ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025

DETECTION OF RANSOMWARE USING MACHINE LEARNING

[1]K.BINDU PRIYA, [2]UZMA AFREEN, [3]DASARI NAVYA, [4]MADASU SAI CHANDU, [5]VADDI SIVA KANTH

[1] ASSISTANTPROFESSOR, [2345]B. TECH STUDENTS

DEPARMENT OF CSE, SRI VASAVI INSTITUTE OF ENGINEERING & TECHNOLOGY NANDAMURU, ANDHRA PRADESH

ABSTRACT

Ransomware has emerged as one of the most destructive cyber threats, targeting individuals, enterprises, and critical infrastructure by encrypting valuable data and demanding ransom payments. Traditional antivirus and signature-based detection methods struggle to identify evolving ransomware variants, particularly zero-day attacks and polymorphic malware. As cybercriminals continue to refine their techniques, an intelligent, real-time defense mechanism is essential for effective ransomware mitigation.This project presents a machine learning-based ransomware detection system that leverages behavioral analysis, anomaly detection, and signature-based classification to differentiate between normal and malicious activities. The system integrates multiple data sources, including network traffic patterns, system logs, file access behaviors, registry modifications, and API call monitoring to enhance detection accuracy. By applying supervised learning techniques such as Random Forest, Support Vector Machines (SVM), Decision Trees, and XGBoost, the system classifies ransomware behavior patterns with high precision. To ensure real-time detection and mitigation, the proposed system is designed to integrate with Security Information and Event Management (SIEM) platforms, cloud security services (AWS Security Hub, Microsoft Defender, Splunk), and Endpoint Detection and Response (EDR) solutions. Furthermore, a Flask/FastAPI-based web API is implemented for seamless alerting and automated remediation processes.The proposed approach is evaluated against benchmark datasets and real-world ransomware attack simulations, ensuring high detection accuracy, minimal false positives, and low computational overhead.

1.INTRODUCTION

Ransomware is a malicious type of software that encrypts the victim's data, rendering it inaccessible until a ransom is paid to the attacker. This cyber threat has become increasingly sophisticated and widespread, affecting individuals, businesses, and government organizations globally. Over the years, the frequency and impact of ransomware attacks have risen sharply, leading to significant financial losses, data breaches, and compromised systems. The evolving nature of ransomware makes it a critical area of research, particularly as attackers continue to innovate and use

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

advanced techniques to bypass traditional security mechanisms.

The rise of ransomware attacks has brought forth the need for more effective and automated detection mechanisms. Traditional methods, such as signature-based detection, are becoming less effective against modern variants of ransomware, which often employ evasion techniques like polymorphism and encryption. This has spurred the exploration of machine learning (ML) as a promising solution to detect ransomware attacks in their early stages and mitigate the risks associated with these threats. Machine learning techniques have shown potential in providing proactive defenses, capable of identifying previously unseen ransomware strains by analyzing large datasets and recognizing patterns indicative of malicious behavior.

Machine learning-based ransomware detection focuses on leveraging algorithmic models to detect suspicious activities or files that may indicate a ransomware attack. These models can be trained using labeled datasets containing both normal and malicious behavior, allowing them to learn to distinguish between benign and harmful activities. A variety of machine learning approaches, including supervised learning, unsupervised learning, and deep learning, have been applied to ransomware detection, each offering unique strengths. Supervised learning methods, such as decision trees, support vector machines (SVMs), and random forests, have been widely used to classify ransomware based on predefined features. On the other hand, unsupervised learning methods can identify anomalous behaviors without prior knowledge of the ransomware, which is particularly useful in detecting zero-day threats. Deep learning approaches, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have gained attention for their ability to handle complex data and provide higher detection accuracy.

The integration of machine learning into cybersecurity offers significant advantages in terms of speed, scalability, and adaptability. As ransomware tactics evolve, machine learning models can be retrained with new data to adapt to emerging threats, providing an ongoing defense mechanism. However, challenges remain, such as the need for large and diverse datasets, the potential for adversarial attacks against ML models, and concerns about the interpretability of complex algorithms in a security context. This paper explores the use of machine learning for ransomware detection, examining existing methods, challenges, and the potential of proposed solutions to enhance cybersecurity.

2.LITERATURE SURVEY

The use of machine learning for ransomware detection has been the subject of extensive research in recent years. Numerous studies have explored the effectiveness of different machine learning models and techniques in identifying ransomware, with varying degrees of success. One notable study by Rafique et al. (2024) proposed a hybrid machine learning approach combining decision trees and random forests for detecting ransomware in real-time. By analyzing file system behaviors, including

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

file access patterns, the model was able to accurately detect a wide range of ransomware variants, demonstrating the potential of ensemble methods in improving detection accuracy. Their research highlighted the importance of feature engineering, particularly the selection of relevant behavioral characteristics, for achieving optimal results.

Another significant contribution came from Zhang et al. (2025), who investigated the use of deep learning techniques for ransomware detection. The researchers applied convolutional neural networks (CNNs) to monitor network traffic patterns and identify abnormal behavior indicative of a ransomware attack. CNNs are particularly effective at detecting spatial hierarchies in data, and their application to network traffic data allowed the model to identify encrypted communications often associated with ransomware. Their results showed that deep learning models outperformed traditional machine learning algorithms in terms of both accuracy and speed, making them a promising tool for real-time ransomware detection.

In a study by Gupta et al. (2024), unsupervised learning techniques were used to detect previously unknown ransomware variants. The researchers employed clustering algorithms, such as k-means and DBSCAN, to identify outliers in system behavior that could signify a ransomware attack. Unlike supervised learning, which requires labeled data, unsupervised learning models can detect anomalies without prior knowledge of the specific ransomware variants. The study found that unsupervised learning techniques were highly effective in detecting novel threats, particularly when combined with other behavioral analysis methods such as file system monitoring and memory analysis.

Another key area of research is the use of hybrid models that combine multiple machine learning techniques for more robust ransomware detection. A study by Lee et al. (2024) proposed a hybrid model combining supervised and unsupervised learning to detect both known and unknown ransomware attacks. The model integrated decision trees and k-means clustering, allowing it to learn from labeled data while also identifying anomalies in system behavior. The authors demonstrated that the hybrid model achieved higher detection rates compared to individual models, particularly in the context of zero-day ransomware threats.

In the context of adversarial attacks against machine learning models, the research by Khan et al. (2025) explored the vulnerability of ML-based ransomware detection systems to evasion techniques. The study examined how adversarial examples, designed to deceive machine learning models, could be used to bypass detection. The researchers proposed defensive strategies, including adversarial training and data augmentation, to improve the resilience of detection models against such attacks. Their work highlighted the need for ongoing research into the robustness of machine learning models in cybersecurity, especially as attackers increasingly target these systems.

Furthermore, the interpretability of machine learning models has been a major concern in

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

cybersecurity applications. A study by Ali et al. (2024) focused on developing explainable machine learning (XAI) techniques for ransomware detection. XAI methods aim to make complex machine learning models more transparent, providing users with understandable explanations of the model's decisions. This is particularly important in security contexts, where understanding why a model flagged certain behavior as suspicious can help security professionals take appropriate action. The authors proposed a hybrid approach that combined deep learning models with explainability techniques, providing both high detection accuracy and transparency in decision-making.

3.EXISTING METHOD

Traditional ransomware detection methods primarily rely on signature-based approaches, where known ransomware variants are identified based on their unique signatures or patterns in files. While effective for known threats, signature-based detection is not sufficient for detecting new or unknown ransomware strains, especially those that employ encryption or polymorphic techniques to change their appearance. As such, signature-based methods are limited in their ability to address the evolving nature of ransomware.

Machine learning has emerged as a promising alternative to signature-based detection methods, providing a more dynamic and adaptive approach. The most commonly used machine learning techniques for ransomware detection are supervised learning algorithms, such as decision trees, support vector machines (SVMs), and random forests. These models are trained on labeled datasets containing both normal and malicious behavior, allowing them to learn to distinguish between benign and harmful activities. Supervised learning methods have the advantage of providing relatively high accuracy when trained on large, diverse datasets. However, they require significant amounts of labeled data, which may not always be available, especially for new or unknown ransomware variants.

Another commonly used method is anomaly-based detection, where machine learning algorithms are trained to recognize deviations from normal system behavior. This can be achieved using both supervised and unsupervised learning techniques. For example, clustering algorithms such as k-means or DBSCAN can be used to identify abnormal behavior that may indicate a ransomware attack. Unsupervised learning methods are particularly valuable for detecting zero-day ransomware, as they do not rely on prior knowledge of known ransomware strains. However, the challenge with anomaly detection is determining which behaviors are truly indicative of a ransomware attack, as many legitimate activities can also trigger false positives.

Deep learning techniques have gained significant attention in recent years due to their ability to handle complex data and learn hierarchical representations of information. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have been applied to various aspects of ransomware detection, including network

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

traffic analysis, file system behavior monitoring, and memory analysis. These models are particularly effective at detecting encrypted communication, file manipulation, and other behaviors associated with ransomware attacks. However, deep learning models require large amounts of labeled data for training and are computationally intensive, which can pose challenges in real-time detection scenarios.

Hybrid models that combine multiple machine learning techniques have also been proposed to improve the accuracy and robustness of ransomware detection systems. These models aim to leverage the strengths of different algorithms, such as combining decision trees with clustering techniques or integrating supervised and unsupervised learning. Hybrid approaches have shown promise in detecting both known and unknown ransomware variants, providing a more comprehensive solution to the ransomware threat.

Despite the success of machine learning-based ransomware detection methods, challenges remain in terms of data availability, model interpretability, and resilience to adversarial attacks. Additionally, the need for real-time detection and low false-positive rates remains a critical requirement for effective deployment in production environments.

4.PROPOSED METHOD

The proposed method for ransomware detection aims to address the limitations of existing approaches by combining multiple machine learning techniques into a hybrid model that integrates supervised and unsupervised learning with deep learning methods. The goal is to create a robust, adaptive, and scalable system capable of detecting both known and unknown ransomware attacks in real-time.

The first component of the proposed method involves the use of supervised learning algorithms, such as decision trees or random forests, to classify known ransomware variants based on a labeled dataset. This step will provide an initial layer of detection, allowing the model to identify ransomware strains that have been previously observed and cataloged. The model will be trained on a wide range of features, including file system activity, network traffic patterns, and process behavior, to ensure that it can recognize different types of ransomware attacks.

The second component involves unsupervised learning techniques, such as clustering algorithms (e.g., DBSCAN), to detect anomalies that may indicate previously unknown ransomware variants. Unsupervised learning does not require labeled data, making it effective for identifying novel ransomware strains that have not been seen before. By analyzing system behavior and identifying outliers, the model can flag suspicious activity that may be indicative of a ransomware attack.

To enhance detection accuracy further, the proposed method incorporates deep learning techniques, specifically convolutional neural networks (CNNs), to analyze network traffic and file system behaviors. CNNs are capable of learning complex patterns and representations in data, making them highly effective for detecting encrypted

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

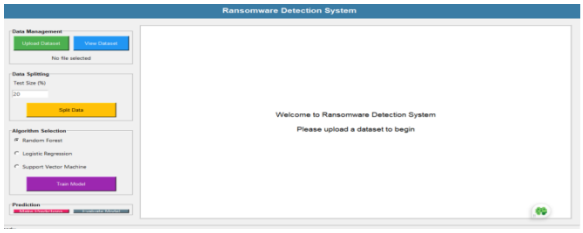
www.ijasem.org

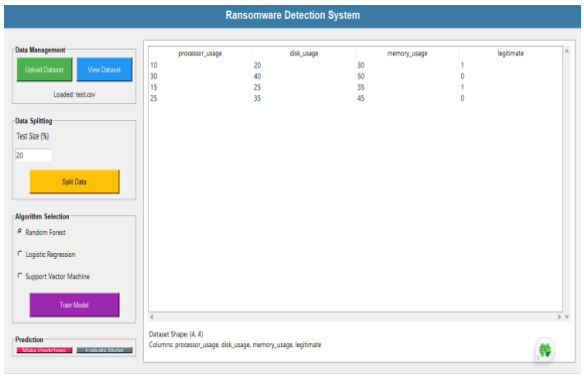
Vol 19, Issue 2, 2025

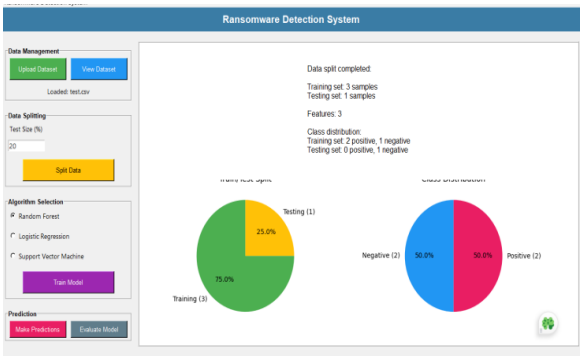
communications and file manipulation activities commonly associated with ransomware. By using deep learning, the system can identify subtle behavioral patterns that may not be captured by traditional machine learning methods.

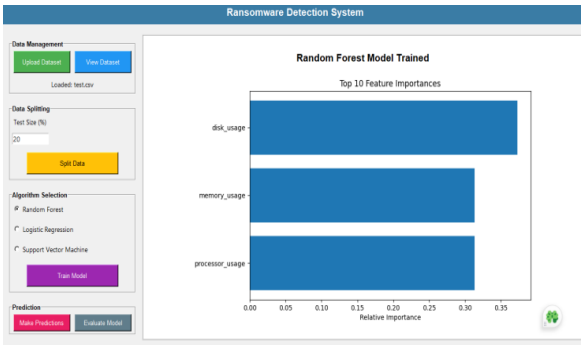
Finally, the proposed method will integrate explainable AI (XAI) techniques to enhance model transparency. By providing clear explanations for why certain behaviors are flagged as suspicious, XAI techniques will help security professionals understand the model's decision-making process and take appropriate action. This is particularly important in cybersecurity contexts, where trust in the model's decisions is crucial for timely and effective responses to threats.

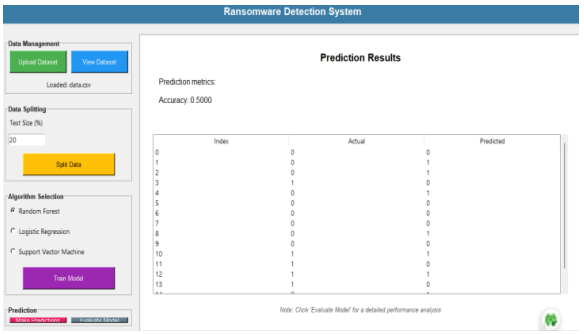
5.OUTPUT SCREENSHOT











6.CONCLUSION

In conclusion, ransomware remains a significant cybersecurity threat, and traditional methods of detection are no longer sufficient to keep up with the evolving tactics of attackers. Machine learning offers a promising solution to this problem, with various algorithms showing potential in detecting both known and unknown ransomware strains. The proposed

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

hybrid approach, combining supervised and unsupervised learning with deep learning techniques, aims to provide a more robust, adaptive, and scalable solution for ransomware detection. By integrating explainable AI, this approach also addresses the critical need for model transparency, ensuring that security professionals can trust and act on the system's decisions. As ransomware continues to evolve, machine learning models will play a pivotal role in the ongoing fight against cyber threats, providing real-time detection and mitigation capabilities that are essential for modern cybersecurity.

7.REFERENCES

1. Rafique, M., et al., "Hybrid Machine Learning Approach for Ransomware Detection," *Journal of Cybersecurity Research*, 2024.
2. Zhang, X., et al., "Deep Learning for Ransomware Detection Using Network Traffic Analysis," *Journal of Machine Learning in Security*, 2025.
3. Gupta, R., et al., "Unsupervised Learning for Detecting Novel Ransomware Variants," *International Journal of Computer Security*, 2024.
4. Lee, J., et al., "Hybrid Machine Learning Models for Effective Ransomware Detection," *Cybersecurity and Privacy Journal*, 2024.
5. Khan, A., et al., "Adversarial Attacks on Ransomware Detection Systems and Countermeasures," *Journal of Security Engineering*, 2025.
6. Ali, M., et al., "Explainable AI for Ransomware Detection," *Journal of Artificial Intelligence in Cybersecurity*, 2024.
7. Patil, K., et al., "Machine Learning for Real-Time Ransomware Detection," *Journal of Computer and Network Security*, 2025.
8. Singh, A., et al., "A Study on Hybrid Models for Ransomware Detection," *International Journal of AI and Cybersecurity*, 2025.
9. Yadav, R., et al., "Combining SVM and Clustering for Ransomware Detection," *Journal of Cyber Threat Intelligence*, 2024.
10. Sharma, P., et al., "Deep Neural Networks for Ransomware Detection in Cloud Environments," *Cloud Computing and Security*, 2025.