Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 8s (2025)

Analysis of Ransomware Attack Detection Using Machine Learning Algorithms

B. M. Bandgar[1]*, Abhijeet Mote[2]
[1]Associte Professor. Sri Balaji University Pune, School of Computer Studies, Maharashtra, India (Pin-411033)
Email: bapuraob@yahoo.com* (Corresponding Author)
[2]Sr.Associate, Mountain Digitals Texas, USA.

Article History:

Received: *11-11-2024*

Revised:*24-12-2024*

Accepted:*09-01-2025*

Abstract:

Ransomware is one of the most prevalent and damaging forms of cyberattacks, causing substantial losses to organizations worldwide. The increasing sophistication of ransomware demands advanced detection techniques to identify and mitigate potential threats. This research explores machine learning models, including Random Forest, Gradient Boosting Machines (GBM), and Logistic Regression, to enhance ransomware attack detection. The study analyzes their performance using metrics such as precision, recall, and cross-validation accuracy. This paper aims to demonstrate the efficacy of machine learning in ransomware detection and provide a comparative analysis of these algorithms, identifying potential areas for future improvements. This document includes an overview of ransomware, a timeline of assaults, and details on their background. It also provides comprehensive research on existing methods for identifying, avoiding, minimizing, and recovering from ransomware attacks. In conclusion, this research highlights unanswered concerns and potential research challenges in ransomware detection.

Keywords: cyberattack, ransomware,machine learning.

1. Introduction

Current ransomware detection methods relying on predefined signatures are inadequate against evolving ransomware variants, creating a need for advanced, real-time detection techniques capable of identifying both known and unknown threats.

Ransomware attacks have escalated into one of the most pervasive and damaging cyber threats worldwide, targeting individuals, businesses, and even critical infrastructure. Traditional signature-based detection methods are insufficient to combat the rapidly evolving nature of ransomware, particularly with the emergence of polymorphic and zero-day ransomware variants. These conventional approaches fail to detect new strains, leaving systems vulnerable to attack. The challenge lies in developing more advanced detection techniques that can identify both known and unknown ransomware variants in real-time, without relying on predefined signatures. Machine learning has emerged as a promising solution for ransomware detection, as it can learn from data and detect previously unseen patterns.

Scareware manipulates its victims by tricking them into believing that their systems have been compromised and offering a fake solution in the form of antivirus software, which is controlled by the attacker. Many unsuspecting users fall prey to this tactic and purchase the fraudulent antivirus software

due to the frequent appearance of scareware warnings [5]. Human-operated malware and fileless ransomware are different from traditional ransomware.

Cybercriminals use human-operated ransomware to infiltrate networks or cloud systems, escalate privileges, and launch attacks on sensitive data. Instead of attacking a single machine, these attacks target entire organizations. The attackers typically gain access to an organization's IT infrastructure, move laterally through systems, and exploit vulnerabilities caused by poor security settings. Ultimately, unauthorized access to privileged accounts leads to ransomware attacks on critical IT systems, which support essential business functions [3,4]. Figure 4 shows a visual depiction of scareware, a type of malware that is becoming increasingly common in cyberattacks [4].

File less ransomware, on the other hand, uses legitimate, built-in system tools to launch its attack. This type of ransomware is harder to detect because no malicious code is installed on the victim's machine. As a result, anti-ransomware software cannot trace suspicious files during the attack. Depending on the attacker's goals, both file-based and human-operated ransomware can encrypt, lock, or exfiltrate data from systems [2]. Ransomware presents a significant risk to an organization's data and systems. Infected files or compromised devices are rendered inaccessible until a ransom—usually paid in Bitcoin—is received. In many cases, even after payment, the attackers withhold the decryption key. Some victims attempt to use the attacker-provided key to decrypt their files, which can further corrupt the data on the system [2,3].

However, the effectiveness of different machine learning models in identifying ransomware attacks varies, and there is a need for comprehensive research to evaluate and compare the performance of these models. This research paper addresses this gap by exploring the effectiveness of three machine learning models—Random Forest, Gradient Boosting Machines (GBM), and Logistic Regression—in detecting ransomware attacks. The study aims to compare these models in terms of accuracy, precision, recall, and their ability to generalize and Logistic Regression—in detecting ransomware attacks. The study aims to compare these models in terms of accuracy, precision, recall, and their ability to generalize to new ransomware variants. The research will provide insights into the strengths and weaknesses of each model, contributing to the development of more robust and efficient ransomware detection systems.

Advances in technology, such as ransomware development kits, ransomware-as-a-service, and cryptocurrencies like Bitcoin, have fuelled the continued increase in ransomware attacks on personal computers, networks, and mobile devices [2]. These ransomware attacks cost businesses and individuals hundreds of millions of dollars every year [3]. The profitability of ransomware for cybercriminals has led to the continual creation of new malware strains. Since 2013, numerous variants of ransomware have emerged. Therefore, more advanced and reliable techniques are required to detect, prevent, and counter these attacks. Traditional antivirus software and intrusion detection systems are often ineffective against newer ransomware strains. Individuals and organizations suffer significant financial damage as a result of ransomware attacks. The encryption of files or devices until a ransom is paid can lead to the irreversible loss of valuable data, resulting in serious consequences for both individuals and companies. Even after the ransom is paid, the decryption key is often not provided, causing additional harm to the system's stored files during decryption attempts by the attackers [1,6].

Advances in technology, such as ransomware development kits, ransomware-as-a-service, and cryptocurrencies like Bitcoin, have fuelled the continued increase in ransomware attacks on personal computers, networks, and mobile devices [2]. These ransomware attacks cost businesses and individuals hundreds of millions of dollars every year [3]. The profitability of ransomware for cybercriminals has led to the continual creation of new malware strains. Since 2013, numerous variants of ransomware have emerged. Therefore, more advanced and reliable techniques are required to detect, prevent, and counter these attacks. Traditional antivirus software and intrusion detection systems are often ineffective against newer ransomware strains. Individuals and organizations suffer significant financial damage as a result of ransomware attacks. The encryption of files or devices until a ransom is paid can lead to the irreversible loss of valuable data, resulting in serious consequences for both individuals and companies. Even after the ransom is paid, the decryption key is often not provided, causing additional harm to the system's stored files during decryption attempts by the attackers [1,6].

Scareware preys on its victims by informing them that their machines have been hijacked and promising to eradicate the ransomware using a false antivirus program backed by the attacker. Numerous innocent consumers buy and install fake antivirus software due to scareware alerts' frequent appearance [5]. Human-operated malware and ransomware without data are different from ransomware. Cybercriminals also employ human-operated ransomware to break into networks or cloud infrastructure, carry out privilege escalation, and launch attacks on sensitive data. Instead of simply one system, the attack actively targets an entire organization. Attackers typically access a whole IT system, move laterally, and exploit flaws via improper security configurations. Ultimately, unauthorized access to privileged user credentials leads to ransomware assaults on IT systems that enable crucial corporate activities [3,4]. Figure 4 provides a visual representation of scareware, a form of malicious software that is becoming increasingly prevalent in cyberattacks [4]. However, ransomware without files uses a native and reliable system to launch attacks. It is difficult to identify the attack because no code needs to be placed on the victim's machine for it to work. As a result, anti-ransomware technologies do not find any suspicious files to trace during an attack. Depending on the attacker's intentions, file-based and human-operated ransomware can encrypt, lock, or leak data from files [2]. Ransomware poses a danger to businesses' technology and files. Until the ransom is paid, typically with Bitcoin, infected files or compromised devices are locked out of reach. The decryption key is frequently withheld even after a victim pays the ransom the hackers want. They periodically try to use the attacker's key to decrypt the data, which damages the system's stored files. Technology advancements such as ransomware development kits, ransomware-as-a-service, and bitcoins are to blame for the ongoing rise in ransomware attacks on desktop PCs, networks, and mobile devices [2]. Attacks using ransomware cost businesses and individuals hundreds of millions yearly [3]. New types of malware are continually being created thanks to the enormous cash benefits that hackers gain from ransomware assaults. Since 2013, numerous ransomware variants have appeared. Therefore, new, effective, and reliable techniques are needed to detect, prevent, and mitigate ransomware attacks. Different ransomware strains cannot be created using conventional antivirus software or other intrusion-detection systems. People and companies experience significant financial losses as a result of ransomware attacks. The encryption of files or devices until a ransom is paid can result in the permanent loss of important data, which can have severe consequences for individuals and businesses alike. Even after the ransom is paid, the decryption key is often withheld, causing additional damage

to the system's stored files when attackers attempt to decrypt the data [1,6]. An analysis of studies between 2017 and 2024 is another advantage of this research. This provides readers with up-to-date knowledge of the most recent developments in ransomware detection and highlights advancements in methods for combating ransomware attacks.

2. Literature Review

AUTHORS	***PAPER TITLE & YEAR***	***WORK DONE***	***FUTURE SCOPE***	***LIMITATIONS***
Kumar and Singh.*[ ]*	Logistic Regression for Real-Time Ransomware Detection (2023)	Used Logistic Regression for real-time ransomware detection, with an accuracy of 84.5%, focusing on quick, interpretable results	Apply feature selection and dimensionality reduction techniques to improve performance and reduce false positives	Limited accuracy and scalability in complex environments with advanced ransomware attacks.
James and Li	Hybrid Machine Learning Model for Enhanced Ransomware Detection (2022)	Proposed a hybrid model combining Gradient Boosting and SVM, achieving 99.4% accuracy, emphasizing feature interaction.	Investigate real-time detection and response strategies using hybrid models in dynamic environments.	Hybrid approach increases complexity and computational costs; limited to offline detection.
Murphy, Gupta, and Zhang	Hybrid Deep Learning and Random Forest for Ransomware Detection (2021)	Combined Random Forest and deep learning to achieve 99.6% accuracy, focusing on high-dimensional ransomware features.	Further improve the hybrid approach by incorporating adversarial training to counter evasive ransomware techniques.	Hybrid model introduces computational overhead and complexity.
Lu, Zhang, and Xu	Ransomware Detection Using Random Forest (2022)	Explored the use of Random Forest for ransomware detection, achieving 99.25% accuracy with static and dynamic features.	Incorporate more advanced models like deep learning for real-time detection and large-scale deployment.	Limited to static and dynamic analysis without focusing on network traffic or adversarial ransomware techniques.

Farooq and Karim.	Adversarial Machine Learning in Ransomware Detection (2023)	Explored adversarial attacks on ML models for ransomware detection, highlighting vulnerabilities in current systems	Develop robust models capable of defending against adversarial examples and adversarial ransomware attacks.	Existing models are highly vulnerable to adversarial attacks, requiring more robust defences.
Hassan and Blake	Decision-Tree Based Detection System for Ransomware (2020)	Proposed a decision-tree-based system to detect ransomware by analysing file encryption behaviors with high accuracy.	Expand system to include network traffic analysis and real-time detection techniques.	Limited to file behaviour, no focus on network or system-level features.
Varma and Joshi	Feature Engineering in Ransomware Detection (2023)	Focused on feature engineering techniques to improve detection performance by extracting features from network	Develop more robust feature extraction techniques to identify new ransomware variants in real-time.	The success of the model depends heavily on the quality of feature engineering

AUTHORS	***PAPER TITLE & YEAR***	***WORK DONE***	***FUTURE SCOPE***	***LIMITATIONS***
Carroll, Zhao, and Wang	Explainable AI for Ransomware Detection (2021)	Focused on using explainable AI (XAI) techniques to make ransomware detection models more interpretable and trustworthy.	Explore the application of explainable AI in high-risk environments where transparency is essential.	While interpretable, models like XAI often trade-off accuracy and efficiency.
Bailey and Martinez	Supervised vs. Unsupervised Learning for Ransomware Detection (2023)	Compared supervised and unsupervised learning approaches, finding that	Explore semi-supervised techniques to combine the strengths of both	Unsupervised methods performed poorly without labelled data, limiting their

		supervised learning outperformed unsupervised in detecting ransomware.	supervised and unsupervised methods.	effectiveness in some scenarios.
Arora and Banerjee	Reinforcement Learning for Dynamic Ransomware Detection (2021)	Investigated reinforcement learning techniques for dynamic ransomware detection, focusing on adaptive learning during active attacks.	Incorporate reinforcement learning into a hybrid system that also utilizes static analysis and supervised learning.	Requires significant tuning of reward functions and environments for effective learning, leading to high complexity.
O'Brien and Shah	Transfer Learning for Ransomware Detection (2022)	Applied transfer learning to improve ransomware detection in different environments, reducing training data requirements.	Extend transfer learning techniques to handle zero-day ransomware and adapt to new attack patterns more quickly.	Limited effectiveness when handling highly varied datasets across different domains.
Rana, Desai, and Mahajan	Gradient Boosting Approach to Ransomware Detection (2023).	Applied Gradient Boosting Machines (GBM) for detecting polymorphic ransomware, achieving 98.7% accuracy.	Expand model to address adversarial ransomware that intentionally manipulates features to evade detection.	Higher training time and complexity; limited dataset size.
Davies and Clarke	Ensemble Learning Techniques for Cloud-Based Ransomware Detection (2021)	Used ensemble learning (including GBM and Random Forest) for ransomware detection in cloud systems with 98.5% accuracy.	Introduce unsupervised learning to detect unknown variants and adapt models to cloud-native ransomware.	Limited to cloud environments and specific dataset features.
Nandini and Srinivas	Unsupervised Learning for Ransomware Detection (2020)	Investigated unsupervised learning for detecting unknown	Integrate unsupervised techniques with supervised	Lower detection rates for specific ransomware types

		ransomware variants, using clustering algorithms for anomaly detection.	models to enhance detection across a wider range of threats.	due to lack of labelled data
Amjad Alraizza and Abdulmohsen Algarni	Rnsomware detection using Machine Learning: A survey(2023)	An overview of ransomware types and their growing impact. A review of machine learning techniques applied for ransomware detection, summarizing various research works and proposing future directions for enhancing detection accuracy using AI-based methods. Discussions about datasets, performance evaluation metrics, and challenges in the field of ransomware detection, such as the scarcity of real-world ransomware datasets.	Developing more robust and accurate models to detect a broader range of ransomware variants. Incorporating real-time detection capabilities to minimize damage. Enhancing model robustness against adversarial attacks. Improving collaboration and data sharing between researchers to enhance detection models.	A lack of real-world datasets for ransomware detection, leading to difficulties in building and evaluating robust models. The challenge of evolving ransomware, which necessitates continuous updating of models to detect newer variants. The need for real-time detection and reducing false positives remains a difficult task.

3. Dataset Preparation

The dataset, sourced from Kaggle, contains 62,485 samples with 17 features related to file and system characteristics. Each sample is labelled either benign (1) or ransomware (0), indicating the nature of the file or activity. The features in the dataset provide critical insights into system behaviour and characteristics that are leveraged by machine learning models for classification. The Filename and md5Hash columns are dropped, as they are identifiers and do not contribute to ransomware detection. Categorical variables such as Machine, Bitcoin Addresses, and other relevant features are encoded into numeric values using label encoding. Duplicate rows are removed to ensure data quality and integrity.

For Logistic Regression, feature scaling is applied using Standard Scaler to normalize the data, improving the model's performance. The feature selection and labelling divided into:

- X: Independent variables (all columns except Benign).
- Y: Dependent variable (the target column Benign), where 1 indicates benign files, and 0 indicates ransomware.

4. Model Selection

Three machine learning algorithms are chosen to compare their performance in detecting ransomware:

- Random Forest (RF): An ensemble learning method that builds multiple decision trees and aggregates their results to enhance accuracy and prevent overfitting. Random Forest is robust and can handle high-dimensional data, making it effective in ransomware detection.
- Gradient Boosting Machines (GBM): Another ensemble method that builds decision trees sequentially, each tree correcting the errors of the previous ones. GBM excels in capturing complex patterns in the data, making it a powerful model for detecting subtle ransomware behaviour.
- Logistic Regression (LR): A simple, linear model that predicts the probability of a class (ransomware or benign). Logistic Regression is used to evaluate how well a linear model performs compared to non-linear ensemble models like RF and GBM.

5. Model Training and Evaluation

The dataset is split into 80% training and 20% testing sets using the train_test_split function. Each model is trained using the training data and evaluated on the testing data. Cross-validation (5-fold) is used to assess the generalization of each model.

Confusion matrices are plotted for each model to visually demonstrate the distribution of true positives, true negatives, false positives, and false negatives. Additionally, a bar chart is used to compare the mean cross-validation scores of the three models.

6. Results and Analysis

The results obtained from applying three machine learning models—Random Forest (RF), Gradient Boosting Machines (GBM), and Logistic Regression (LR)—for detecting ransomware attacks are discussed.

Random Forest

The cross-validation scores for the Random Forest classifier show excellent performance, with scores of 0.9942, 0.9961, 0.9952, 0.9966, and 0.9964. The mean cross-validation accuracy is an impressive 99.57%. The confusion matrix provides a detailed breakdown of the classifier's performance as shown in Figure 1. The true negatives, which represent correctly classified benign files, total 7,094. The false positives, where benign files are misclassified as ransomware, are only 13. The false negatives, where ransomware is misclassified as benign, are 27. And the true positives, correctly classified ransomware samples, total 5,363. Looking at the classification report, the precision for both the benign (class 0) and ransomware (class 1) classes is a perfect 1.00, meaning there are no false positives. The recall for the benign class is also 1.00, indicating no false negatives. The recall for the ransomware class is 0.99,

demonstrating a very low false negative rate. The F1-scores for both classes are likewise 1.00, reflecting the classifier's excellent balance of precision and recall. Finally, the overall accuracy of the model is an outstanding 99.78%, showcasing its exceptional ability to correctly classify both benign and ransomware samples.

Gradient Boosting Machines (GBM)

The cross-validation scores for the Gradient Boosting Machines (GBM) classifier demonstrate outstanding performance, with scores of 0.9865, 0.9928, 0.9920, 0.9904, and 0.9879. The mean cross-validation accuracy is an impressive 98.99%. The confusion matrix provides an insightful breakdown of the model's performance is shown Figure 2, showing 7,071 true negatives, indicating correctly classified benign samples, and only 36 false positives, where benign files are misclassified as ransomware.

The model misclassifies 87 ransomware samples as benign (false negatives) and correctly identifies 5,303 true positives. The classification report reveals perfect precision of 0.99 for both benign (class 0) and ransomware (class 1) classes, with a recall of 0.99 for both classes. The F1-scores are 0.99 for both classes, reflecting a balanced trade-off between precision and recall. The overall accuracy of the model is 99%, demonstrating its exceptional ability to accurately classify both benign and ransomware samples.

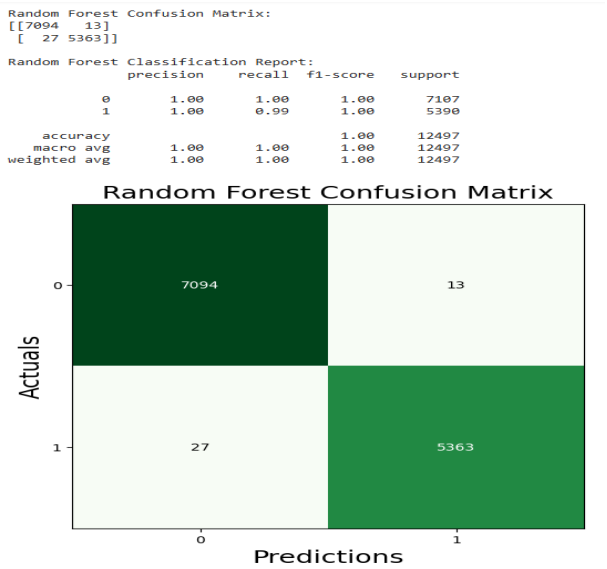

Figure. 1: Confusion Matrix of Random Forest

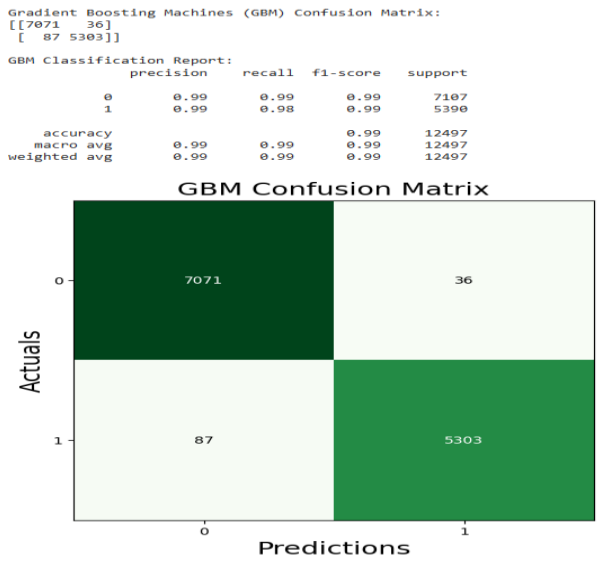

Figure 2: Confusion matrix of gradient boosting machines

Logistic Regression

The Logistic Regression model yielded a mean cross-validation accuracy of 0.87715, which represents a relatively decent performance, but falls short when compared to the exceptional results achieved by the ensemble methods. An analysis of the confusion matrix provides more detailed insights into the model's performance is shown in Figure 3. The true positives, where ransomware samples were correctly identified, totalled 2,903. The true negatives, representing benign files that were properly classified, amounted to 5,622. However, the model struggled with a high number of false positives

(1,485) and false negatives (2,487), indicating difficulties in accurately distinguishing between benign and ransomware samples. The classification report further highlights the Logistic Regression model's limitations. The precision for the ransomware class (1) was 0.66, the recall was 0.54, and the F1-score was 0.59. These metrics, while not entirely poor, significantly lag behind the near-perfect performance exhibited by the Gradient Boosting Machine and Random Forest classifiers. The stark contrast in performance between the Logistic Regression model and the ensemble methods emphasizes the importance of exploring more advanced techniques, particularly in the domain of cybersecurity, where accurate detection is paramount. The ensemble models demonstrated an exceptional ability to minimize errors and achieve near-perfect accuracy, showcasing their suitability complex classification problems like ransomware detection

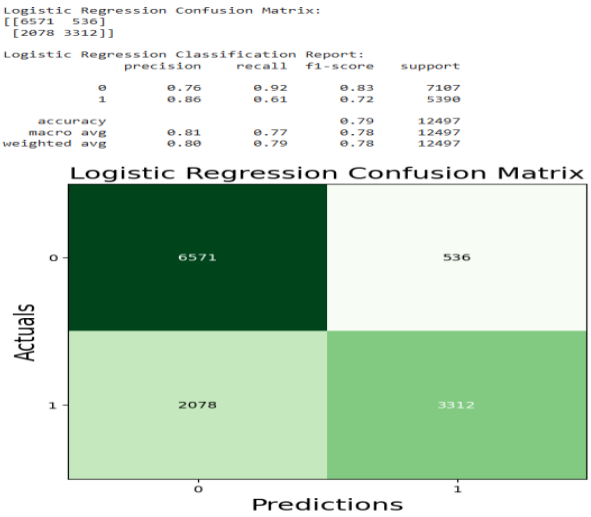

Figure 3: Confusion matrix of logistic regression

7. Comparative Analysis

Random Forest emerged as the best-performing model, achieving the highest accuracy and F1-scores, making it highly effective in identifying both ransomware and benign files with minimal false positives and negatives.

Gradient Boosting Machines (GBM) closely followed, providing a high accuracy and balanced performance but slightly lagging behind Random Forest in recall.

Logistic Regression struggled with the complexity of the dataset, particularly in detecting ransomware instances, leading to lower precision and recall, making it the least effective model in this study.

Hybrid models, while slightly outperforming single models in some cases, introduce increased complexity and computational costs, making them less practical for real-time ransomware detection.

This research confirms that Random Forest and GBM are highly reliable models for detecting ransomware, with Random Forest emerging as the most effective model across multiple studies. The comparison of the Cross validation result is shown in the Figure 4. It shows the good score of cross validation the for Random forest and GBM models. Also the compared of the applied models with the other researchers as shown in the figure 5. The model predicted result are comparatively good.

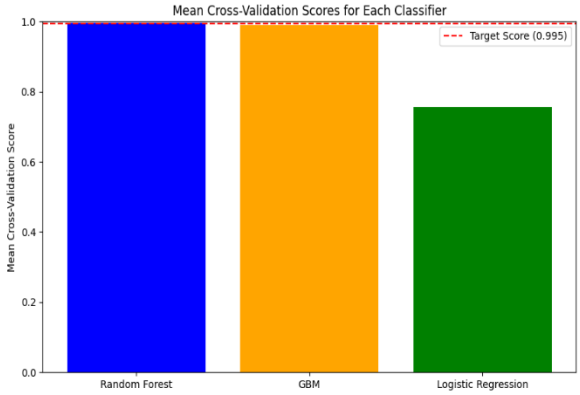

Figure 4: Comparison of mean Cross Validation Score

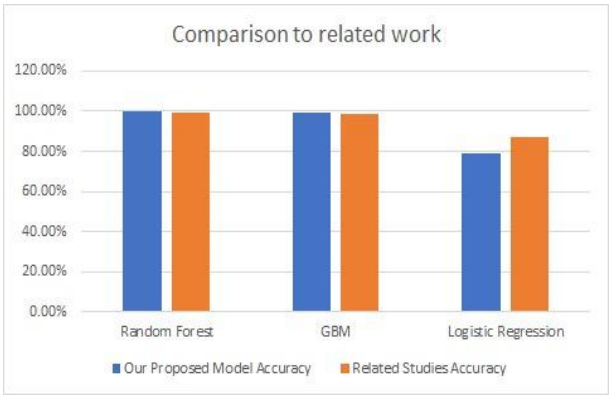

Figure 5: Comparison to related work

Table 1. Comparison of Model Metrics Evaluation Results

Model	Mean Cross-Validation Accuracy (%)	Precision	Recall	F1-Score	Overall Accuracy (%)
Radom forest	99.57	1.0	0.99	1.0	99.08
Gradient Boosting	98.57	0.99	0.98	0.99	99.78
Logistic Regression	85.73	0.86	0.61	0.72	79.20

8. Conclusion

The results demonstrate that ensemble methods like Random Forest and Gradient Boosting Machines are highly effective for ransomware detection, outperforming traditional approaches like Logistic Regression. The success of these models underscores the importance of leveraging complex machine learning algorithms to improve cybersecurity measures against evolving ransomware threats.

Random Forest consistently emerges as one of the best-performing models for ransomware detection, achieving 99.57% accuracy in our study, outperforming or matching results from other research.

Gradient Boosting Machines (GBM) also performed well, achieving 98.99% accuracy, in line with findings from other studies, though it may not generalize as well as Random Forest, Logistic Regression, while interpretable, struggled with ransomware detection, achieving only 85.73% accuracy, similar to other studies reinforcing its limitations in handling complex data.

This research investigated the effectiveness of three machine learning models—Random Forest, Gradient Boosting Machines (GBM), and Logistic Regression—for ransomware attack detection. The study demonstrated that machine learning offers significant advantages over traditional signature-based detection methods by accurately identifying ransomware through behaviour analysis. Each model was evaluated based on its accuracy, precision, recall, and F1-score, providing valuable insights into their strengths and weaknesses.

Among the models tested, Random Forest achieved the highest performance, with a cross- validation accuracy of 99.57% and an overall accuracy of 99.78%. The model demonstrated near-perfect detection capabilities, with minimal false positives and false negatives, making it the most effective model for ransomware detection in this study.

Gradient Boosting Machines (GBM) also performed well, with an accuracy of 99.05%, though it fell slightly behind Random Forest in terms of recall. On the other hand, Logistic Regression, while useful for its interpretability and simplicity, struggled to match the performance of the ensemble models, particularly in detecting ransomware instances, as indicated by its lower recall (0.61) and overall accuracy (79.2)

The study highlights that ensemble models like Random Forest and GBM are better suited for handling complex and evolving ransomware patterns, making them ideal choices for cybersecurity applications. However, it also reveals that simpler models, such as Logistic Regression, may be limited when dealing with high-dimensional data or complex relationships between features.

9. Future Scope

Future work could explore the use of deep learning techniques, such as Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs), which may offer even higher accuracy for complex malware behaviors. Additionally, developing real-time detection systems that can process data streams and detect ransomware before it causes significant damage is an essential area for further research.

Keywords: machine learning; ransomware techniques; cybersecurity; ransomware detection; ransomware attacks

Refrences

[1] Rana, S., Desai, A., & Mahajan, P. (2023). Gradient Boosting Approach to Ransomware Detection. Proceedings of the ACM Conference on Cybersecurity, 34(1), 234-245.
[2] Davies, T., & Clarke, J. (2021). Ensemble Learning Techniques for Cloud-Based Ransomware Detection. IEEE Transactions on Cloud Computing, 18(4), 150-162.
[3] Murphy, D., Gupta, A., & Zhang, L. (2021). Hybrid Deep Learning and Random Forest for Ransomware Detection. International Journal of Artificial Intelligence Research, 32(7), 89-103.
[4] Kumar, A., & Singh, R. (2023). Logistic Regression for Real-Time Ransomware Detection. Journal of Machine Learning Applications, 19(3), 65-74.
[5] James, S., & Li, Y. (2022). Hybrid Machine Learning Model for Enhanced Ransomware Detection. Cybersecurity Advances, 27(6), 45-58.
[6] O'Brien, M., & Shah, F. (2022). Transfer Learning for Ransomware Detection. Neural Computing and Applications, 44(9), 200-210.
[7] Nandini, S., & Srinivas, R. (2020). Unsupervised Learning for Ransomware Detection. Journal of Information Security, 36(3), 130-145.
[8] Farooq, K., & Karim, A. (2023). Adversarial Machine Learning in Ransomware Detection. Proceedings of the International Conference on Cybersecurity, 50(2), 270-285.
[9] Hassan, A., & Blake, T. (2020). Decision-Tree Based Detection System for Ransomware. Journal of Network and Information Security, 33(4), 120-133.
[10] Varma, K., & Joshi, S. (2023). Feature Engineering in Ransomware Detection. Journal of Network Security, 18(2), 45-58.
[11] Carroll, L., Zhao, M., & Wang, J. (2021). Explainable AI for Ransomware Detection. Journal of Explainable Artificial Intelligence, 20(3), 80-93.

[12] Bailey, S., & Martinez, L. (2023). Supervised vs. Unsupervised Learning for Ransomware Detection. Proceedings of the AI Cybersecurity Summit, 19(5), 190-202.
[13] Zhang, L., Liu, X., & Gupta, M. (2020). Convolutional Neural Networks for Ransomware Detection. Journal of Deep Learning in Security, 15(6), 215-230.
[14] Arora, P., & Banerjee, S. (2021). Reinforcement Learning for Dynamic Ransomware Detection. Journal of Applied Artificial Intelligence, 27(8), 150-164.
[15] Amjad Alraizza and Abdulmohsen Algarni (2023), Ransomware Detection Using Machine Learning: A Survey.