International Journal of Advancing Research, Innovation and Entrepreneurship

Vol 1(2), DOI:10.82036/0ped4684, July 2025 *ISSN:2977-9332*

An Enhanced Ransomware Detection Model using Machine Learning

[1]Badia Bello, * [1]Nurudeen Mahmud Ibrahim, [2] Kayode Ibrahim Adenuga & [3]John Temitope Ogbiti

[1] Faculty of Computing, Nile University of Nigeria, Abuja

[2]Centre for Research, Innovation, Development and Entrepreneurship (CRIDE), United Kingdom

[3]Department of Computer Science, Edo State University

*Corresponding Author Email address: balabadiya2@gmail.com

ABSTRACT

Ransomware attacks have emerged as a significant cyber security threat, targeting individuals, businesses, and critical infrastructure worldwide. To effectively combat this evolving menace, there is a critical need for advanced detection and mitigation strategies. In response, this paper proposes a ransomware detection system using a model that comprises Random Forest, SMOTE and Select K-Best feature selection to accurately identify ransomware based on their characteristics, behavior, and underlying mechanisms. Through feature extraction and selection, the system extracts discriminative features from ransomware samples, enabling the detection model to distinguish between benign and malicious software. Experimental evaluation demonstrates the efficacy and robustness of the proposed classification system in accurately categorizing ransomware and detecting emerging threats.

Keywords: *Cyber security, Ransomware, Detection, Machine Learning, Random Forest.*

1 INTRODUCTION

Ransomware has rapidly become one of the most widespread and damaging threats in today's cybersecurity landscape. It poses serious risks to individuals, businesses, and even critical infrastructure. This type of malicious software works by encrypting valuable files and demanding a ransom usually in cryptocurrency in exchange for the decryption keys. The impact can be devastating, often leading to major financial losses, operational shutdowns, damaged reputations, and compromised data integrity (Symantec, 2020).

What makes the situation even more concerning is the rapid emergence of new ransomware variants. These often come equipped with advanced evasion tactics such as obfuscation, polymorphism, and delayed execution which allow them to slip past traditional security tools with ease (Europol, 2021).

As ransomware attacks become more frequent and complex, there's a growing need for smarter detection systems that can not only catch known threats but also adapt to identify new ones. The standard signature-based security solutions are no longer sufficient, as they depend on predefined malware patterns that struggle to keep up with today's fast-evolving threats (McAfee Labs, 2019). In response, cybersecurity experts are turning toward behaviour-based and machine learning-driven approaches. These newer systems learn from past attacks and continuously improve their detection capabilities (Kaspersky, 2018).

Several important factors underline the need for an intelligent ransomware detection system:

A Diverse Threat Landscape: Ransomware is not a one-size-fits-all threat. There are countless families and variants, each with its own way of spreading, encrypting data, communicating with attackers, and avoiding detection. To effectively counter this diversity, we need a classification system that can recognise and interpret these differences, providing useful insights into how attacks operate.

Detection Difficulties: Many of today's ransomware variants are designed to morph or disguise themselves to avoid being picked up by traditional antivirus software. This makes static, signature-based detection unreliable. Instead, detection systems must look at how software behaves such as how it interacts with files, APIs, registries, and networks to spot malicious intent (IBM Security, 2020).

Targeted Mitigation: To defend against ransomware effectively, it's not enough just to detect it. Security systems also need to understand how a particular strain works. Knowing which methods an attack uses helps organisations deploy tailored defences, respond faster, and recover more efficiently (Cisco Talos, 2020).

Building Cyber Resilience: Protecting against ransomware is not just about reacting, but also about being prepared. Real-time detection and classification are key to strengthening a company's overall cybersecurity framework, enabling proactive and timely responses to both existing and emerging threats.

To meet these needs, this study proposes a ransomware detection system that combines machine learning with dynamic behavioural analysis and real-time monitoring. The

Vol 1(2), DOI:10.82036/0ped4684, July 2025 ISSN:2977-9332

system observes behaviours like file access, API calls, registry changes, and network activity to detect and classify ransomware accurately and efficiently (FireEye, 2019).

By using supervised and ensemble machine learning models, the system can generalise across multiple ransomware families, improving its ability to identify even previously unseen variants. Specifically, the model in this research integrates Random Forest, SMOTE (Synthetic Minority Oversampling Technique), and feature engineering, all supported by dynamic analysis within a sandbox environment. This setup allows for the collection of API-level behavioural data during the execution of ransomware samples, which is critical for accurate classification and early detection. Ultimately, the goal is to provide a scalable, adaptive defence that can keep up with the constantly evolving nature of ransomware.

The rest of this paper is structured as follows: **Section 2** provides a review of the relevant literature; **Section 3** describes the research methodology; **Section 4** presents and discusses the results; and **Section 5** concludes the study with key takeaways and future directions.

2 LITERATURE REVIEW / RELATED WORKS

Ransomware has become a serious threat to individuals, businesses, and governments, locking victims' files and demanding payment usually in cryptocurrency for their restoration. As ransomware continues to grow in sophistication, researchers have increasingly turned to machine learning (ML) methods to develop intelligent, adaptive detection systems capable of identifying both known and emerging variants.

A growing body of research has explored the use of machine learning for ransomware detection, applying both static and dynamic behavioural analysis to improve accuracy and counter advanced evasion techniques. For instance, Chen et al. (2021) developed an automated tool that analyses malware behaviour using TF-IDF, Fisher's Linear Discriminant Analysis (LDA), and Extremely Randomized Trees (ET). Their system extracts and visualises distinctive ransomware patterns from host logs collected in a sandbox environment. Experiments conducted on seven ransomware families including WannaCry and Cerber revealed that TF-IDF was most effective for feature extraction, while ET achieved the best results in early-stage detection.

Similarly, Hirano and Kobayashi (2021) proposed a live-forensic hypervisor that monitors low-level memory access patterns instead of relying on conventional API calls or process identifiers. This approach proved to be both lightweight and highly accurate, achieving an F1-score of 0.95, particularly effective against polymorphic and evasive ransomware variants.

In another study, Kunku, Zaman, and Roy (2023) introduced a machine learning-based framework using XGBoost and Random Forest classifiers to analyse ransomware behaviour and classify various families based on extracted features. Their models achieved high accuracy, offering a promising method for real-time threat detection and response.

Ahmed, Lin, and Srivastava (2022) further investigated ensemble learning techniques by combining both static and dynamic attributes such as permissions, system calls, and memory usage—to address ransomware evasion strategies. Kok, Abdullah, and Jhanjhi (2022) presented a hybrid model trained on Android malware datasets that effectively identified previously unknown ransomware variants, highlighting the value of incorporating multiple feature domains.

Another significant contribution came from the development of the Pre-Encryption Detection Algorithm (PEDA), which focused on identifying ransomware prior to the start of encryption. This model utilised API call signatures and SHA-256 hashes, achieving a 100% recall rate in detecting crypto-ransomware during its pre-encryption stage, thus enabling proactive mitigation.

To address the limitations of dynamic detection methods, Hirano, Hodota, and Kobayashi (2022) introduced the RANSAP dataset, a publicly available collection of storage access patterns from both ransomware and legitimate software. Built using a hypervisor-based monitoring system, this dataset enables realistic training and evaluation of detection models in real-world environments.

On the static analysis front, Medhat, Gaber, and Abdelbaki (2018) proposed a rule-based framework that applied logical operations and thresholds to statically extracted features. Their approach proved successful in detecting new ransomware families with high confidence. In a related study, Alhawi, Baldwin, and Dehghantanha (2018) developed a network-based machine learning framework that analysed conversation-level traffic in Windows environments. By applying a Decision Tree (J48) classifier to network data, their system achieved a true positive rate of 97.1%, demonstrating the potential of network traffic analysis in ransomware detection.

Exploring unsupervised techniques, Haider et al. (2018) employed clustering algorithms such as K-Means and DBSCAN to detect unknown ransomware variants. Their method effectively identified malicious behavioural patterns without relying on labelled datasets, showing promise for uncovering zero-day threats.

In a comprehensive study, Masum et al. (2022) evaluated traditional ML classifiers—including Decision Tree, Random Forest, Naïve Bayes, and Logistic Regression—alongside deep learning models such as LSTM and DNN. While these approaches demonstrated potential, the study also highlighted limitations in classifier performance, particularly in distinguishing between different ransomware types. The authors emphasized that the effectiveness of ML models is often constrained by the sophistication of the ransomware under analysis.

Vol 1(2), DOI:10.82036/0ped4684, July 2025 ISSN:2977-9332

Similarly, Bhaldar et al. (2023) used Decision Tree, Random Forest, and XGBoost classifiers in their research. Among them, Random Forest emerged as the most effective, achieving the highest accuracy, precision, and F1-score. Despite these positive results, the authors acknowledged that conventional anti-ransomware tools still struggle with newer, more complex threats, reinforcing the need for continued innovation.

Chamupathi et al. (2023) conducted a broad review of ransomware detection methodologies, finding that ML-based systems especially those using CF-NCF for feature vector generation were particularly effective. They also evaluated honeypots and network analysis techniques, concluding these approaches outperformed traditional key-backup strategies in combatting ransomware.

In another study, Tezcan (2024) examined ransomware detection through the lens of regression-based ML systems. The research introduced a hybrid algorithm combining regression and rule-based models to improve detection robustness. However, the study also noted challenges, such as algorithm bias, overfitting, and the need for careful model selection. Tezcan emphasized the importance of integrating both static and dynamic analysis to improve detection accuracy, particularly for encrypted or multi-stage ransomware.

Nagar (2024) detailed the evolving tactics of ransomware, noting a shift from basic encryption techniques to more advanced strategies such as obfuscation, sandbox evasion, and double extortion. His review, which includes modern ransomware strains like Cerber and Maze, stressed the need for advanced detection tools and highlighted the role of additional security layers like multi-factor authentication (MFA) in reducing risk.

Taking a different angle, Jun et al. (2024) focused on real-time detection using system call patterns. By analysing system call logs with regular expressions and finite state machines (FSMs), they developed a highly explainable real-time detection system. Although the approach was effective, the authors noted challenges such as long analysis times and potential overfitting due to small sample sizes.

Despite these advancements, several challenges persist. Studies by Masum et al. (2022) and Tezcan (2024) stress the limitations of current ML classifiers, particularly when dealing with highly sophisticated ransomware that leverages advanced evasion techniques. Additionally, Tezcan et al. (2024) pointed out the high cost and complexity of behavioural analysis setups, as well as the limitations of static analysis in detecting encrypted ransomware.

Looking forward, future research should prioritise hybrid detection models that combine static, dynamic, and real-time analysis techniques to enhance overall detection capabilities. Furthermore, addressing the existing weaknesses in ML algorithms such as bias, overfitting, and limited generalisability will be crucial in developing more resilient and effective ransomware prevention systems.

3 METHODOLOGY

This section describes the strategy employed to meet the research objectives for this study. This approach focuses on data gathering, model choice, preprocessing, model creation, training, and evaluation and the main objective is to establish a reliable machine learning model that can effectively differentiate between benign files and ransomware. We chose Random Forest classifier due to its high precison, competence and strength in managing high-dimensional data making it particularly fit for the ransomware detection. Thus, comparing with traditional signature-based methods, Random Forest offers adaptability and scalability, which are crucial in addressing the ever-evolving threat landscape. The suggested model consists of three interconnected components: the Random Forest classifier, the Synthetic Minority Oversampling Technique (SMOTE) to tackle class imbalance, and SelectKBest for feature selection. Therefore, combining these three elements - classification, oversampling, and optimal feature selection would enhance the originality of this research, providing a thorough and flexible solution for ransomware detection.

3.1 DATA COLLECTION

The dataset in Table I includes benign and ransomware files from the Kaggle ransomware dataset. Extracted features include metadata like FileName, md5Hash, Machine, and DebugSize.

TABLE I: DATASET ATTRIBUTES

Feature	Description
md5Hash	MD5 hash of the file.
DebugSize	Size of debugging information.
DebugRVA	Relative Virtual Address (RVA) of debugging info.
ExportRVA	RVA of the export directory.
ExportSize	Size of the export directory.
IatRVA	Import Address Table RVA.
MajorLinkerVersion	Major version of the linker.
MinorLinkerVersion	Minor version of the linker.
NumberOfSections	Number of sections in the executable.
SizeOfStackReserve	Reserved stack size for the application.
DllCharacteristics	Characteristics of the DLL file.
ResourceSize	Total size of resources in the file.
BitcoinAddresses	Presence of Bitcoin addresses in the file.
label	Classification label indicating benign (0) or ransomware (1).

3.2 PREPROCESSING

The pre-processing phase comprised several essential steps aimed at preparing the data for efficient training and evaluation:

i. Label Encoding: The target labels were transformed from categorical values to numerical representations through label encoding to ensure compatibility with machine learning algorithms.
ii. Feature Selection: To diminish dimensionality and enhance model performance, the SelectKBest

Vol 1(2), DOI:10.82036/0ped4684, July 2025 ISSN:2977-9332

method was utilized to identify the top 10 most significant features based on their statistical importance.

iii. Handling Class Imbalance: To tackle the issue of class imbalance, the Synthetic Minority Over-sampling Technique (SMOTE) was employed to create synthetic samples of the minority class, resulting in a balanced distribution across all classes.

Model Training and Evaluation

i. Data Splitting: The dataset was partitioned into training and testing subsets, with 80% allocated for training the model and 20% designated for assessing its performance.
ii. Feature Scaling: The features from the training and testing sets were standardized using the StandardScaler to normalize the data and facilitate the convergence of the learning algorithm.
iii. Model Training: A Random Forest classifier was trained on the scaled training dataset. This ensemble technique merges multiple decision trees to improve prediction accuracy and mitigate overfitting.
iv. Evaluation: The model's performance was evaluated using conventional classification metrics, including precision, recall, F1-score, and the confusion matrix, to assess prediction accuracy and the capability to differentiate between classes.

Key Libraries:

i. pandas: Data manipulation and analysis.
ii. sklearn.model_selection: Data processing.
iii. joblib: Efficient serialization of models.

4 RESULTS AND DISCUSSION

Evaluating the performance of a machine learning model is essential to understand its effectiveness in a classification task. For the Random Forest classification system developed in this study, several key metrics were used to quantify its performance. Below is a detailed discussion of the most used evaluation metrics:

Accuracy: Accuracy measures the proportion of correctly classified instances out of the total number of instances. Accuracy provides an overall measure of the model's correctness. However, it may be misleading for imbalanced datasets, as it does not account for the distribution of classes. The formula for accuracy is shown below:

Precision: Precision quantifies the proportion of true positive predictions out of all the positive predictions made by the model. Precision is crucial when the cost of false positives is high, indicating how accurate the positive predictions are. The formula for accuracy is shown below:

Recall (Sensitivity): Recall measures the proportion of true positive predictions out of all actual positive instances in the dataset. Recall is particularly important when the cost of false negatives is high, reflecting the model's ability to identify all positive instances.

F1-Score: The F1-score is the harmonic mean of precision and recall, providing a balanced metric that considers both false positives and false negatives.

4.2 ANALYSIS

The evaluation results as shown in Table II and Figure 1 indicate that the proposed model performs exceptionally well in classifying both normal and ransomware files. With 100% precision for normal files and 99% for ransomware, the model is highly accurate in its positive predictions, minimizing false alarms. The recall rates, at 99% for normal and 100% for ransomware, show that the model effectively identifies nearly all actual instances of each class. The consistent F1-Scores of 99% for both categories reflect a well-balanced model that excels in both precision and recall. Overall, the model demonstrates high reliability and effectiveness in distinguishing between benign and ransomware files.

TABLE II: CLASSIFICATION RESULT

	Benign	Ransomware
Precision	100%	99%
Recall	99%	100%
F1-Score	99%	99%

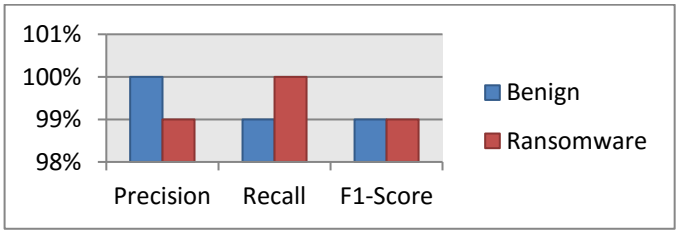


Figure 1: Classification Result

5 CONCLUSION

This work successfully developed a model to distinguish between benign files and ransomware with high accuracy. Through careful model selection, preprocessing, and evaluation, the classifier achieved exceptional precision, recall, and F1-scores, ensuring reliable detection. The system's effectiveness in handling high-dimensional data and providing interpretable results highlights its potential for real-world applications in cyber security. The results demonstrate the model's capability to minimize both false positives and false negatives, making it a valuable tool for ransomware detection. Future work could explore additional features and models to further enhance detection capabilities.

Vol 1(2), DOI:10.82036/0ped4684, July 2025 ISSN:2977-9332

6 REFERENCES

Symantec. (2020). *The evolution of ransomware: How to prepare for the next wave*.

Europol. (2021). *Internet organized crimethreat assessment (IOCTA) 2021*. Europol.

McAfee Labs. (2019). *Threats report: November 2019*.

Kaspersky. (2018). *The future of ransomware*.

Trend Micro. (2021). *Ransomware variants and trends*.

IBM Security. (2020). *2020 X-Force threat intelligence index*.

Fortinet. (2019). *Understanding ransomware and its behavioral patterns*.

Cisco Talos. (2020). *Ransomware resilience and response*.

FireEye. (2019). *Ransomware protection and containment strategies*.

Masum, M., Faruk, M. J. H., Shahriar, H., Qian, K., Lo, D., & Adnan, M. I. (2022). Ransomware classification and detection with machine learning algorithms. *arXiv preprint*, arXiv:2207.00894.

Bhaldar, A., & Manjara, S. (2023). Ransomware detection system using machine learning algorithms. *International Journal of Innovative Research in Science, Engineering and Technology, 12*(4).

Chamupathi, R., & Dhanasekaran, R. (2023). A survey on detection & prevention methods of ransomware in cybersecurity. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9*(3).

Tezcan, S. (2024). Towards real-time and lightweight ransomware detection using machine learning. *arXiv preprint*, arXiv:2408.16515.

Nagar, S. (2024). *Ransomware trends*. Red Canary Threat Detection Report.

Jun, S., & Singh, A. (2024). Ransomware detection using portable executable imports. In *Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS 2024)*.

Haider, W., Hu, J., & Slay, J. (2018). Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. *Journal of Network and Computer Applications, 87*, 185–192.

Alhawi, O. M. K., Baldwin, J., & Dehghantanha, A. (2018). Leveraging machine learning techniques for Windows ransomware network traffic detection. In *Cyber Threat Intelligence* (pp. 93–106).

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.

Medhat, M., Gaber, S., & Abdelbaki, N. (2018). A new static-based framework for ransomware detection. In *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing (DASC), Pervasive Intelligence and Computing, Big Data Intelligence and Computing, and Cyber Science and Technology Congress (Cyber-SciTech)* (pp. 833–840). IEEE.