**A System for Analyzing and Categorizing Ransomware Threats Using Machine Learning Techniques**

Harichandana Bethapudi1, Dhana Lakshmi Anke 2, Kiranmayee Sai Thammineni 3, Jahnavi Ediga 4, Snehalatha Mangapoti 5

1 Associate Professor, Dept. of CSE, Srinivasa Ramanujan Institute of Technology, Anantapur, India;

2,3,4,5. Dept. of CSE, Srinivasa Ramanujan Institute of Technology, Anantapur, India;

Email: harichandana.cse@srit.ac.in, 214g1a0519@srit.ac.in, 214g1a0544@srit.ac.in, 214g1a0539@srit.ac.in, 204g1a0598@srit.ac.in

**Abstract**

Ransomware attacks are among the most critical cybersecurity challenges today, as they compromise sensitive data and demand high ransoms for data recovery. Conventional detection methods based on signature matching often struggle to identify new and evolving ransomware strains. To address these challenges, a machine learning system has been developed to effectively evaluate and categorize ransomware threats. This methodology examines network behavior and tracks interactions with Command and Control (C&C) servers to identify malicious activities. By utilizing annotated datasets, the framework incorporates various machine learning techniques, such as Random Forest algorithm, Logistic Regression, and Support Vector Machines to differentiate between benign and ransomware activities. Random Forest algorithm exhibited superior performance, attaining an accuracy of 95.96%, using ANOVA-based feature selection improving its accuracy and interpretability. Additionally, the system provides a mechanism to classify ransomware into specific families, including previously unknown variants, enabling a proactive and robust defense against emerging threats.

**Keywords:** Ransomware, Random Forest Algorithm, Logistic Regression, Support Vector Machines.

**1. Introduction**

Ransomware is a major cybersecurity threat, increasingly using advanced methods to attack people, organizations, and governments. These malicious attacks encrypt sensitive data, making it completely inaccessible. A ransom, typically cryptocurrency, is then demanded for the data's release. IBM's 2023 cybersecurity report indicates an important increase in ransomware attacks and large financial losses resulting from these attacks during the last year. These attacks result in financial losses, functional disruptions, sensitive data breaches and reputational harm, causing important long-term economic consequences for victims [12].

Ransomware's ability to change considerably obstructs its prevention. Prominent modern ransomware groups, such as LockBit and BlackCat, now use several advanced evasion techniques, including highly effective domain generation algorithms (DGA), heavily encrypted communications and rapidly mutating polymorphic payloads. Advanced attackers can exploit several of these important features to readily circumvent many customary signature-based detection systems, consequently compromising a meaningful number of important vulnerabilities in even the strongest network infrastructures. The increasing complexity of ransomware points out the necessity of revolutionary and flexible security protocols.

Ransomware infections rely on command and control servers for remote control of infected systems so that attackers can issue commands and conduct malicious operations. These servers perform several key operations, including the exchanging of encryption keys, delivering the malicious payload, and exfiltration of data. Ransomware frequently avoids detection through some methods such as dynamically generated domain names and encrypted communication channels. These strategies obstruct identifying C&C activity. They also make intercepting this activity more challenging. Overcoming these meaningful obstacles requires a shift from static detection techniques to considerably more adaptive and dynamic approaches.

Machine learning provides an effective solution to address the limitations of traditional cybersecurity methods. Machine learning algorithms analyze many terabytes of network traffic data. These algorithms can detect subtle patterns and anomalies associated with ransomware. Highly advanced ML models offer considerably more proactive threat detection than conventional signature-based approaches because of their superior adaptability to new and evolving ransomware variants. Recent advances in machine learning have made it better to detect the latest ransomware variants. It has been quite effective against most modern cybersecurity threats [13].

This research introduces a detailed machine learning approach for detecting and classifying ransomware, utilizing Random Forest, SVM, and Logistic Regression classifiers. The framework analyzes network traffic attributes. These attributes include domain entropy, DNS query rate and packet size to distinguish benign from malicious activities. Its categorization of many ransomware families provides several deeper understandings of their behavioral patterns. By identifying the most important predictors, feature selection techniques achieve optimal model performance.

**2****. Literature Survey**

H. Daku et al. Performed a behavioral analysis of ransomware detection, reviewing 150 samples from 10 different families. The study identified 12 key features from an initial set of 27 attributes. By applying the J48 Decision Tree algorithm, the classification accuracy increased from 72.66% to 78%. However, Cerber ransomware exhibited only 50% accuracy, highlighting its advanced evasion techniques, and emphasizing the importance of integrating static and dynamic analysis for improved classification [1]. Y.-L. Wan et al. Proposed a flow-oriented ransomware detection method that utilized Biflow and Argus for packet preprocessing. Feature selection reduced the complexity of decision trees and enhanced accuracy. Using the J48 Decision Tree algorithm, the method effectively classified ransomware families like Locky and Cerber, demonstrating the critical role of feature selection in detection [2]. M. Saberi and F. Noorbehbahani investigated semi-supervised learning techniques for detecting ransomware, achieving improved results with family-specific datasets and feature selection using the wrapper method. The need for advanced techniques to address the limitations of supervised learning approaches was emphasized [3]. W. Cassel and N. E. Majd. Investigated machine learning techniques for classifying obfuscated ransomware, achieving 89.4% accuracy. Continuous updates to detection methods were identified as essential to combat evolving obfuscation techniques [4]. S. Poudyal, K. P. Subedi et al. Developed a multi-level machine learning model to analyze different sections of ransomware code. The model achieved classification accuracies ranging from 76% to 97% [5].

M. Aggarwal provided insights into ransomware groups such as LockBit, REvil, and Ryuk, which target sectors through infiltration, encryption, and ransom demands. Key defenses highlighted include regular updates, employee training, and data backups. In 2022, the U.S. experienced the highest number of ransomware attacks, with average ransom demands reaching $13.2 million [6]. A. Vehabovic, N. Ghani et al. Examined various ransomware detection methods, encompassing static and dynamic analysis, machine learning approaches, and binary code examination. Tools like UNVEIL and PAYBREAK monitor ransomware activity, while forensic methods aid in data recovery. The use of Bitcoin in ransom payments, sustaining further attacks, was also noted [7]. Chittooparambil, Helen Jose et al. Categorized ransomware into scareware, lock-screen ransomware, and crypto-ransomware. The paper outlined the operational stages of ransomware attacks, challenges in existing detection methods, and the need for early detection to minimize damage. Future research was recommended to improve understanding through controlled monitoring [8]. Masum, Mohammad et al. Evaluated machine learning classifiers for ransomware detection, identifying Random Forest as the most effective. Other classifiers examined included decision trees, Naive Bayes, and neural networks. The study emphasized robust classification techniques as a countermeasure against ransomware threats, supported by the United States National Science Foundation [9]. Alhawi, Omar MK et al. Introduced NetConverse, a system that attained a 97.1% true positive detection rate with the J48 classifier for identifying Windows ransomware through network traffic analysis. Data from nine ransomware families was analyzed using TShark and WEKA tools. [10]. The increasing cost of ransomware payouts and recovery in 2023 was highlighted, underscoring the urgency of improved detection and mitigation strategies [11].

**3. Proposed Methodology**

The suggested framework employs a machine learning-driven approach, incorporating SVM, Random Forest, and Logistic Regression models to classify network traffic into benign or ransomware categories. It leverages advanced feature selection techniques, such as KBest with ANOVA F-statistic, to identify significant network attributes, enabling efficient and accurate classification. The system demonstrates high accuracy in distinguishing ransomware families, including Rhysida, Play Ransomware, Akira, BlackCat, and LockBit.

To handle diverse datasets effectively, the system applies generalized preprocessing techniques to prepare network attributes for analysis. These steps include addressing inconsistencies, normalizing data, encoding features, and ensuring robust and reliable machine-learning performance across varied data inputs. This comprehensive approach enhances ransomware detection and classification, contributing to improved defenses against evolving threats.

Figure 1 depicts a supervised machine learning process, which starts with data input and preprocessing, and is followed by feature selection. Subsequently, the dataset is partitioned into training and evaluation sets. During training, algorithms like Random Forest, SVM, and Logistic Regression are applied. The testing stage emphasizes assessment, identification, and categorization to ensure precise predictions and optimal model performance.

A diagram of a software development process

Description automatically generated

Figure 1: Flowchart of Machine Learning Model Development

**Dataset Specification**

The dataset utilized in this study comprises labeled network traffic samples representing both benign and ransomware activities. It includes data collected from various ransomware families such as LockBit, BlackCat (ALPHV), Rhysida, Akira, and Play Ransomware. Each sample captures distinct communication patterns and network behaviors, focusing on Command and Control (C&C) server interactions. With 18 attributes, the dataset provides a diverse and detailed representation of network characteristics. This enables effective analysis to distinguish ransomware from benign traffic and classify it into specific families based on behavioral patterns. Figure 2 summarizes the dataset, highlighting the distribution of benign and ransomware samples across multiple classes, supporting effective multi-class classification.

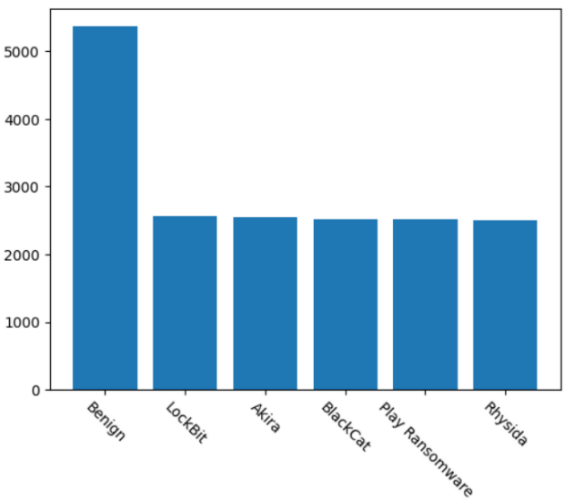
****

Figure 2: Distribution of Dataset Labels

**Preprocessing**

The preprocessing phase involved addressing categorical features and missing values to prepare the dataset for machine learning. Ordinal encoding was applied to non-numeric columns using scikit-learn's OrdinalEncoder, which converted categorical features into numeric values. The mappings between the original categorical values and their corresponding numeric representations were displayed to ensure transparency. Missing values were addressed by replacing categorical features with the most common value and numerical features with the mean, preserving data consistency. These preprocessing steps allowed machine learning algorithms to effectively process the data, preserve the original distribution, and maintain transparency throughout the encoding and imputation processes.

**Feature Selection**

Feature selection was performed using the SelectKBest method with the ANOVA (Analysis of Variance) F-statistic, a widely adopted technique for identifying the most relevant features in machine learning models. The ANOVA F-statistic evaluates the variance between different categories (such as benign files and ransomware) to determine the strength of each feature’s relationship with the target variable. Features with higher variance and greater significance are selected, ensuring that only the most informative attributes are retained for the model.

In this study, 12 out of the 18 available features were selected based on their statistical significance, allowing the system to focus on key attributes critical for ransomware detection, such as network behavior, file entropy, and encryption patterns. By prioritizing these essential features, the model achieves more accurate and interpretable results, ultimately improving its ability to detect and classify various ransomware families with greater precision.

Table 1: Key Features for Analysis and Classification

|  |  |
| --- | --- |
| **No** | **Features** |
| 1 | Domain Entropy |
| 2 | Vowel Ratio |
| 3 | Domain Length |
| 4 | Outbound Connections |
| 5 | Packet Size |
| 6 | Communication Time |
| 7 | Non-Standard Ports |
| 8 | Distinct IPs |
| 9 | TLS Validity |
| 10 | DNS Query Rate |
| 11 | User Agent |
| 12 | Exfiltration Indicator |

Table 1 shows the 12 most relevant features selected from 18 attributes using the SelectKBest method with the ANOVA F-statistic. These features, critical for effective ransomware detection, include network behavior, file entropy, and encryption patterns.

**Model Training and Evaluation**

This research assesses three machine learning models Random Forest, SVM, and Logistic Regression to classify ransomware threats and benign. The models received training on a specified dataset and were later assessed using a distinct test dataset. Their performance was assessed through key evaluation metrics to determine the most effective model for ransomware detection.

1. **Random Forest (RF):** Random Forest was opted for due to its effectiveness in handling sophisticated patterns by integrating multiple decision trees. It combines predictions from multiple trees to improve accuracy and minimize the likelihood of overfitting. Each decision tree learns from a randomly selected portion of the dataset, allowing the model to identify varied patterns and connections within the feature space. The trained model was evaluated using the test dataset, with its predictions analyzed against the actual labels to assess performance. Random Forest is known for its resilience against noisy data and its ability to identify feature importance, which helps in interpreting which factors contribute to the classification decision.
2. **Support Vector Machine (SVM):** It employs a linear kernel and was chosen for its effectiveness in handling multi-class classification problems. SVM works by finding the best decision boundary that maximizes the separation between different classes, effectively distinguishing benign files from various ransomware types. After training, the model's performance in classification was evaluated with the test dataset. Although SVM is designed for linearly separable data, it can handle more complex, non-linear relationships by using kernel functions, allowing it to adapt to higher-dimensional spaces.
3. **Logistic Regression:** Logistic Regression was employed as a foundational model given its straightforward nature and effectiveness in binary classification tasks. Despite being a linear model, To determine the likelihood of a threat being classified into a specific category, the model's effectiveness was evaluated using the dataset, serving as a reference point for comparing more advanced models. **While it may not capture complex non-linear relationships as effectively as more advanced techniques, Logistic Regression remains a valuable tool for understanding fundamental classification tasks and assessing the performance of more sophisticated models.**

Figure 3 depicts a ransomware detection using preprocessed network traffic data, selected features, and trained models (Random Forest, SVM, Logistic Regression) to predict and display ransomware types.

A diagram of a network traffic disaster

Description automatically generated

Figure 3: System Design for Ransomware Analysis and Classification

The ability of each model to classify ransomware threats was measured using essential evaluation criteria such as accuracy, precision, recall, and F1-score. These measures were derived from the test dataset to enable a comparative analysis of the models. The approach that best-balanced accurate ransomware detection and classification while minimizing incorrect positive and negative classifications was selected as the optimal solution.

1. **Accuracy:** Accuracy indicates how well the model correctly classifies instances, providing an overall measure of its reliability in making predictions.

Accuracy **=**

1. **Precision:** It measures how accurately the model identifies positive cases, reflecting its reliability in making positive predictions.

Precision =

1. **Recall:** Recall measures the model's ability to correctly identify all relevant instances within a dataset. It is calculated as the proportion of correctly predicted positive cases to the total number of actual positive instances.

Recall =

1. **F1-Score:** Calculated as the harmonic mean of precision and recall, the F1 score provides a comprehensive evaluation of both metrics. It is particularly useful in imbalanced datasets, where reducing incorrect positive and negative classifications is crucial.

F1-score =

**4. Results and Discussions**

The proposed system was assessed using three machine learning models such as Support Vector Machine (SVM), Random Forest (RF) and Logistic Regression. Among these, Random Forest exhibited optimal performance was attained with an accuracy of 95.96%, which highlights its resilience to noise and its capacity to manage complex patterns within the data. SVM exhibited strong performance with an accuracy of 92.13%, effectively separating classes using an optimal hyperplane, which proved beneficial for multi-class classification. Logistic Regression, serving as a baseline model, achieved an accuracy of 89.13%, but it was outperformed by RF and SVM, due to its limitations in capturing non-linear data relationships effectively.

Table 2: Evaluation Metrics of the Proposed ML Models

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Model | Accuracy | Precision | Recall | F1-Score |
| Random Forest | 95.96 | 95.97 | 95.96 | 95.96 |
| Support Vector Machines | 92.13 | 92.29 | 92.13 | 92.11 |
| Logistic Regression | 89.13 | 89.25 | 89.13 | 89.08 |

Table 2 shows Random Forest performed best with 95.96% accuracy, followed by Support Vector Machines at 92.13% and Logistic Regression at 89.13%.

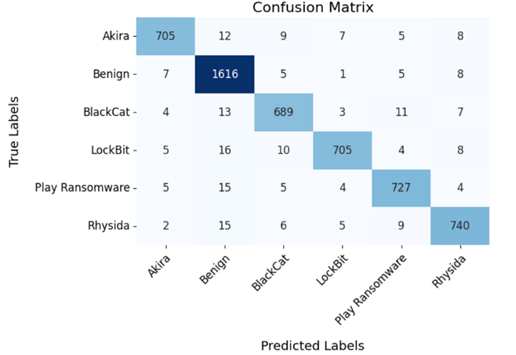


Figure 4: Random Forest Confusion Matrix

Figure 4 describes Confusion Matrix for the Random Forest Model, offering detailed insights into its classification performance. It displays the count of accurate and inaccurate predictions for each class, showcasing the model's capability to accurately differentiate between ransomware threats and benign. High values along the diagonal signify the model's proficiency in correctly predicting class labels, while minimal off-diagonal values indicate low misclassification rates. This highlights the strong effectiveness of the Random Forest model in detecting ransomware.

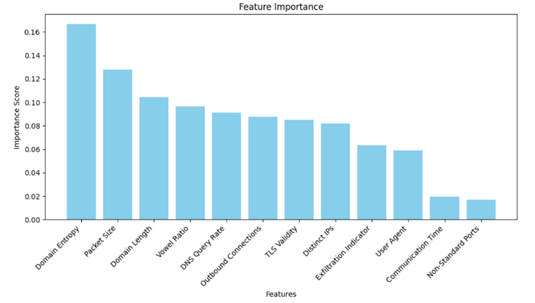


Figure 5: Ranking Key Features in Model Performance

The bar chart in Figure 5 illustrates the feature importance scores for the attributes used in the model. Feature importance measures the contribution of each feature to the model's predictive capability. Domain Entropy was identified as the most critical feature, with an score of 0.16. This indicates its strong influence in distinguishing patterns or anomalies within the data. Other notable features include DNS query rate, packet size, and outbound connections, all of Which significantly influence the model's decision-making process. Features such as domain length and vowel ratio also exhibit considerable importance, reflecting their relevance in capturing intricate patterns. Attributes like TLS Validity and Distinct IPs contribute moderately, while features such as Communication Time and Non-Standard Ports show lower importance, suggesting their relatively limited impact on model predictions. This evaluation emphasizes the effectiveness regarding chosen features contributing to model performance enhancement while also highlighting the need to prioritize features with higher importance scores for feature engineering and optimization efforts.

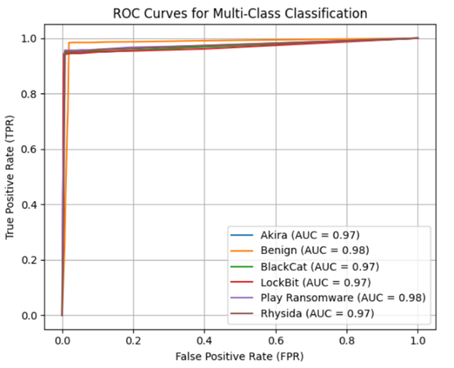


Figure 6: ROC Curve of Random Forest Classifier

Figure 6 illustrates the Receiver Operating Characteristic curve of Random Forest, which categorizes files into six groups: Akira, Benign, BlackCat, LockBit, Play Ransomware, and Rhysida. The values reflect the model's effective performance, with Benign and Play Ransomware achieving the highest value of 0.98. The other classes, Akira, BlackCat, LockBit, and Rhysida, achieved an AUC of 0.97. The ROC curves highlight the model's effectiveness in managing the trade-off between detection sensitivity and false alarms across different thresholds, emphasizing its effectiveness in distinguishing between the various categories.

**5. Conclusion**

The Random Forest-based framework demonstrates strong performance in detecting and classifying ransomware families while distinguishing them from benign files. Timely detection is vital for mitigating attacks and protecting critical systems. This research underscores machine learning's effectiveness in cybersecurity and its potential for future enhancements, including adaptability to new threats and real-world application integration.

**6. Acknowledgement**

The authors gratefully acknowledge the unwavering support and guidance provided by the faculty members of the Department of Computer Science and Engineering at Srinivasa Ramanujan Institute of Technology. Their expertise and encouragement have been instrumental in shaping this research. We also extend our heartfelt thanks to our fellow students who collaborated and contributed to this project, sharing their insights and efforts. Lastly, we appreciate the institution's administration for creating an environment that fosters academic excellence and innovation.

**7. References**

1. H.Daku, P. Zavarsky and Y. Malik, "Behavioral-Based Classification and Identification of Ransomware Variants Using Machine Learning," *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, USA, 2018, pp. 1560-1564, doi: 10.1109/TrustCom/BigDataSE.2018.00224.
2. Y. -L. Wan, J. -C. Chang, R. -J. Chen and S. -J. Wang, "Feature-Selection-Based Ransomware Detection with Machine Learning of Data Analysis," *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*, Nagoya, Japan, 2018, pp. 85-88, doi: 10.1109/CCOMS.2018.8463300.
3. F. Noorbehbahani and M. Saberi, "Ransomware Detection with Semi-Supervised Learning," *2020 10th International Conference on Computer and Knowledge Engineering (ICCKE)*, Mashhad, Iran, 2020, pp. 024-029, doi: 10.1109/ICCKE50421.2020.9303689.
4. W. Cassel and N. E. Majd, "Obfuscated Ransomware Family Classification Using Machine Learning," *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 2023, pp. 788-792, doi: 10.1109/CSCI62032.2023.00134.
5. S. Poudyal, K. P. Subedi and D. Dasgupta, "A Framework for Analyzing Ransomware using Machine Learning," *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, Bangalore, India, 2018, pp. 1692-1699, doi: 10.1109/SSCI.2018.8628743.
6. M. Aggarwal, "Ransomware Attack: An Evolving Targeted Threat," *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Delhi, India, 2023, pp. 1-7, doi: 10.1109/ICCCNT56998.2023.10308249.
7. A. Vehabovic, N. Ghani, E. Bou-Harb, J. Crichigno and A. Yayimli, "Ransomware Detection and Classification Strategies," *2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, Sofia, Bulgaria, 2022, pp. 316-324, doi: 10.1109/BlackSeaCom54372.2022.9858296.
8. Chittooparambil, Helen Jose, et al. "A review of ransomware families and detection methods." *Recent Trends in Data Science and Soft Computing: Proceedings of the 3rd International Conference of Reliable Information and Communication Technology (IRICT 2018)*. Springer International Publishing, 2019.
9. Masum, Mohammad, et al. "Ransomware classification and detection with machine learning algorithms." *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2022.
10. Alhawi, Omar MK, James Baldwin, and Ali Dehghantanha. "Leveraging machine learning techniques for windows ransomware network traffic detection." *Cyber threat intelligence* (2018): 93-106.
11. "Ransomware payouts and recovery costs went way up in 2023," *SC Media*.  
    Accessed: Jan. 3, 2025. [Online]. Available: <https://www.scworld.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023>.
12. IBM, *Cost of a Data Breach Report 2023*, IBM, Jul. 24, 2023. [Online]. Available: <https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs>.
13. J. Ispahany, M. R. Islam, M. Z. Islam and M. A. Khan, "Ransomware Detection Using Machine Learning: A Review, Research Limitations and Future Directions," in *IEEE Access*, vol. 12, pp. 68785-68813, 2024, doi: 10.1109/ACCESS.2024.3397921.