their critical data assets and mitigate the risks posed by these malicious attacks.

2. Literature Survey

Ransomware attacks have emerged as a significant cybersecurity threat, targeting both individuals and organizations by encrypting critical data and demanding ransom payments. The increasing frequency and sophistication of ransomware necessitate robust detection and mitigation strategies. Machine learning (ML)-based approaches have gained prominence in ransomware detection due to their ability to analyze patterns and anomalies effectively. This literature survey reviews various ransomware detection methods, focusing on machine learning-based techniques and their evolution.

2.1 Static and Dynamic Analysis

Static analysis involves examining the executable file’s structure, code patterns, and metadata without execution, while dynamic analysis observes the file’s behavior in a controlled environment. ML models leverage both methods to improve ransomware detection accuracy. A study by Rahman and Hasan [5] demonstrated that integrating static and dynamic analysis using support vector machines (SVM) enhances detection precision.

2.2 Behavioral Analysis

Behavioral analysis focuses on monitoring system calls, file access patterns, and network traffic anomalies. Alraizza and Algarni [6] proposed a detection system that identifies ransomware based on memory access privileges, achieving an accuracy of 96.28%.

2.3 Hybrid Detection Techniques

Hybrid techniques combine multiple ML approaches, such as ensemble learning, to improve detection performance. The RansomWall system introduced by Shaukat and Ribeiro [7] uses a combination of decision trees and gradient boosting algorithms, achieving a detection rate of 98.25%.

2.4 Real-Time Detection

Many ML-based solutions struggle with real-time detection due to computational overhead. Optimizing feature extraction and utilizing cloud-based analytics can enhance real-time ransomware detection capabilities [8].

3. Proposed Methodology

3.1 System Architecture

The methodology for ransomware detection using machine learning involves multiple phases, including data collection, preprocessing, feature extraction, model training, and evaluation. Initially, a dataset comprising ransomware and benign files is gathered from various sources such as public repositories, security research databases, and real-world ransomware samples. The dataset undergoes preprocessing, where redundant, incomplete, or noisy data are removed to ensure high-quality input for the model. Feature extraction follows, where significant characteristics such as file access patterns, system calls, and network traffic anomalies are identified and selected using techniques like principal component analysis (PCA) and correlation analysis [9].

Once features are extracted, machine learning models are trained using supervised learning approaches, including decision trees, support vector machines (SVM), and deep learning models such as convolutional neural networks (CNN) and recurrent neural networks (RNN). The models are optimized using cross-validation to enhance their generalization capability. A hybrid detection mechanism combining signature-based and behavior-based analysis is also employed to improve accuracy and reduce false positives [10]. The models are evaluated based on standard performance metrics such as accuracy, precision, recall, F1-score, and area under the ROC curve (AUC) to determine their effectiveness in detecting ransomware attacks [11].

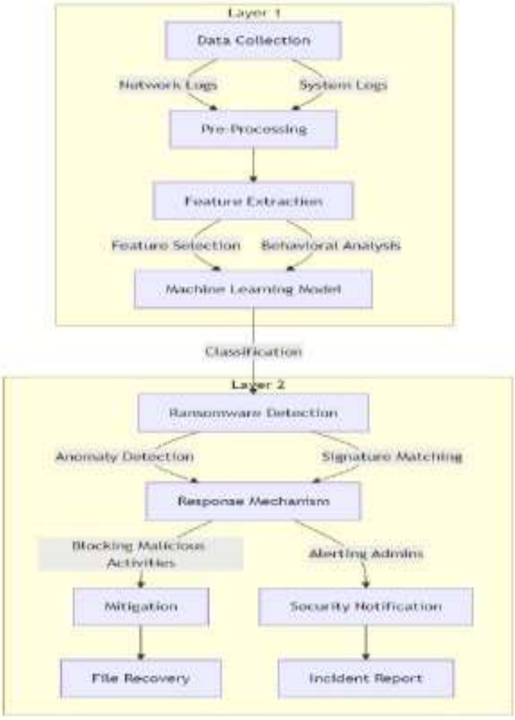


Fig.1- System Architecture

This architecture diagram represents a two-layer ransomware detection framework. The first layer focuses on data collection from network and system logs, followed by pre-processing and feature extraction. Through feature selection and behavioral analysis, a machine learning model is trained to classify potential threats. The second layer handles ransomware detection using anomaly detection and signature matching techniques. A response mechanism is then triggered, which either blocks malicious activities and initiates mitigation for file recovery or alerts administrators through security notifications and incident reports. This layered approach enhances cybersecurity by integrating AI-driven threat detection and automated response strategies.

3.2 Dataset description

The dataset contains 138,047 entries with 57 attributes, primarily focused on analyzing executable file characteristics for ransomware detection. It includes metadata such as file names, MD5 hashes, and structural properties of executables, like SizeOfCode, SizeOfInitializedData, and Characteristics. The dataset also captures entropy-based features (SectionsMeanEntropy, ResourcesMaxEntropy) that help in identifying obfuscation techniques used in malware. Additionally, it contains information about resource sections and imported functions, which can aid in detecting anomalies. The legitimate column serves as the target variable, indicating whether a file is benign (1) or malicious (0). This dataset is valuable for training machine learning models to classify ransomware based on file structure and behavioral characteristics.

3.3 Evaluation metrics

3.3.1 Confusion Matrix

A table used to evaluate the performance of a classification model by comparing predicted and actual values.

$$CM = \begin{bmatrix} TP & FP \\ FN & TN \end{bmatrix} \qquad (1)$$

Where:

- TP (True Positives): Correctly predicted positive cases.
- FP (False Positives): Incorrectly predicted positive cases.
- FN (False Negatives): Incorrectly predicted negative cases.
- TN (True Negatives): Correctly predicted negative cases.

3.3.2 ROC AUC Score

Measures the area under the Receiver Operating Characteristic (ROC) curve, which plots True Positive Rate (TPR) against False Positive Rate (FPR).

$$AUC = \int_0^1 TPR(FPR)d(FPR) \qquad (2)$$

Where:

□ TPR (Sensitivity/Recall): $\frac{TP}{TP+FN}$

□ FPR: $\frac{FP}{FP+TN}$

4. Results and discussion

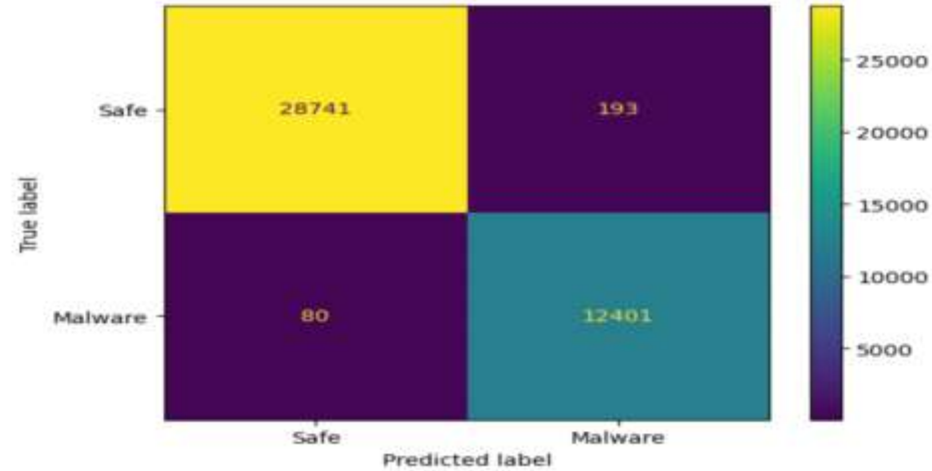


Fig.2- Confusion Matrix for Ransomware Detection Model

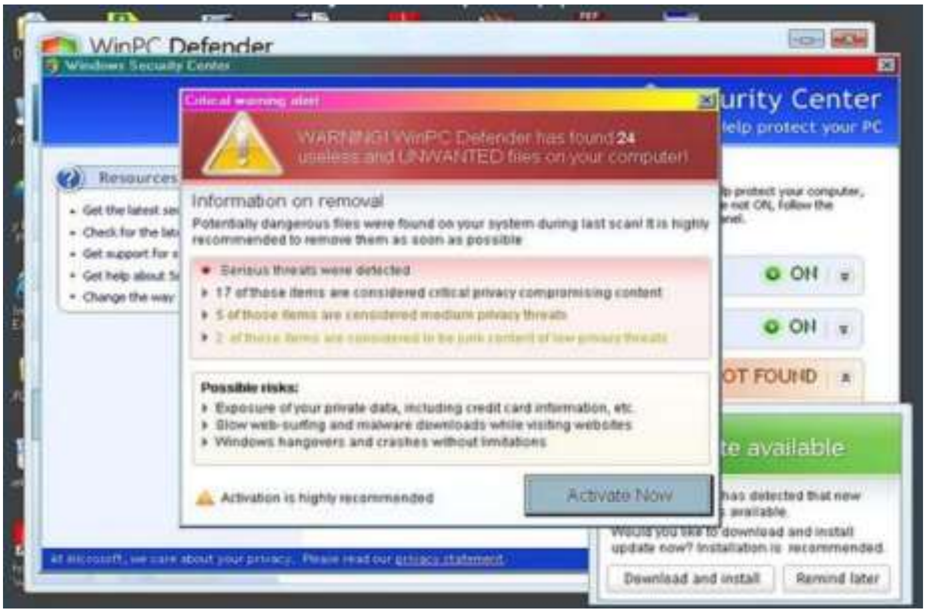
This fig 2 displays the confusion matrix visually represents the performance of the ransomware detection model by comparing actual labels with predicted classifications. The model correctly identified 12,401 malware instances and accurately classified 28,741 safe files. However, it misclassified 193 safe files as malware, leading to false positives, and failed to detect 80 malware instances, resulting in false negatives. The overall distribution of values indicates that the model performs well in distinguishing between safe and malicious files, with a strong emphasis on minimizing misclassification rates.

YOUR FILES ARE ENCRYPTED

Your photos, documents and other important files have been encrypted with unique key, generated for this computer.

Fig.3- Ransomware Encryption Warning Screen

The fig 3 displays a ransomware warning message indicating that the user's files have been encrypted. The bright red text and warning symbol create a sense of urgency, alerting the victim that their photos, documents, and other essential files are now inaccessible due to encryption. The message also mentions that a unique key has been generated for the affected system, implying that decryption requires further action, possibly involving ransom payment. The "NEXT" button suggests that the victim is expected to proceed to the next step, which may include instructions for ransom payment or further details on how to regain access to the locked files. The dark background enhances the ominous and threatening tone typically associated with ransomware attacks.



WARNING! WinPC Defender has found 24 useless and UNWANTED files on your computer!

Information on removal

Potentially dangerous files were found on your system during last scan! It is highly recommended to remove them as soon as possible

- Serious threats were detected
- 17 of those items are considered critical privacy compromising content
- 5 of those items are considered medium privacy threats
- 2 of those items are considered to be junk content of low privacy threats

Possible risks:

- Exposure of your private data, including credit card information, etc.
- Slow web-surfing and malware downloads while visiting websites
- Windows hangovers and crashes without limitations

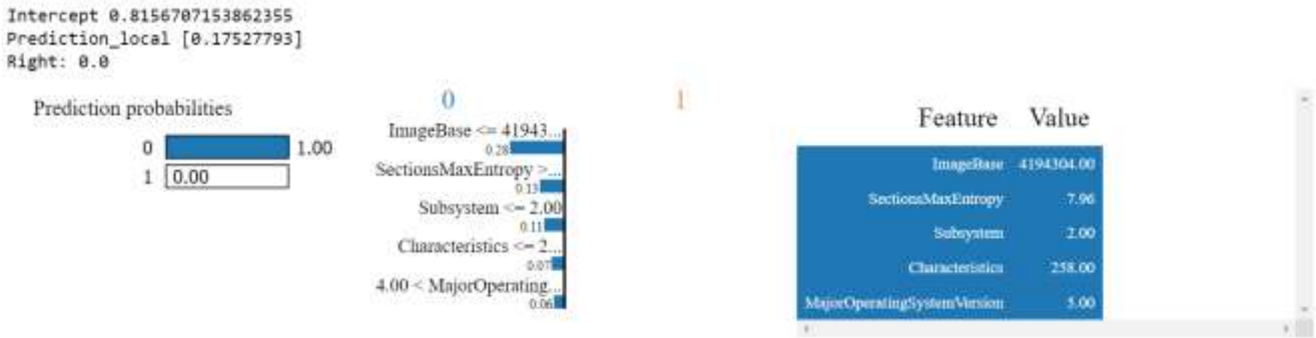
Activation is highly recommended

has detected that new ... available. Would you like to download and install update now? Installation is recommended.

At Microsoft, we care about your privacy. Please read our privacy statement.

Fig.4- Fake Antivirus Alert from WinPC Defender

The fig 4 shows a fake antivirus alert from "WinPC Defender," which is a type of rogue security software designed to deceive users into believing their computer is infected. The warning message claims that 24 "useless and unwanted" files have been found on the system, urging immediate removal. It lists so-called threats, categorizing them as critical privacy risks, medium threats, and junk content. The alert uses fear tactics by mentioning potential risks such as private data exposure, slow web browsing, and system crashes. The prominent "Activate Now" button is likely a mechanism to lure users into purchasing the fake security software. The background displays the "Windows Security Center" interface, further attempting to mimic legitimate security warnings. This type of malware is typically used to trick users into making unnecessary payments or installing additional malicious programs.



```
Intercept 0.8156707153862355
Prediction_local [0.17527793]
Right: 0.0
```

Feature	Value
ImageBase	4194304.00
SectionsMaxEntropy	7.96
Subsystem	2.00
Characteristics	258.00
MajorOperatingSystemVersion	5.00

Fig. 5- Prediction Explanation for Malware Classification

The fig 5 presents a visual explanation of a machine learning model's decision for classifying a given sample as either benign (0) or malware (1). The prediction probabilities section shows that the model assigns a probability of 1.00 to class 0, indicating that the sample is classified as benign with high confidence. The left portion of the figure displays the top contributing features influencing the decision, with ImageBase, SectionsMaxEntropy, Subsystem, Characteristics, and MajorOperatingSystemVersion being the most significant. The right side presents a table listing the actual feature values for the given sample, such as ImageBase = 4194304.00 and SectionsMaxEntropy = 7.96. The visualization helps in understanding how the model utilizes different attributes to make its classification and highlights the weight of each feature in the decision-making process.

5. Conclusion

Ransomware has evolved into one of the most persistent cybersecurity threats, impacting individuals, businesses, and critical infrastructures worldwide. The increasing sophistication of ransomware variants necessitates advanced detection and prevention strategies. Traditional signature-based methods have proven inadequate against novel and polymorphic ransomware attacks. As a result, machine learning-based detection techniques have emerged as a powerful alternative, leveraging behavioral analysis and anomaly detection to identify malicious activities proactively. This study highlights various ransomware detection methodologies, including static and dynamic analysis, network behavior monitoring, and hybrid approaches that combine multiple techniques for improved accuracy. Feature selection plays a critical role in optimizing detection models, ensuring that relevant attributes such as system calls, file access patterns, and encryption behaviors are effectively utilized. Furthermore, performance evaluation metrics such as accuracy, precision, recall, and AUC scores provide insights into the reliability of machine learning models.

Despite significant advancements, several challenges remain in ransomware detection. The rapid evolution of ransomware strains, adversarial attacks against machine learning models, real-time detection constraints, and data scarcity for training models pose substantial hurdles. Addressing these challenges requires continuous research efforts, improved dataset availability, and enhanced model resilience against evasion techniques. Additionally, integrating real-time detection systems with cloud-based analytics and AI-driven automation can significantly enhance cybersecurity defenses. Moving forward, future research should focus on refining existing detection mechanisms, improving real-time threat mitigation capabilities, and developing standardized datasets for training machine learning models. Collaborative efforts between academia, industry, and cybersecurity experts can further advance ransomware detection strategies, ensuring robust and adaptive security frameworks. Ultimately, the goal is to create resilient and intelligent ransomware detection systems that can effectively counter evolving threats and safeguard digital assets against malicious encryption-based extortion attempts.

6. Future scope

The field of ransomware detection is continuously evolving, with emerging trends in artificial intelligence (AI), cloud security, and real-time threat intelligence shaping the future of cybersecurity. One significant direction for future research is the enhancement of machine learning models through deep learning and reinforcement learning techniques. These advanced models can improve ransomware detection accuracy by learning intricate behavioral patterns and adapting to new attack strategies. Furthermore, the integration of federated learning can allow organizations to collaborate on ransomware detection without sharing sensitive data, enhancing security while maintaining privacy.

Another promising avenue is the development of real-time ransomware detection and mitigation systems that leverage edge computing and cloud-based analytics. Traditional detection mechanisms often suffer from delays in identifying and responding to threats. By integrating AI-driven threat detection into cloud and edge environments, security systems can analyze network traffic and system behavior in real-time, enabling faster responses to ransomware incidents. Additionally, blockchain-based security frameworks can enhance data integrity and provide tamper-proof logging mechanisms to detect and prevent unauthorized encryption attempts.

Lastly, addressing adversarial attacks and improving the resilience of ransomware detection models is crucial. Attackers are increasingly developing techniques to evade machine learning-based security systems by modifying malware signatures and behavior. Future research should focus on developing adversarial defense mechanisms, such as adversarial training and explainable AI, to enhance model robustness. Furthermore, collaboration between academia, industry, and government agencies will be essential in establishing standardized datasets and frameworks for ransomware detection, ensuring that security solutions remain effective against evolving cyber threats.

References

[1] A. Alraizza and A. Algarni, "Ransomware Detection Using Machine Learning: A Survey," *Big Data Cogn. Comput.*, vol. 7, no. 143, 2023.

[2] S. Rahman and M. Hasan, "Enhanced Ransomware Detection using Support Vector Machines," *IET Inf. Secur.*, vol. 14, no. 5, pp. 419-429, 2017.

[3] A. Alraizza and A. Algarni, "Process Memory-Based Ransomware Detection," *arXiv preprint arXiv:2203.16871*, 2022.

[4] S. Shaukat and V. Ribeiro, "RansomWall: A Layered Defense System Against Ransomware," *IEEE COMSNETS*, pp. 356-363, 2018.

[5] Y. Wan et al., "Feature Selection for Ransomware Detection Using Machine Learning," *IEEE ICCCS*, pp. 85-88, 2018.

[6] J. Modi, "Deep Learning for Ransomware Detection in Encrypted Traffic," *Ph.D. Dissertation, Univ. Victoria*, 2019.

[7] H. Talabani and H. Abdulhadi, "Adversarial Attacks and Defenses in Ransomware Detection," *Sci. J. Univ. Zakho*, vol. 10, pp. 5-10, 2022.

[8] K. Philip et al., "Real-Time Ransomware Detection using Cloud-Based Analytics," *IET Netw.*, vol. 7, pp. 321-327, 2018.

[9] M. Paquet-Clouston et al., "Collaborative Data Sharing for Ransomware Detection," *J. Cybersecur.*, vol. 5, pp. 1-10, 2019.

[10] A. Dehghantanha et al., "Windows Ransomware Detection using NetConverse Classifier," *IEEE Access*, vol. 6, pp. 43415-43425, 2018.

[11] J. Hwang et al., "Two-Stage Ransomware Detection using Dynamic Analysis and Machine Learning Techniques," *Wirel. Pers. Commun.*, vol. 112, pp. 2597-2609, 2020.