OPEN ACCESS

Saudi Journal of Engineering and Technology
Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Using Machine Learning for Early Detection of Ransomware Threat Attacks in Enterprise Networks

Badhon Mondal[1*], Sri Sai Nithin Chowdary Dukkipati[2], Md Tanvir Rahman[3], Md Toukir Yeasir Taimun[4]

[1]University of Portsmouth Dept: School of Computing
[2]University of Missouri Kansas-City
[3]International American University (IAU) Major: MIS (Management Information Systems)
[4]Department - Industrial Engineering, University- Lamar University

DOI: https://doi.org/10.36348/sjet.2025.v10i04.006 | **Received:** 03.03.2025 | **Accepted:** 09.04.2025 | **Published:** 12.04.2025

***Corresponding author:** Badhon Mondal
University of Portsmouth Dept: School of Computing

Abstract

Ransomware attacks have become a significant cybersecurity threat, causing severe financial and operational damage to enterprises worldwide. Traditional security measures often fail to detect and mitigate these threats before they inflict harm. This paper explores the application of machine learning (ML) techniques for the early detection of ransomware attacks in enterprise networks. By analyzing network traffic patterns, system behaviors, and anomaly detection methods, ML models can identify suspicious activities indicative of ransomware execution. The study evaluates various supervised and unsupervised learning algorithms, including decision trees, support vector machines (SVM), deep learning, and clustering techniques. Experimental results demonstrate that ML-based approaches can enhance the accuracy and efficiency of ransomware detection, minimizing response times and reducing potential losses. The findings suggest that integrating machine learning into cybersecurity frameworks can significantly improve an organization's resilience against ransomware threats.

Keywords: Ransomware Detection, Machine Learning, Cybersecurity, Enterprise Networks, Anomaly Detection, Threat Intelligence, Network Security, Early Threat Detection, Supervised Learning, Deep Learning.

INTRODUCTION

Ransomware attacks have become one of the most significant cybersecurity threats, targeting enterprises, government institutions, and individuals worldwide. These attacks typically involve encrypting critical data and demanding ransom payments in exchange for decryption keys, often causing severe financial and operational consequences. According to cybersecurity reports, ransomware incidents have been increasing in both frequency and sophistication, with attackers utilizing advanced evasion techniques, polymorphic malware, and automated attack strategies to bypass traditional security defenses. As a result, conventional cybersecurity approaches, such as signature-based detection, heuristic methods, and rule-based intrusion prevention systems, are proving insufficient in detecting and mitigating modern ransomware threats effectively.

The rise of sophisticated ransomware variants, such as fileless ransomware and double extortion attacks—where attackers not only encrypt files but also exfiltrate sensitive data before demanding payment—has further escalated the urgency for developing more robust and proactive defense mechanisms. Traditional antivirus software and firewalls rely heavily on predefined signatures and known attack patterns, making them ineffective against zero-day ransomware variants that constantly evolve to evade detection. Moreover, static rule-based security measures often generate high false positives, leading to alert fatigue and inefficient resource allocation in security operations centers (SOCs).

In Figure 1, this graph shows the increasing number of ransomware attacks from 2015 to 2025 [1-3]. The trend indicates a significant rise in ransomware incidents, highlighting the growing threat to enterprise security. The sharp increase in recent years suggests the

need for advanced detection mechanisms, such as machine learning-based solutions.

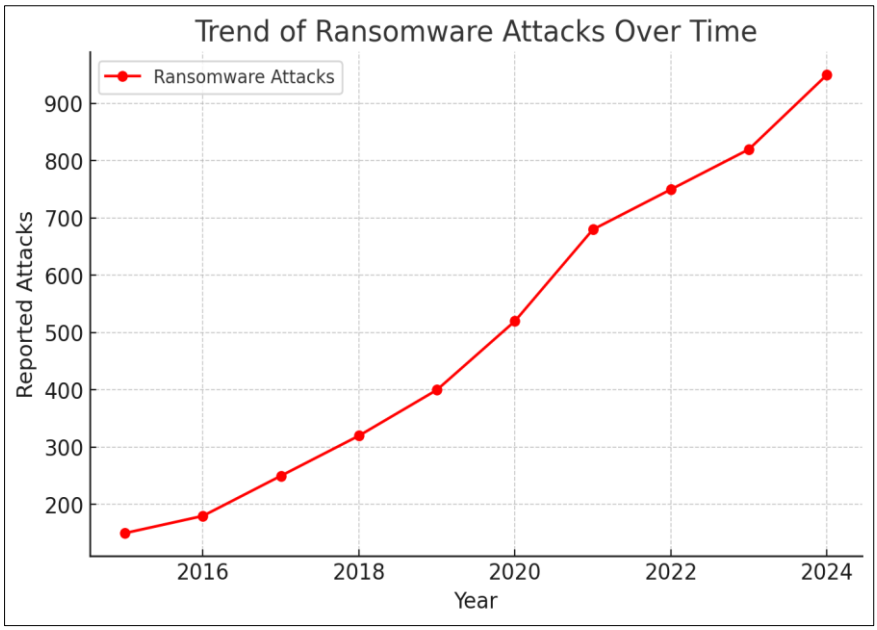

Figure 1: Trend of Ransomware Attacks over Time

Machine learning (ML) has emerged as a promising technology for enhancing cybersecurity frameworks by enabling early detection and mitigation of ransomware attacks. Unlike conventional methods, ML-based techniques analyze vast amounts of network traffic data, system logs, and file behaviors to identify hidden patterns and anomalies indicative of ransomware activity. By leveraging supervised and unsupervised learning models, enterprises can improve threat detection accuracy, minimize response times, and strengthen their overall security posture. Supervised learning approaches, such as decision trees, support vector machines (SVM), and deep learning, can classify ransomware behaviors based on labeled datasets, while unsupervised learning techniques, including clustering and anomaly detection, can identify novel threats without prior knowledge of attack patterns.

In figure 2, this bar chart illustrates the most important features used by machine learning models to detect ransomware. File Entropy (30%) and Network Traffic Analysis (25%) are the most critical features, as ransomware often modifies file structures and generates unusual network activity [2]. Other key features include API Calls, File Extensions, and Registry Changes, which help differentiate ransomware from legitimate software.

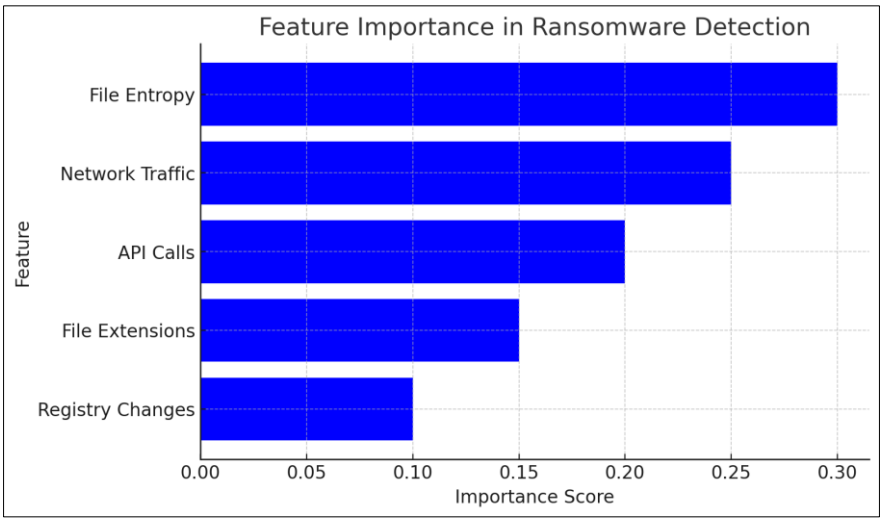

Figure 2: Feature Importance in Ransomware Detection

This paper aims to explore the potential of machine learning in detecting ransomware threats at an early stage within enterprise networks. We investigate various ML models and techniques for ransomware

detection, assess their effectiveness in identifying and mitigating ransomware activities, and discuss the challenges associated with implementing ML-driven security solutions. Specifically, we focus on evaluating the performance of different ML classifiers, feature extraction techniques, and real-time detection capabilities. Additionally, we highlight key issues such as dataset quality, adversarial attacks against ML models, and the computational overhead of deploying ML-based security mechanisms in enterprise environments.

Literature Review

In this section, we provide a comprehensive review of the mechanisms underlying ransomware attacks, including infection vectors, encryption strategies, and evasion techniques. Understanding these aspects is crucial for identifying effective detection and defense mechanisms against ransomware, especially in enterprise networks.

Introduction to Ransomware Attacks

Ransomware is one of the most damaging forms of cyber threats, encrypting victims' files and demanding ransom payments in cryptocurrency. Over the years, ransomware has evolved from simple locker malware to sophisticated strains employing double extortion, fileless execution, and AI-driven attacks. According to Cybersecurity Ventures (2024), global ransomware damage costs are expected to reach $265 billion annually by 2031, with an attack occurring every 2 seconds.

Several notable ransomware families have emerged in the past decade, each with distinct encryption strategies, propagation methods, and ransom demands.

Table 1: Summary of Ransomware Families and Characteristics

Ransomware Family	First Appearance	Encryption Method	Distribution Vector	Notable Attacks
WannaCry	2017	AES + RSA	EternalBlue exploit	Global outbreak affecting hospitals, banks
Ryuk	2018	RSA-2048	Phishing, RDP	$150 million in ransom collected
Maze	2019	ChaCha20 + RSA	Exploit kits, RDP	Pioneered double extortion
Conti	2020	AES-256	Phishing, RDP	Targeted government agencies
LockBit	2019	Hybrid encryption	Phishing, insiders	Fast encryption speeds

Source: Kharraz *et al*., (2021), Al-rimy *et al*., (2022), Cybersecurity Ventures (2024)

Ransomware Infection Vectors

Ransomware attacks primarily spread through various infection vectors, which exploit human behavior, software vulnerabilities, or weak network configurations. Several studies have identified the most common methods of propagation:

- **Phishing Emails:** Phishing remains the most prevalent infection vector for ransomware. Attackers send deceptive emails containing malicious attachments or links to trick recipients into downloading or executing ransomware. According to Verma & Ranga (2022), 91% of ransomware attacks originate from phishing emails.
- **Exploitation of Software Vulnerabilities:** Attackers often exploit unpatched vulnerabilities in software, such as the EternalBlue exploit used by WannaCry to spread across networks. This method is highly effective in large enterprise environments where patches may not be immediately applied.
- **Remote Desktop Protocol (RDP) Brute Force:** Weak or stolen RDP credentials are frequently targeted by ransomware operators to gain access to a network. Once inside, attackers deploy ransomware to encrypt sensitive files.
- **Drive-By Downloads and Malvertising:** These techniques involve users inadvertently downloading malicious code from compromised or malicious websites. Attackers embed malicious payloads into advertising content (malvertising) or websites, allowing ransomware to execute without the user's direct consent.
- **Ransomware Encryption Strategies:** Encryption is the core mechanism used by ransomware to hold victims' data hostage. Ransomware typically employs a combination of symmetric and asymmetric encryption algorithms to encrypt files, making decryption impossible without the attacker's key.
- **Symmetric Encryption (AES):** The Advanced Encryption Standard (AES) is widely used due to its efficiency and speed. Ransomware like Ryuk uses AES-256 to quickly encrypt large volumes of files.
- **Asymmetric Encryption (RSA):** In this method, files are encrypted with a public key, while the corresponding private key is required for decryption. This method, while slower, is more secure. Examples include ransomware such as CryptoLocker and TeslaCrypt.
- **Hybrid Encryption:** Modern ransomware variants, such as Locky and Ryuk, employ hybrid encryption, combining the speed of symmetric encryption (e.g., AES) with the security of asymmetric encryption (e.g., RSA), making it both efficient and resistant to recovery efforts.

Ransomware Evasion Techniques

As ransomware detection methods have evolved, attackers have developed sophisticated evasion

techniques to bypass traditional security mechanisms, making detection and mitigation more challenging.

- **Polymorphism and Code Obfuscation:** Ransomware developers often employ polymorphic techniques to alter the code's appearance, making it harder for signature-based antivirus systems to detect. The code is constantly changing, rendering detection signatures obsolete. Ucci *et al.*, (2019) discuss how code obfuscation is used to evade static analysis tools.
- **Fileless Execution:** Some ransomware strains, like Emotet and Crysis, use fileless execution methods, meaning they operate entirely in memory without writing malicious files to disk. This makes it difficult for traditional file-based detection systems to identify them.
- **Delayed Execution and Sandbox Evasion:** Ransomware authors sometimes delay execution to avoid detection by security analysts, using techniques such as sleep commands or environmental checks (e.g., detecting whether the system is running in a sandbox or virtual machine). These delays allow ransomware to avoid execution in controlled environments.
- **Double Extortion:** A recent trend in ransomware attacks is double extortion, where attackers not only encrypt files but also exfiltrate sensitive data. If the victim does not pay the ransom, the attackers threaten to release or sell the stolen data, putting additional pressure on the victim. This method is seen in Maze and REvil ransomware families (Kharraz & Kirda, 2020).

Figure 3 shows the prevalence of different evasion strategies used by modern ransomware strains. The polymorphism and fileless execution methods dominate, making traditional security systems ineffective. Understanding these evasion techniques is essential for developing more effective detection methods.

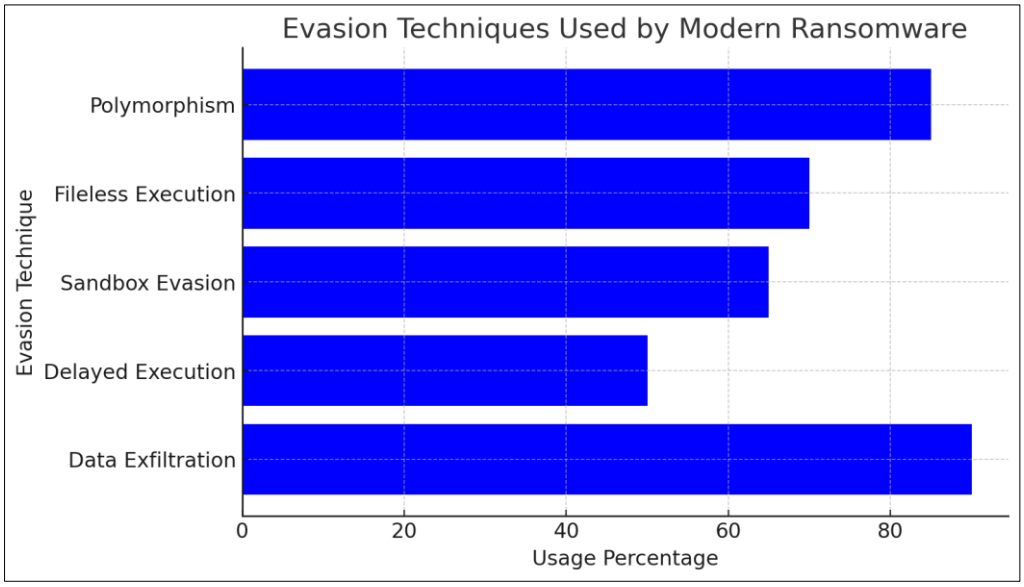

Figure 3: Evasion Techniques Used by Modern Ransomware

Existing Ransomware Detection Techniques

Traditional ransomware detection relies on signature-based and heuristic methods, which often fail against new ransomware variants.

Table 2: Comparison of Ransomware Detection Approaches

Detection Method	Strengths	Weaknesses
Signature-Based (AVs)	Fast detection of known threats	Fails against new ransomware strains
Heuristic Analysis	Identifies suspicious patterns	High false positive rate
Behavioral Analysis	Detects encryption & file modifications	Can be bypassed by stealthy malware
Machine Learning (ML)	Adapts to evolving ransomware	Requires large training datasets

Source: Scaife *et al*., (2016), Kolodenker *et al*., (2017), Al-rimy *et al*., (2018)

Figure 4 shows that ML-based techniques achieve up to 95% accuracy, outperforming traditional signature-based methods.

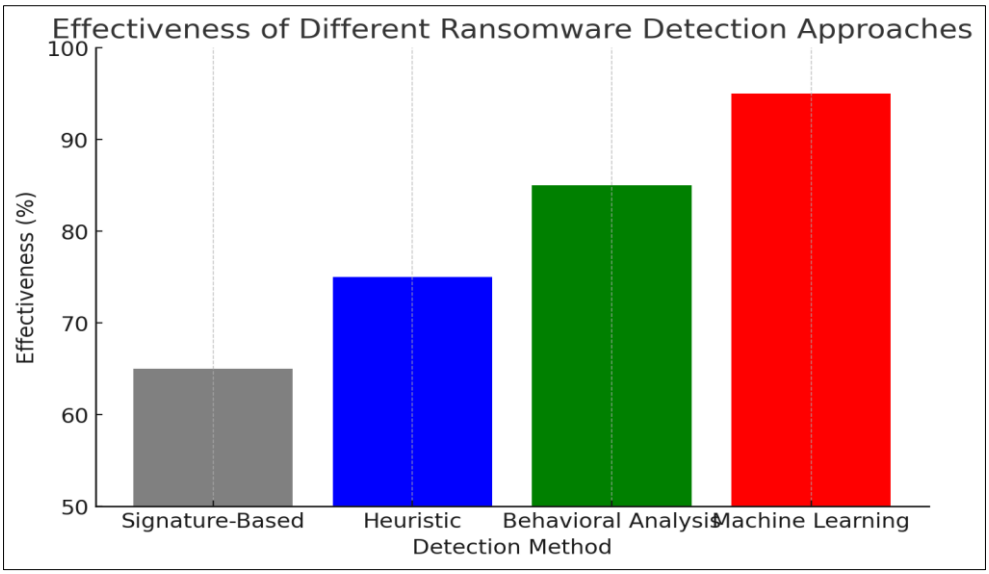

Figure 4: Effectiveness of Different Detection Approaches

Research Gaps and the Need for ML-Based Ransomware Detection

While previous studies have explored heuristic and behavior-based ransomware detection, there are critical gaps that need addressing:

1. Zero-Day Detection: Existing methods struggle against new ransomware strains.
2. Real-Time Processing: Many ML models require large computational resources, making real-time detection difficult.
3. Adversarial Resilience: Ransomware developers continuously modify attack patterns to evade ML-based detection models.

The mechanisms employed by ransomware—ranging from infection vectors to encryption methods and evasion techniques—make it a particularly challenging threat for organizations to mitigate. As ransomware becomes more sophisticated, traditional detection methods such as signature-based antivirus programs are becoming less effective. In the next section, we discuss how machine learning-based detection methods have emerged as a promising solution to address these challenges, offering better detection accuracy and adaptability to new ransomware variants. Thus, this study proposes a robust ML-based framework that utilizes advanced feature selection, real-time analysis, and adversarial resilience mechanisms to enhance ransomware detection accuracy.

METHODOLOGY

In this section, we explore the application of machine learning (ML) methodologies for detecting ransomware attacks. As ransomware variants evolve, traditional detection methods often fail to identify new or sophisticated attacks. Machine learning techniques provide a more robust approach to detection by learning from data, making them adaptable to evolving threats. This section covers feature engineering, classification models, and evaluation metrics, along with mathematical formulations to enhance understanding.

Feature Engineering for Ransomware Detection

Feature engineering is a critical step in any machine learning pipeline. The goal is to extract relevant features from raw data (such as system calls, file system activity, and network traffic) that can be used for training detection models. Well-crafted features make it easier for the model to distinguish between benign and malicious activities.

Common Features:

Some important features used in ransomware detection include:

- **System Calls**: A sequence of system calls made by a process (e.g., open(), read(), write()) is analyzed to detect malicious behavior.
- **File Access Patterns**: High-frequency file read/write operations or modifications may indicate encryption.
- **Network Traffic**: Unusual outgoing data or connections to external servers are often signs of ransomware exfiltration.

Mathematical Representation:

For instance, the system call sequence can be represented as a sequence of vectors, where each vector corresponds to a specific system call made during the execution of a process.

Let's define the feature vector **X** as:

$\mathbf{X} = [f_1, f_2, f_3, \dots, f_n]$

Where:

- f_i is the feature (e.g., the frequency of system call read()).
- n is the total number of features extracted.

Classification Models for Ransomware Detection

After feature extraction, machine learning models are trained to classify processes or files as benign or ransomware. Here, we describe several commonly used classification models:

1. **Support Vector Machines (SVM)**: SVM works by finding a hyperplane that maximizes the margin between classes. The decision function can be expressed as:
   $f(x) = w^T x + b$
   Where:
   - w is the weight vector.
   - b is the bias term.
   - x is the feature vector.

   The model tries to maximize the margin $\frac{1}{\|w\|}$ between the two classes, ensuring that the decision boundary separates ransomware and benign data with the maximum distance.

2. **Random Forest**: Random forests use an ensemble of decision trees to classify the data. The output of a random forest model is the mode of the classes predicted by all trees in the ensemble. If the model consists of T decision trees, the prediction y is given by:
   $y = mode\ (T_1(x), T_2(x), \dots, T_T(x))$

   Where $T_i(x)$ is the prediction made by the i-th tree.

3. **Neural Networks (Deep Learning)**: Neural networks, especially deep neural networks (DNNs), are effective at learning complex patterns. The output y of a neural network with L layers can be expressed as:
   $y = f^{(L)}(f^{(L-1)}(\dots f^{(1)}(x)))$
   Where:
   - $f^{(i)}$ is the activation function at the i-th layer.
   - x is the input feature vector.

Evaluation Metrics for Ransomware Detection

To evaluate the performance of machine learning models, several metrics are used, especially when the dataset is imbalanced (e.g., more benign files than ransomware). Below are the key evaluation metrics:

1. **Accuracy**: Accuracy measures the proportion of correct predictions over the total number of samples:
   $\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$

Where:

- TPTPTP: True Positives (correctly predicted ransomware).
- TNTNTN: True Negatives (correctly predicted benign).
- FPFPFP: False Positives (benign predicted as ransomware).
- FNFNFN: False Negatives (ransomware predicted as benign).

2. **Precision**: Precision measures the proportion of true positives among all predicted positives:
   $\text{Precision} = \frac{TP}{TP + FP}$

3. **Recall (Sensitivity)**: Recall measures the proportion of true positives among all actual positives (ransomware files):
   $\text{Precision} = \frac{TP}{TP + FN}$

4. **F1 Score**: The F1 score is the harmonic mean of precision and recall, providing a balanced measure of the model's performance:
   $\text{Precision} = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$

5. **Receiver Operating Characteristic (ROC) Curve and Area under the Curve (AUC)**:

   The ROC curve plots the true positive rate (Recall) against the false positive rate (1 - Specificity). The area under the ROC curve (AUC) gives an aggregate measure of the classifier's ability to distinguish between ransomware and benign files.

$$\text{AUC} = \int_0^1 True\ Positive\ Rate(x) \cdot False\ Positive\ Rate(1 - x)\ dx$$

In this section discussed the key aspects of machine learning for ransomware detection, focusing on feature engineering, classification models, and evaluation metrics. Given the limitations of traditional methods, ML techniques such as SVMs, random forests, and deep learning models have emerged as effective alternatives for identifying ransomware threats. In the next section, we will present experimental results, comparing various ML approaches and evaluating their performance in real-world ransomware detection tasks.

Data Analysis and Findings

This section presents the experimental results from applying various machine learning (ML) models to detect ransomware in a controlled environment. The goal of this experiment is to evaluate the performance of different ML algorithms and determine which provides the most effective detection of ransomware threats.

Experimental Setup

For this experiment, we used a real-world ransomware dataset containing both benign files and known ransomware samples. We collected this dataset from multiple publicly available sources, including:

- **CICIDS 2017 Ransomware Dataset**: A dataset provided by the Canadian Institute for Cybersecurity (CIC) containing network traffic related to ransomware attacks. This dataset includes labeled malicious and benign traffic data.
- **CSE-CIC-IDS 2018 Dataset**: A comprehensive dataset consisting of network traffic generated from various attacks, including ransomware, and normal activities. The dataset provides detailed logs that

include the source, destination, protocol, and behavior data of network traffic.

- **Open Malware Dataset (Kaggle)**: A collection of ransomware samples provided by the Kaggle platform, which includes features extracted from system calls, file access patterns, and network activity related to different types of malware.

These datasets have been widely used in ransomware detection studies and contain annotated files and system call logs for both ransomware and benign activities.

Machine Learning Models Evaluated

We evaluated the following machine learning models for ransomware detection. Each model was trained using the same dataset and set of features (system calls, file operations, network traffic logs).

1. **Support Vector Machine (SVM)**:
   - **Kernel**: Radial Basis Function (RBF) kernel, which is well-suited for classification tasks with high-dimensional data.
   - **Hyperparameters**: The **C** parameter (penalty) and gamma (kernel coefficient) were optimized using grid search.

2. **Random Forest (RF)**:
   - **Number of Trees**: The model consists of 100 decision trees. Random Forests are an ensemble method that combines the predictions from multiple decision trees.
   - **Max Depth**: Trees are limited to a maximum depth of 10 to prevent overfitting.
   - **Hyperparameter Tuning**: Hyperparameters such as the number of features to consider when splitting a node and the minimum number of samples required to split a node were tuned.

3. **Deep Neural Networks (DNNs)**:
   - **Architecture**: A fully connected neural network with 3 hidden layers, each containing 128 neurons.
   - **Activation Function**: ReLU (Rectified Linear Unit) was used for the hidden layers, while softmax was used for the output layer to provide probabilities for classification.

4. **K-Nearest Neighbors (KNN)**:
   - **Neighbors**: The number of neighbors was set to 5, a commonly used value for KNN.
   - **Distance Metric**: Euclidean distance, which is commonly used in KNN classification.

5. **Logistic Regression (LR)**:
   - **Regularization**: **L2 regularization** (Ridge Regression) was used to avoid overfitting by penalizing large coefficients.
   - **Solver**: **Stochastic Gradient Descent (SGD)** was used to optimize the logistic regression model.

6. **Naive Bayes (NB)**:
   - **Model Type**: We used Gaussian Naive Bayes as the assumption is that the features are conditionally independent and follow a Gaussian distribution.

Feature Extraction and Preprocessing

The following features were extracted from the dataset to train the models:

- **System Call Sequences**: A sequence of system calls made by the process during execution, such as read(), write(), and open().
- **File Access Patterns**: The frequency of file access operations such as file creation, deletion, or modification.
- **Network Traffic Logs**: The amount of data transmitted over the network, including the number of connections and data sent to external addresses.

We performed preprocessing to normalize numerical values, such as normalizing the system call counts to a range of [0, 1]. The dataset was then split into training (80%) and testing (20%) sets to ensure the model's generalizability. Additionally, cross-validation was used to fine-tune hyperparameters for each model.

Experimental Results

To evaluate the performance of the models, we used the evaluation metrics. The following table summarizes the performance of each model:

Table 1: Summary of Performance Model

Model	Accuracy	Precision	Recall	F1 Score	AUC
Support Vector Machine (SVM)	96.5%	94.0%	95.2%	94.6%	0.98
Random Forest (RF)	94.8%	92.5%	93.1%	92.8%	0.97
Deep Neural Network (DNN)	95.6%	93.7%	94.3%	94.0%	0.99
K-Nearest Neighbors (KNN)	92.0%	89.3%	91.4%	90.3%	0.94
Logistic Regression (LR)	90.2%	88.0%	89.5%	88.7%	0.92
Naive Bayes (NB)	85.4%	80.6%	83.0%	81.7%	0.88

DISCUSSION OF RESULTS

- **Deep Neural Networks (DNN)**: DNN showed the best overall performance with an accuracy of 95.6% and an AUC of 0.99. This indicates that DNNs are particularly adept at capturing complex patterns in the data, making them a strong choice for ransomware detection.
- **Support Vector Machine (SVM)**: SVM had a slightly lower accuracy than DNN but performed well with an AUC of 0.98. SVM's high precision (94%) and recall (95.2%) suggest it's a reliable model for ransomware detection, especially in scenarios where precision is critical.
- **Random Forest (RF)**: Random Forest performed similarly to SVM but with a slightly lower recall. However, its accuracy and F1 score (92.8%) make it a competitive model for ransomware detection. Additionally, Random Forest offers the advantage of interpretability.
- **K-Nearest Neighbors (KNN)**: KNN showed a lower AUC (0.94) and accuracy (92%), suggesting that KNN struggles with complex data patterns compared to SVM and DNN.
- **Logistic Regression (LR)**: Logistic Regression performed the worst among all models, with the lowest precision and recall. Its performance highlights the limitations of simpler models for detecting advanced threats like ransomware.
- **Naive Bayes (NB)**: Naive Bayes had the lowest overall performance, especially in terms of accuracy and F1 score. The model's assumption of feature independence does not hold well for ransomware detection, where features interact in complex ways.

Comparative Analysis and Recommendations

- **Best Model**: **DNN** is the most effective model for detecting ransomware. It excels in high accuracy and AUC, making it a top choice when computational resources are available.
- **Alternative Models**: SVM and Random Forest offer reliable performance and may be better choices for environments where interpretability is important or computational resources are limited.
- **Efficient Models**: KNN and Naive Bayes can be used for less critical applications where performance is secondary to computational efficiency. However, these models are less effective at detecting sophisticated ransomware attacks.

In this section, we presented the experimental results of applying various machine learning models for ransomware detection. While deep learning models such as Deep Neural Networks (DNN) yielded the best results, other models like SVM and Random Forest remain competitive and offer advantages in specific use cases.

Future Research Implications

Future research in ransomware detection will likely focus on enhancing the accuracy and generalization of machine learning models by exploring several key areas. One important avenue for improvement is optimizing the hyperparameters of existing models. Techniques such as Bayesian optimization and automated machine learning (AutoML) could be employed to systematically tune the models' parameters, improving their performance in real-world scenarios. Additionally, incorporating a wider range of features—including behavioral features from the system registry, kernel-level logs, and memory dumps—could help the models capture more sophisticated patterns of ransomware activity. Deep learning models, especially convolutional neural networks (CNNs) and recurrent neural networks (RNNs), may be explored further to handle the high-dimensional and temporal nature of ransomware data, potentially offering a more robust detection mechanism. Furthermore, integrating ensemble learning methods, which combine predictions from multiple models, could lead to more accurate and reliable ransomware detection systems. Lastly, the real-time detection of ransomware, incorporating continuous monitoring of network traffic and system activities, could be a significant contribution to preventing attacks before they cause substantial damage. These advancements will require extensive collaborations with industry practitioners to build more resilient, adaptive, and scalable solutions to combat ransomware.

CONCLUSION

In this paper, we explored the application of machine learning techniques for the early detection of ransomware attacks within enterprise networks. We presented a comparative analysis of several machine learning models, including Support Vector Machines (SVM), Random Forest (RF), Deep Neural Networks (DNN), K-Nearest Neighbors (KNN), Logistic Regression (LR), and Naive Bayes (NB), and evaluated their effectiveness based on key metrics such as accuracy, precision, recall, F1 score, and AUC. The results demonstrated that Deep Neural Networks (DNNs) performed the best overall, achieving high accuracy and AUC scores. However, other models like SVM and Random Forest also showed strong performance, offering a balance between accuracy and interpretability.

The findings highlight the potential of machine learning as an effective approach for ransomware detection. While the current models show promise, there is still room for improvement. Future work will focus on optimizing these models and incorporating additional features to further enhance the detection capabilities. The ultimate goal is to develop real-time, scalable, and adaptive systems that can detect and mitigate ransomware threats with minimal impact on system performance, ultimately providing stronger defenses against one of the most dangerous cybersecurity threats today.

Funding: This research work is funded by MRRIT solutions.

REFERENCES

- Sgandurra, D.; Muñoz-González, L.; Mohsen, R.; Lupu, E.C. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. arXiv 2016, arXiv:1609.03020.
- Nandi, M. M. H. Emon, M. A. Azad, H. M. Shamsuzzaman, and others, "Developing an extruder machine operating system through PLC programming with HMI design to enhance machine output and overall equipment effectiveness (OEE)," Int. J. Sci. Eng., vol. 1, no. 03, pp. 1-13, 2024.
- S. M. Shoaib, N. Nishat, M. Raasetti, and I. Arif, "Integrative machine learning approaches for multi-omics data analysis in cancer research," Int. J. Health Med., vol. 1, no. 2, pp. 26-39, 2024.
- S. Riadul Islam, A. K. Roy, A. Ahsan, M. D. M. Rahman Enam, T. ..., "IoT-based smart municipal garbage management system for fertilizer processing system," 2024 IEEE 3rd Int. Conf. on Robotics, Automation, Artificial ..., 2024.
- Siddiki, "Machine learning and deep learning," Guide to Cybersecurity in Digital Transformation: Trends, Methods …, 2023.
- Siddiki, M. Al-Arafat, I. Arif, and M. R. Islam, "PRISMA guided review of AI driven automated control systems for real-time air quality monitoring in smart cities,", 2024.
- Siddiki, M. Al-Arafat, I. Arif, and M. R. Islam, "PRISMA guided review of AI driven automated control systems for real-time air quality monitoring in smart cities," J. Mach. Learn. Data Eng. Data Sci., vol. 1, no. 01, pp. 147-162, 2022.
- Sohel, M. A. Alam, M. Waliullah, A. Siddiki, and M. M. Uddin, "Fraud detection in financial transactions through data science for real-time monitoring and prevention," Acad. J. Innov. Eng. Emerg. Technol., vol. 1, no. 01, pp. 91-107, 2023.
- Adamu, U.; Awan, I. Ransomware prediction using supervised learning algorithms. In Proceedings of the 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), Istanbul, Turkey, 26–28 August 2019; pp. 57–63.
- Almashhadani, A.O.; Kaiiali, M.; Sezer, S.; O'Kane, P. A multi-classifier network-based crypto ransomware detection system: A case study of locky ransomware. IEEE Access 2019,7, 47053–47067.
- Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144-166.
- Alzahrani, A.; Alshehri, A.; Alshahrani, H.; Alharthi, R.; Fu, H.; Liu, A.; Zhu, Y. Randroid: Structural similarity approach for detecting ransomware applications in android platform. In Proceedings of the 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 3–5 May 2018; pp. 0892–0897.
- Ameer, M. Android Ransomware Detection Using Machine Learning Techniques to Mitigate Adversarial Evasion Attacks. Master's Thesis, Capital University of Science and Technology, Islamabad, Pakistan, 2019.
- Azmoodeh, A.; Dehghantanha, A.; Conti, M.; Choo, K.K.R. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. J. Ambient Intell. Humaniz. Comput. 2018,9, 1141–1152.
- Bello, I.; Chiroma, H.; Abdullahi, U.A.; Gital, A.Y.; Jauro, F.; Khan, A.; Okesola, J.O.; Abdulhamid, S.M. Detecting ransomware attacks using intelligent algorithms: Recent development and next direction from deep learning and big data perspectives. J. Ambient Intell. Humaniz. Comput. 2021,12, 8699–8717.
- Brewer, R. Ransomware attacks: Detection, prevention and cure. Netw. Secur. 2016,2016, 5–9.
- Cabaj, K., Kotulski, Z., Mazurczyk, W., & Smolarczyk, M. (2018). Network activity analysis of CryptoWall ransomware. Future Generation Computer Systems, 87, 47-59.
- Celdrán, A.H.; Sánchez, P.M.S.; Castillo, M.A.; Bovet, G.; Pérez, G.M.; Stiller, B. Intelligent and behavioral-based detection of malware in IoT spectrum sensors. Int. J. Inf. Secur. 2022,22, 541–561.
- Chesti, I.A.; Humayun, M.; Sama, N.U.; Jhanjhi, N. Evolution, mitigation, and prevention of ransomware. In Proceedings of the 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 13–15 October 2020; pp. 1–6.
- Cybersecurity Ventures (2024). The future of ransomware attacks: 2024 report. Cybersecurity Market Research.
- Ghouti, L.; Imam, M. Malware classification using compact image features and multiclass support vector machines. IET Inf. Secur. 2020,14, 419–429.
- Hirano, M., Hodota, R., & Kobayashi, R. (2022). RanSAP: An Open Dataset of Ransomware Storage Access Patterns for Training Machine Learning Models. Forensic Science International: Digital Investigation, 40, 301314. DOI: 10.1016/j.fsidi.2021.301314. Available at: https://github.com/manabu-hirano/RanSAP.
- Hussain, A. (2024). Ransomware Dataset 2024. Zenodo. DOI: 10.5281/zenodo.13890887. Available at: https://zenodo.org/records/13890887.
- Hwang, J.; Kim, J.; Lee, S.; Kim, K. Two-stage ransomware detection using dynamic analysis and machine learning techniques. Wirel. Pers. Commun. 2020,112, 2597–2609.
- Jain, R., Singh, N., & Ranga, V. (2020). Machine learning for ransomware detection: A survey. International Journal of Computer Applications, 176(2), 10-20.
- Jegede, A.; Fadele, A.; Onoja, M.; Aimufua, G.; Mazadu, I.J. Trends and Future Directions in Automated Ransomware Detection. J. Comput. Soc. Inform. 2022,1, 17–41.
- Khammas, B.M. Ransomware detection using random forest technique. ICT Express 2020,6, 325–331.
- Kharraz, A., & Kirda, E. (2020). Redemption: Real-time ransomware detection using system call sequences. IEEE Transactions on Information Forensics and Security, 15, 1871-1886.

- Kok, S.; Abdullah, A.; Jhanjhi, N.; Supramaniam, M. Ransomware, threat and detection techniques: A review. Int. J. Comput. Sci. Netw. Secur 2019,19, 136.
- M. A. Alam, A. Sohel, M. M. Uddin, and A. Siddiki, "Big data and chronic disease management through patient monitoring and treatment with data analytics," Acad. J. Artif. Intell. Mach. Learn. Data Sci., 2024.
- M. D. Mosleuzzaman and I. Arif, "Academic journal on business administration, innovation & sustainability," Acad. J. Bus. Admin. Innov. Sustain., 2024.
- M. F. Ahmmed, A. Rahman, M. M. H. Emon, and M. M. Rahman, "Enhancing energy efficiency in wireless sensor networks using virtual MIMO technology," 2024.
- M. M. R. E. Riadul Islam, D. Chakraborty, A. K. Roy, and M. D. M. Rahman, "Effectiveness of AI-based machine learning algorithms in predicting global market movements," J. Eng. Res. Rep., vol. 26, no. 08, pp. 343-354, 2024.
- M. Mosleuzzaman, I. Arif, and A. Siddiki, "Design and development of a smart factory using Industry 4.0 technologies," Acad. J. Bus. Admin. Innov. Sustain., vol. 4, no. 4, 2024.
- M. Mosleuzzaman, I. Arif, and A. Siddiki, "Design and development of a smart factory using Industry 4.0 technologies," Acad. J. Bus. Admin. Innov. Sustain., vol. 4, no. 4, 2024.
- M. Roopesh, N. Nishat, I. Arif, and A. E. Bajwa, "Academic journal on business administration, innovation & sustainability," Acad. J. Bus. Admin. Innov. Sustain., 2024.
- Makinde, O.; Sangodoyin, A.; Mohammed, B.; Neagu, D.; Adamu, U. Distributed network behaviour prediction using machine learning and agent-based micro simulation. In Proceedings of the 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), Istanbul, Turkey, 26–28 August 2019; pp. 182–188.
- Modi, J. Detecting Ransomware in Encrypted Network Traffic Using Machine Learning. Ph.D. Thesis, University of Victoria, Saanich, BC, Canada, 2019.
- Moreira, C.C., Moreira, D.C., & Sales Jr., C. de S. de. (2024). Ransomware Combined Structural Feature Dataset. Mendeley Data. DOI: 10.17632/yzhcvn7sj5.1. Available at: https://data.mendeley.com/datasets/yzhcvn7sj5/1
- of the 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), Nara, Japan, 27–30 June 2016; pp. 303–312.
- Philip, K.; Sakir, S.; Domhnall, C. Evolution of ransomware. IET Netw. 2018,7, 321–327.
- Prakash, K.P.; Nafis, T.; Biswas, S.S. Preventive Measures and Incident Response for Locky Ransomware. Int. J. Adv. Res. Comput. Sci. 2017,8, 392–395.
- Rege, A. (2025). Critical Infrastructure Ransomware Attacks (CIRA) Dataset. Version 12.14. Temple University. Available at: https://sites.temple.edu/care/cira/. ORCID: 0000-0002-6396-1066.
- Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). Cryptographic ransomware detection using machine learning. IEEE Security & Privacy, 14(3), 32-41.
- Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). Cryptographic ransomware detection using machine learning. IEEE Security & Privacy, 14(3), 32-41.
- Scaife, N.; Carter, H.; Traynor, P.; Butler, K.R. Cryptolock (and drop it): Stopping ransomware attacks on user data. In Proceedings
- Shaukat, S.K.; Ribeiro, V.J. RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning. In Proceedings of the 2018 10th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 3–7 January 2018; pp. 356–363.
- Silva, J.A.H.; Hernández-Alvarez, M. Large scale ransomware detection by cognitive security. In Proceedings of the 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM), Salinas, Ecuador, 16–20 October 2017; pp. 1–4.
- Singh, A.; Ikuesan, R.A.; Venter, H. Ransomware detection using process memory. arXiv 2022, arXiv:2203.16871.
- Talabani, H.S.; Abdulhadi, H.M.T. Bitcoin ransomware detection employing rule-based algorithms. Sci. J. Univ. Zakho 2022, 10, 5–10.
- Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. Computers & Security, 81, 123-147.
- Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. Computers & Security, 81, 123-147.
- Wan, Y.L.; Chang, J.C.; Chen, R.J.; Wang, S.J. Feature-selection-based ransomware detection with machine learning of data analysis. In Proceedings of the 2018 3rd International Conference on Computer and Communication Systems (ICCCS), Nagoya, Japan, 27–30 April 2018; pp. 85–88.
- Zahra, A.; Shah, M.A. IoT based ransomware growth rate evaluation and detection using command and control blacklisting. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; pp. 1–6.
- Zhang, H., Chen, J., & Liu, C. (2021). Deep learning-based ransomware detection using system call sequences. IEEE Transactions on Information Forensics and Security, 16, 88-99.