Ransomware Detection using Machine Learning

Dr. Nadesh R K
Department of Information Technology
School of Computer Science
Engineering and Information Systems
Vellore, India
rknadesh@vit.ac.in

Abhijeet Kushwaha
School of Computer Science
Engineering and Information Systems
VIT University, Vellore
Prayagraj, India
abhijeet.kushwaha2023@vitstudent.ac.in

Tanmay Choudharay
School of Computer Science
Engineering and Information Systems
VIT University, Vellore
Bhilwara, India
tanmay.choudhary2023@vitstudent.ac.in

***Abstract*—In this Modern Era, the Internet is an integral part of the lives of human beings. And as the internet continues to expand, malware continues to pose a hazard. By presenting a larger attack surface, the Internet of Things' (IoT) quick development has further contributed to this issue. Among these malwares Ransomware is a category that spreads like a worm and inhibits or limits users from accessing their system, either by locking the system screen or encrypting and locking users' files unless a ransom is paid. This project looks to detect Ransomwares using different Machine Learning Algorithms like Random Forest (RF), Naïve Bayes (NB), Decision Tree (DT), Logistic Regression (LR), Neural Network (NN) by taking the historical data that will predict presence of malware in given set of files. The dataset used for this purpose is from the popular data set platforms like Kaggle, UCI Machine Learning Repository, AWS Public Datasets and Google's Dataset Search Tool. Concluding comparison of the accuracy of the models used and then use the most accurate algorithm for detection of Ransomware. The decision tree comes as most accurate algorithm with accuracy 99.19% and least accurate was Naïve Bayes with accuracy 69.70%.**

Keywords—malware, ransomware, Machine Learning, encryption, datasets

I. Introduction

Ransomware is a type of malicious software or attacks, malware, and ransomware families that continue to pose critical security threats to cybersecurity and can cause catastrophic damage to computer systems and data centers, as well as web and mobile applications across different industries and businesses [1]. Ransomware is typically designed to block and deny targeted victims access to computer data by using an unbreakable encryption method that only the attacker can decrypt. If the ransomware is removed, the victim suffers irreparable losses and is forced to pay as per the demands of the attacker [2]. Failure or denial of payment will result in the loss of data permanently. Modern technology is enabling attackers to transform conventional ransomware into new ransomware families, making it more difficult to reverse a ransomware infection [4]. What is ransomware? Ransomware, also known as ransomware, is a sophisticated and variant threat affecting users worldwide. It restricts access to a user's system or data by locking the system's screen or encrypting and the user's files until a ransom is paid. Based on attack methods, there are two types of ransomwares: locker ransomware, which limits access to the computer or device, and crypto ransomware, which prohibits access to files or data [5]. It is quite impossible to revert after these attacks without paying for the extortion. Traditional ransomware detection methods, such as event-based, statistical-based, and data-centric-based strategies, are ineffective. As a result, achieving the maximum level of optimal protection and security against such advanced malicious attacks should be a top priority for the research community. Machine learning, for example, in ransomware detection is a novel research field that can be greatly leveraged in the creation of creative ransomware solutions [2]. Using Machine Learning (ML) techniques enables automatic identification of malware, including ransomware, based on their dynamic activities, and improves security [6]. Decision Tree (DT), Random Forest (RF), Nave Bayes (NB), Logistic Regression (LR), and Neural Network (NN)-based architectures offer the potential for ransomware categorization and detection. Undertake a complete examination and investigate machine learning algorithms for ransomware categorization. The paper's primary contributions are listed below:

- Examination of various types of ransomwares, frequent attack vectors, and a threat landscape to emphasize the full potential the full potential and catastrophic nature of such malware-based attacks. Addressing the most recent ransomware outbreak as a potential threat, as well as advice and techniques for prevention and security against these attacks.
- Presentation of robust tests to illustrate the models' generality and compare it to other approaches.

The remainder of the paper is organized as follows: Section II discusses ML-based ransomware detection efforts. Section III describes the strategies used. Section IV describes the experimental design and outcomes. Section V brings the paper to a close.

II. Related Work

Various malware, including ransomware, has been classified using traditional detection techniques. A well-defined behavioural structure can be used to analyse various ransomware, and most ransomware families share common behavioural traits such as payload persistence, stealth techniques, and network traffic. The most widely used traditional anti-malware system is signature-based analysis, and A. M. Abiola and M. F. Marhusin [13] proposed a signature-based detection model for malware by extracting the Brontok worms and using an n-gram technique to break down the signatures. The framework detects malware and generates a credible solution that eliminates all threats. Addressing

limitation, [14] introduced a static and dynamic-based or behaviour-based framework in which static-based analysis analyses the application's code to determine malicious activities and dynamic-based analysis monitors the processes to determine the behaviour of malicious intent and will be flagged as suspicious and terminated. Both static and dynamic analysis have limitations in terms of detecting unknown malware and being ineffective against code obfuscation, high variant output, and targeted attacks.

[15] where dynamic malware detection was suggested utilizing a dynamic malware detection framework utilizing Deep Neural Network (DNN) and Convolutional Neural Network (CNN). Long Short-Term Memory is used in the construction of the machine learning model (LSTM). To distinguish suspicious malware samples, a novel approach was employed between CNNs and the LSTM network. The evaluation report states that a combination of DNN and LSTM is effective at 91.63% accuracy in detecting new malware. Malware detection in Android has also been accomplished with deep learning. Mechanized as a deep learner, the deep learning framework (Droid-NNet) for malware classification in Android was proposed by M. Masum and H. Shahriar. It performs better than state-of-the-art machine learning techniques.

The use of cutting-edge machine learning concepts in ransomware detection and prevention is necessary to enhance current methods. Researchers [16] introduced a revolutionary flow-oriented method called Biflow for ransomware detection, and as a result, they offered a network intrusion detection system that consists of Argus server and client applications.

III. Methodology

Several machine methods, including the random forest classifier, logistic regression, decision tree, naive bayes classifier, and neural network, have been used to identify ransomware.

The steps took for model are depicted in the image below. Pre-processing techniques were utilized to reduce the dataset's size into a comparable range, as it had a huge number of rows and columns. For instance, eliminated the characteristics Name and md5. Used the feature selection approach to identify the key characteristics, and selected those features as parameters in several classifiers to distinguish ransomware from genuine data. Assessed and learned about the models' performance using a variety of assessment criteria, including accuracy, f1_score, precision, and recall.

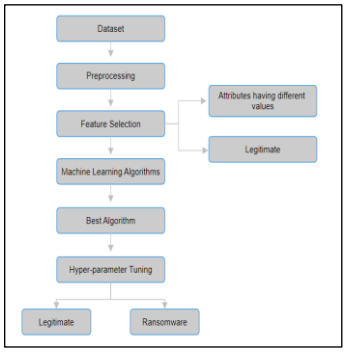

Figure 1: Framework to detect ransomware

IV. Experiments and Result

A. Dataset specification

Dataset has 138047 data and 57 characteristics, whereby 70.07% of the samples are ransomware and 29.93% are authentic according to the figure.

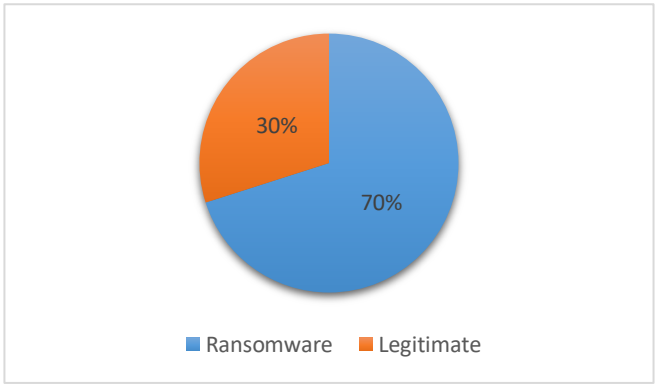

Figure 2: Legitimate Attribute Values

B. Feature Selection

Features with correlations larger than 0.75 were chosen. Exclude low variation and highly linked characteristics from the data, used feature selection techniques.

C. Evaluation metrics

1) Precision: The proportion of the correctly identified positives to all the predicted positives. Mathematically:

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

2) Recall: The number of correct positive predictions among all the positive samples. Mathematically:

$$Recall = \frac{\text{True Positive}}{\text{True Positive+False Negetive}}$$

3) F_1 score: The harmonic means of Precision and Recall. $F1\ score$ is a better performance metric than the accuracy metric for imbalanced data.

$$\text{F}_1\text{score} = 2 \times \frac{Precision \times Recall}{Precision \pm Recall}$$

4) Accuracy: The measurement used to determine which model is best at identifying relationships and patterns between variables in a dataset based on the input, or training, data.

$$\text{Accuracy} = \frac{True\ Positives + True\ Negatives}{True\ Positives + True\ Negetives + False\ Positives + False\ Negetives}$$

D. Experimental Setting

Acquiring a Ransomware Dataset and proceeded to choose the 'legitimate' feature as the predictor variable for algorithms. Assessing each model's performance by contrasting its results with those of the Neural Network, Decision Tree, Random Forest Classifier, Naïve Bayes, and Logistic Regression techniques. Then, utilizing predictor

variables, created algorithmic models to predict values. Evaluated the models' accuracy, precision, recall, f1_score. To define the performance of these algorithms, built a confusion matrix after obtaining each accuracy.
Following model construction, evaluate each model's accuracy and found that decision tree and random forest had the highest accuracy scores—99.195 and 98.381—among the models. Using the given hyperparameter settings, the Python scikit-learn package was used to implement the algorithms.
Four layers make up the neural network-based architecture: an input layer, two hidden layers, and an output layer. Since this is a binary classification problem, employed the "sigmoid" function in the output layer and the "ReLu" activation function in the input and hidden layers. Binary cross-entropy and RMSprop were employed as the optimizer and loss function, respectively.

E. Results

To distinguish between genuine and ransomware samples, employed Random Forest, Logistic Regression, Decision Trees, Naive Bayes Classifiers, and Neural Networks.

	Algorithms	Accuracy	F1_Score	Precision	Recall
0	Random Forest	98.38	97.30	97.94	96.68
1	Logistic Regression	69.72	0.00	0.00	0.00
2	Decision Tree	99.23	98.73	98.56	98.79
3	Naive Bayes	69.72	0.02	98.56	98.79
4	Neural Networks	69.72	0.00	98.56	98.79

Figure 3: Experimental Results analysis of different algorithms

Models' outcomes in terms of accuracy, F1 score, recall, and precision are displayed in the table. The models that outperform others in terms of accuracy, F1 score, precision, and recall are Decision Tree and Random Forest.

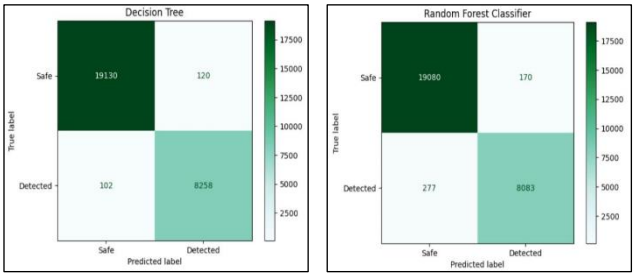

Figure 4: Decision Tree and Random Forest Confusion Matrixes

Inferring that decision trees outperform random forests in terms of accuracy, i.e., 99.39% after doing hyper-parameter tweaking on both types of trees.

V. Conclusion

Financial institutions, businesses, and individuals are facing a growing threat to their security from malware, which includes ransomware. Effectively classify and detect ransomware and lower the risk of malicious activities, an automatic system must be developed. To effectively classify and detect ransomware, adopted various machine learning algorithms, such as neural network-based classifiers, and have presented a novel framework for feature selection. Used a ransomware dataset to apply the framework and all the experiments, and assessed the models' performance using a thorough comparison of the DT, RF, NB, LR, and NN classifiers. The results of the experiment show that the Decision Tree classifier performed better than other classifiers by obtaining the highest accuracy.

Acknowledgment

Our guide, Dr. Nadesh R.K., helped us out with most of the work. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors.

References

[1] Nadeem Shah, Mohammed Farik-(2017)- Ransomware- Threats, Vulnerabilities and Recommendations - ISSN-2277-8616

[2] Mohammad Masum, Md Jobair Hossain Faruk, Hossain Shahriar Kai Qian, Dan Lo, Muhaiminul Islam Adnan (2020)- Ransomware Classification and Detection With Machine Learning Algorithms

[3] Seong Il Bae, Gyu Bin Lee, Eul Gyu Im (2018)- Ransomware detection using machine learning algorithms DOI: 10.1002/cpe.5422

[4] Ali Ahmed Mohammed Ali Alwashali, Nor Azlina Abd Rahman, Noris Ismail (2021)- A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack- 2021 14th International Conference on Developments in eSystems Engineering (DeSE)

[5] A. K. Maurya, N. Kumar, A. Agrawal, R. A. Khan (2017) Ransomware: Evolution, Target and Safety Measures International Journal of Computer Sciences and Engineering · January 2018 DOI: 10.26438/ijcse/v6i1.8085

[6] Sujit Kumar Dwivedi - Ransomware - Threats, Vulnerabilities, and Targets in Cloud Environment - PAGE 100078-100090| DOI: 10.14704/NQ.2022.20.6.NQ22981

[7] Md Naseef-Ur-Rahman Chowdhury, Ahshanul Haque, Hamdy Soliman, Mohammad Sahinur Hossen Imtiaz Ahmed, Tanjim Fatima (2018)- Android malware Detection using Machine learning: A Review

[8] Hiroshi Fujinoki Lasya Manukonda (2023)- Proactive Damage Prevention from Zero-Day Ransomwares- International Conference on Computer Communication and the Internet

[9] Jafar Alzubi - Machine Learning from Theory to Algorithms: An Overview et al 2018 J. Phys.: Conf. Ser. 1142 012012

[10] Mariwan Ahmed Hama Saeed (2020)- Malware in Computer Systems: Problems and Solutions Vol. 9, No. 1, 2020, Pp. 1-8 DOI: 10.14421/ijid.2020.09101

[11] Irina Baptista, Stavros Shiaeles and Nicholas Kolokotronis (2021)- A Novel Malware Detection System Based On Machine Learning and Binary Visualization

[12] Syam Akhil Repalle, Venkata Ratnam Kolluru (2017)- Intrusion Detection System using AI and Machine Learning Algorithm - International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056

[13] A. M. Abiola and M. F. Marhusin, "Signature-based malware detection using sequences of N-grams," Int. J. Eng. Technol., vol. 7, no. 4, pp. 120–125, 2018, doi:10.14419/ijet.v7i4.15.21432.

[14] D. Nieuwenhuizen, "A behavioural-based approach to ransomware detection," *MWR Labs*, 2017, [Online]. Available:https://labs.fsecure.com/assets/resourceFiles/mwri-behaviouralransomware-detection-2017-04-5.pdf

[15] H. Ghanei, F. Manavi, and A. Hamzeh, "A novel method for malware detection based on hardware events using deep neural networks," J. Comput. Virol. Hacking Tech., vol. 17,no. 4, pp. 319–331, 2021, doi: 10.1007/s11416-021-00386-y.

[16] Y. L. Wan, J. C. Chang, R. J. Chen, and S. J. Wang, "FeatureSelection-Based Ransomware Detection with Machine Learning of Data Analysis," 2018 3rd Int. Conf. Comput. Commun. Syst. ICCCS 2018, pp. 392–396, 2018, doi: 10.1109/CCOMS.2018.8463300.