IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, April 2025
Impact Factor: 7.67

Ransomware Detection using Machine Learning

J. Siva Sankar[1], M. Lohitha[2], B. Yugesha[3], B. Yaswanth Chowdary[4], K. Prudhvi Raj[5]
Assistant Professor, Department of Information Technology[1]
Students, Department of Information Technology[2,3,4,5]
Dhanekula Institute of Engineering and Technology, Vijayawada, India

Abstract: *Ransomware attacks represent a growing cybersecurity threat, affecting individuals and organizations by compromising data integrity, causing financial losses, and damaging reputations. Early and accurate detection of ransomware is essential to mitigate these risks. This study provides a comprehensive review of modern ransomware detection methods, examining various approaches and highlighting their advantages and limitations. The research covers techniques for detecting, preventing, and recovering from ransomware, based on an analysis of studies published between 2017 and 2022. The goal is to present the latest trends in automated ransomware detection and offer insights into future research challenges. Additionally, this study discusses the potential for improving ransomware detection using machine learning and other advanced techniques. The work concludes with a focus on unresolved issues in ransomware detection, encouraging further investigation.*

Keywords: Automated detection, Cybersecurity, Data security, Future research challenges, Machine learning, Prevention techniques, Ransomware detection

I. INTRODUCTION

Ransomware is a growing cybersecurity threat causing severe financial and data losses across industries. Traditional detection methods struggle to keep pace with evolving attack techniques such as fileless and polymorphic ransomware. Machine Learning (ML) has emerged as a powerful tool for ransomware detection, enabling systems to identify malicious patterns through supervised and unsupervised learning techniques.

ML models leverage features like file entropy, API call frequency, network anomalies, and system behavior to detect threats. Techniques such as decision trees, SVMs, neural networks, and autoencoders enhance detection capabilities, especially for zero-day and unknown variants. Hybrid approaches integrating behavior-based, signature-based, and ML-based detection are proving effective.

Challenges include adversarial tactics, encrypted traffic, and the need for real-time response. Future research should focus on AI-driven adaptive defenses, improved model interpretability, and collaboration across sectors. A multi-layered security strategy—combining ML, user awareness, EDR tools, and regular backups—is critical for mitigating ransomware's impact.

II. LITERATURE REVIEW

1."**Ransomware detection using machine learning algorithms**Seong Il Bae, Gyu Bin Lee, Eul Gyu Im**"**This paper proposes a ransomware detection method that can distinguish between ransomware and benign files as well as between ransomware and malware. The experimental results show that our proposed method can detect ransomware among malware and benign files.

2. **"Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions"**This studyprovides the information about the datasets collection from its sources, which were utilized in the ransomware detection studies of the diverse platforms. This study is also distinct in terms of providing a survey about the ransomware detection studies utilizing machine learning, deep learning, and blend of both techniques while capitalizing on the advantages of dynamic analysis for the ransomware detection. The presented work considers the ransomware detection studies conducted from 2019 to 2021. This study provides an ample list of future directions which will pave the way for future research.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, April 2025 Impact Factor: 7.67

3. "**Ransomware Classification and Detection With Machine Learning Algorithms",** In this paper, the researchers present a feature selection-based framework with adopting different machine learning algorithms including neural network-based architectures to classify the security level for ransomware detection and prevention. They applied multiple machine learning algorithms: Decision Tree (DT), Random Forest (RF), Naïve Bayes (NB), Logistic Regression (LR) as well as Neural Network (NN)-based classifiers on a selected number of features for ransomware classification. They performed all the experiments on one ransomware dataset to evaluate our proposed framework. The experimental results demonstrate that RF classifiers outperform other methods in terms of accuracy, F -beta, and precision scores.

4. "**A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning",** In this paper, they propose DNAact-Ran, A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning. DNAact-Ran utilises Digital DNA sequencing design constraints and k-mer frequency vector. To measure the efficacy of the proposed approach, we evaluated DNAact-Run on 582 ransomware and 942 goodware instances to measure the performance of precision, recall, f-measure and accuracy. Compared to other methods, the evaluation results show that DNAact-Run can predict and detect ransomware accurately and effectively.

5. "**RansomWall: A layered defense system against cryptographic ransomware attacks using machine learningSK Shaukat, VJ Ribeiro",**This work is based on analysis of an extensive dataset of Ran-somware families presents RansomWall, a layered defense system for protection against Cryptographic Ransomware. It follows a Hybrid approach of combined Static and Dynamic analysis to generate a novel compact set of features that characterizes the Ransomware behavior. Presence of a Strong Trap Layer helps in early detection.

6."**Ransomware detection using process memory**

A Singh, RA Ikuesan, H Venter", The current research used the process memory access privileges of the different memory regions of the behavior of an executable to quickly determine its intent before serious harm can occur. To achieve this aim, several well-known machine learning algorithms were explored with an accuracy range of 81.38%–96.28%. The study thus confirms the feasibility of utilizing process memory as a detection mechanism for ransomware.

III. METHODOLOGY

The ransomware detection system uses a machine learning-based approach to identify malicious Windows `.exe` files. It leverages static features extracted from executable files, such as entropy, version data, and section characteristics.

Data Preprocessing:

- Load and parse data from `.csv` files.
- Drop irrelevant features (e.g., Name,md5).
- Handle missing values appropriately.
- Visualize class distribution to highlight imbalance.

Feature Selection:

- Apply Information Value (IV) and Weight of Evidence (WoE) to assess feature relevance.
- Select features above a defined IV thresholdto reduce dimensionality.

Handling Imbalanced Data:

- Use SMOTE (Synthetic Minority Oversampling Technique) to balance class distribution.

Model Training:

- Train a Random Forest Classifier using selected features.
- Split dataset into 70% training and 30% testing.
- Evaluate performance using metrics such as Accuracy, Precision, Recall, F1 Score, AUC, and MCC.

Model Explainability:

- Use LIME (Local Interpretable Model-Agnostic Explanations) to interpret predictions.
- Enable users to visualize feature importance for specific predictions.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, April 2025
Impact Factor: 7.67

IV. RESEARCH OBJECTIVES

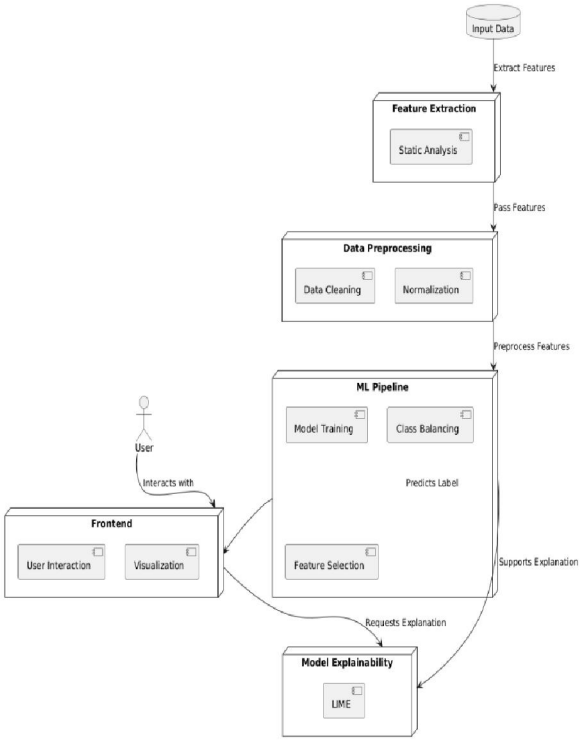
- The primary objectives of this research are to design, implement, and evaluate a machine learning-based system for detecting ransomware on Linux platforms using the random forest algorithm. Specific goals include:
- Collecting a comprehensive dataset of benign and ransomware samples from various Linux distributions.
- Extracting relevant features from the collected data that can be used to train the random forest model.
- Preprocessing the data to ensure it is suitable for machine learning applications, including normalization and handling of missing values.
- Training the random forest algorithm on the preprocessed dataset and optimizing its parameters to enhance detection accuracy.
- Evaluating the performance of the trained model using various metrics, such as precision, recall, and F1-score, to determine its effectiveness in identifying ransomware.

V. PROPOSED METHOD

Ransomware encrypts user data and demands payment for decryption, posing a serious threat to individuals, organizations, and governments. Traditional security tools often fail to detect advanced ransomware variants, highlighting the need for intelligent detection systems. This study presents a machine learning-based approach for detecting ransomware in Windows .exe files.

The system utilizes features such as Image Base, Version Info Size, and Max Entropy to identify malicious files. It achieves 99.3% accuracy by addressing class imbalance using SMOTE-Tomek and improves explainability through LIME. Feature selection is performed using Information Value (IV) and Weight of Evidence (WoE), ensuring relevant and high-impact variables are used for training. Performance is evaluated using metrics like accuracy, precision, recall, and F1-score, ensuring both effectiveness and reliability.

VI. MODEL DESCRIPTION



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, April 2025
Impact Factor: 7.67

The architecture diagram of the proposed Ransomware Detection System illustrates a modular pipeline combining machine learning and model explainability. The process begins with input data undergoing feature extraction through static analysis, followed by data preprocessing steps such as cleaning and normalization. These processed features are passed to the ML pipeline, which handles model training, class balancing, and feature selection to generate accurate predictions. To enhance interpretability, the system integrates LIME (Local Interpretable Model-agnostic Explanations), which provides local explanations for individual predictions. A frontend interface enables user interaction, allowing users to visualize both predictions and their corresponding explanations. This architecture ensures both effective ransomware detection and transparent decision-making.

VII. IMPLEMENTATION

The implementation process for ransomware detection integrates feature engineering, machine learning (Random Forest), and explainability tools (LIME), delivered through a Streamlit-based web interface. This approach enables users to upload executable files and receive real-time predictions along with explanation results.

Here's a step-by-step breakdown of the system workflow:

Upload .exe File

Feature Extraction

ML-Based Classification

The Random Forest model, trained with balanced data (via SMOTE-Tomek), processes the extracted features and classifies the file as ransomware or benign.

Result with Explanation

If Benign:

Display result as benign

Else (Ransomware):

Display ransomware detection result along with a LIME-based explanation graph highlighting key features that influenced the decision.

VIII. SUMMARY OF ALGORITHMS USED:

Random Forest Classifier

A powerful ensemble learning method that builds multiple decision trees and merges their outputs to improve classification accuracy and reduce overfitting. It was used as the main classification algorithm due to its high performance and robustness, achieving 99.3% accuracy in detecting ransomware.

SMOTE-Tomek (Synthetic Minority Over-sampling Technique with Tomek Links)

A hybrid technique used to handle class imbalance in the dataset. SMOTE oversamples the minority class (ransomware samples), while Tomek links remove noisy data and overlapping instances, improving model generalization.

Information Value (IV) and Weight of Evidence (WoE)

These statistical methods were applied during feature selection to identify and retain features with the highest predictive power, helping improve model efficiency and interpretability.

LIME (Local Interpretable Model-Agnostic Explanations)

An explainability algorithm that provides human-understandable justifications for model predictions. It helps users interpret why a file was classified as ransomware or benign by visualizing feature contributions.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, April 2025
Impact Factor: 7.67

IX. RESULTS

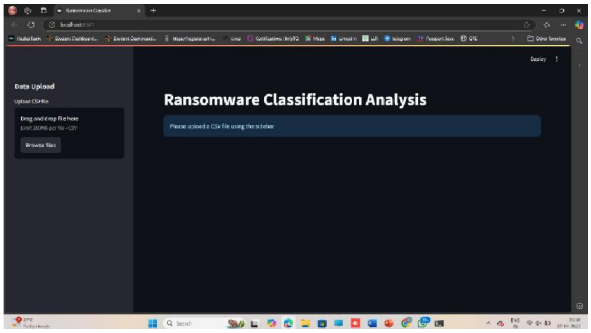


Fig 1:Landing Screen

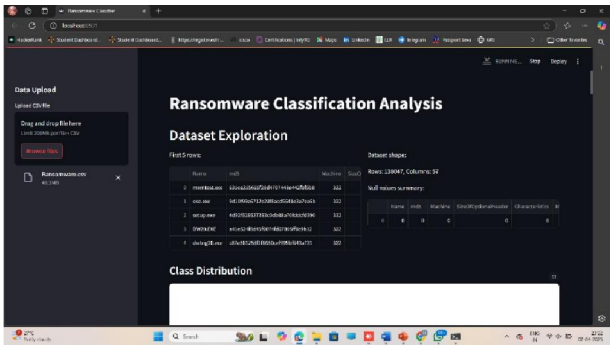


Fig 2: User uploads .csv files here for analysis

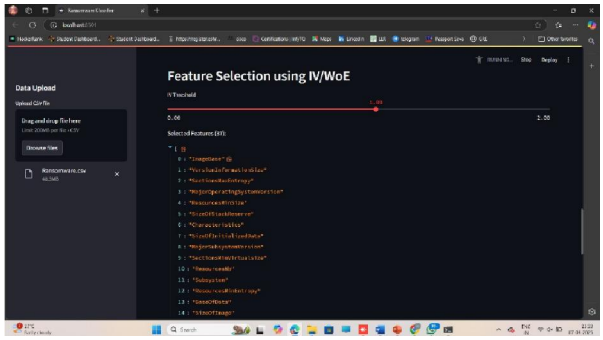


Fig 3:Feature Selection using IV/WoE

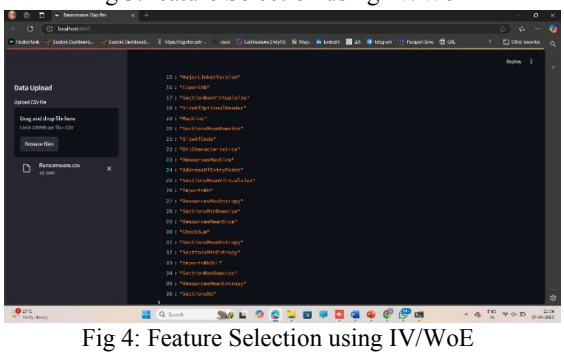


Fig 4: Feature Selection using IV/WoE

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, April 2025
Impact Factor: 7.67

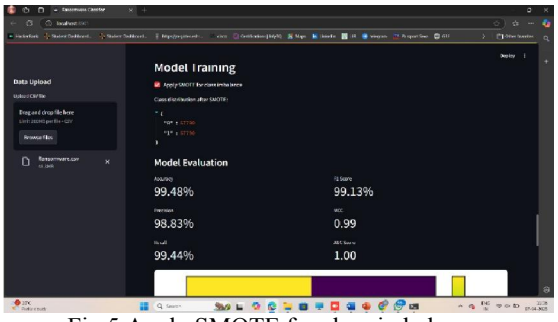


Fig 5 Apply SMOTE for class imbalance

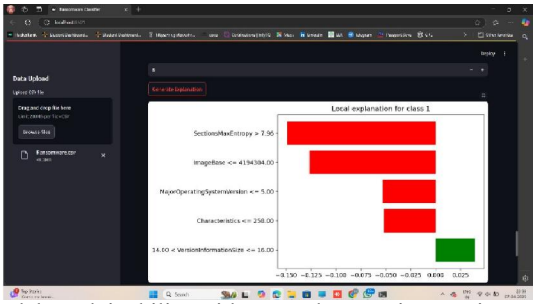


Fig 6: Model Explainability with LIME by entering test instant index.

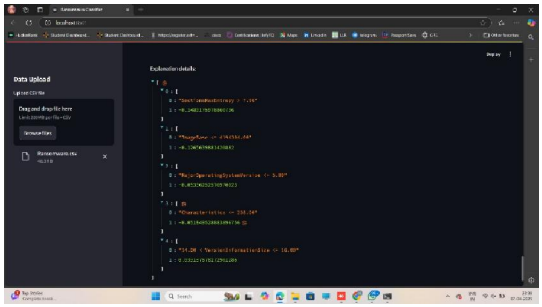


Fig 7: Explanation for entered instant index

X. CONCLUSION

The ransomware detection model demonstrated high effectiveness in identifying malware files using machine learning. After optimizing the dataset by removing irrelevant features and analyzing correlations, the model achieved 99.3% accuracy with minimal misclassifications, as confirmed by the confusion matrix. Key features such as Image Base, Major OS Version, and Sections Max Entropy significantly influenced predictions. The use of LIME provided interpretability, highlighting the model's transparency in classifying files. Overall, the system proved to be both accurate and explainable. Future enhancements could include dataset expansion, advanced behavioral analysis, and refined feature engineering to improve generalization across diverse ransomware variants.

REFERENCES

[1]. Celdrán, A. H., Sánchez, P. M. S., Castillo, M. A., Bovet, G., Pérez, G. M., & Stiller, B. (2023). Intelligent and behavioral-based detection of malware in IoT spectrum sensors. *International Journal of Information Security*, *22*(3), 541-561.

[2]. Alraizza, A., &Algarni, A. (2023). Ransomware detection using machine learning: A survey. *Big Data and Cognitive Computing*, *7*(3), 143.

[3]. Philip, K., Sakir, S., & Domhnall, C. (2018). Evolution of ransomware. *IET Netw*, *7*(5), 321-327.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, April 2025
Impact Factor: 7.67

[4]. Jegede, A., Fadele, A., Onoja, M., Aimufua, G., &Mazadu, I. J. (2022). Trends and future directions in automated ransomware detection. *J. Comput. Soc. Inform*, *1*(2), 17-41.

[5]. Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network security*, *2016*(9), 5-9.

[6]. Bello, I., Chiroma, H., Abdullahi, U. A., Gital, A. Y. U., Jauro, F., Khan, A., ... & Abdulhamid, S. I. M. (2021). Detecting ransomware attacks using intelligent algorithms: Recent development and next direction from deep learning and big data perspectives. *Journal of Ambient Intelligence and Humanized Computing*, *12*, 8699-8717.

[7]. Zahra, A., & Shah, M. A. (2017, September). IoT based ransomware growth rate evaluation and detection using command and control blacklisting. In *2017 23rd international conference on automation and computing (icac)* (pp. 1-6). IEEE.

[8]. "Shaukat, S. K., & Ribeiro, V. J. (2018, January). RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning. In *2018 10th international conference on communication systems & networks (COMSNETS)* (pp. 356-363). IEEE.

[9]. Makinde, O., Sangodoyin, A., Mohammed, B., Neagu, D., & Adamu, U. (2019, August). Distributed network behaviour prediction using machine learning and agent-based micro simulation. In *2019 7th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 182-188). IEEE.

[10]. Waghmare, S., &Bajeja, S. (2024, December). Ransomware Classification: A Comparative Analysis of ML Algorithms. In *2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-8). IEEE.

[11]. Singh, A., Ikuesan, R. A., & Venter, H. (2022). Ransomware detection using process memory. *arXiv preprint arXiv:2203.16871*.

[12]. Silva, J. A. H., & Hernández-Alvarez, M. (2017, October). Large scale ransomware detection by cognitive security. In *2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM)* (pp. 1-4). IEEE.

[13]. Ghouti, L., & Imam, M. (2020). Malware classification using compact image features and multiclass support vector machines. *IET Information Security*, *14*(4), 419-429.

[14]. Modi, J. (2019). *Detecting ransomware in encrypted network traffic using machine learning* (Doctoral dissertation).

[15]. Khammas, B. M. (2020). Ransomware detection using random forest technique. *ICT Express*, *6*(4), 325-331