Advancement in Ransomware Detection Using Deep Learning

Vardaan Shukla
SCSET
Bennett University
Greater Noida, India
Shukla02var@gmail.com

Shobhit Kumar
SCSET
Bennett University
Greater Noida, India
shobhit.bluestar@gmail.com

Rajesh Kumar Shrivastava
SCSET
Bennett University
Greater Noida, India
0000-0002-5656-9111

***Abstract*—In the digital era malicious devices, viruses, and ransomware are quite common problems that are being faced by people, as the world is moving forward towards technology. We are exploring new ways for automation that increase digital footprint. Hence, hackers introduce new viruses and ransomware very frequently. This paper mainly focuses on the detection of ransomware using machine learning and deep learning models. Here, we test a malicious dataset for ransomware detection with SVC(Support vector classification), ANN(Artificial neural network), CNN (Computational neural network), Xgboost, and RandomForest classifier. The experimental result got up to 99% accuracy.**

***Index Terms*—Classification, Ransomware, Deep Learning, CNN, Cybersecurity.**

I. Introduction

In recent years ransomware become the name of cyber threat. Ransomware locks the digital device and asks for a ransom to decrypt the digital device. As per the report generated by CISCO, Every year ransomware attacks cost up to 150 million dollars. Major targets of ransomware attacks are individuals, businesses, and critical infrastructure worldwide. Ransomware has evolved in this changing environment, posing substantial challenges to cybersecurity experts and organizations. Existing methods of detecting and mitigating ransomware attacks often fall short in the rapidly evolving environment along with changing attack strategies along with a significant increment in the scale of the threat landscape.

The application of deep learning techniques has emerged as a promising factor in enhancing ransomware detection capabilities. Deep learning is a subset of Machine learning inspired by the structure and functions of the Human brain's neural networks and has demonstrated remarkable success in the field of cybersecurity in the detection and prevention of threats.

This research paper explores the development of ransomware detection facilitated by deep learning methodologies. In this paper, we will be discussing the existing research completed in the field of ransomware using deep learning and what we have contributed in the same area of work using the latest set of technology and methods to make it more accurate and efficient. Furthermore, the inherent ability of deep learning models to continuously learn and improve over time makes them particularly well-suited for addressing the dynamic nature of ransomware threats.

In this paper, we talk about the key principles and techniques underpinning deep learning-based ransomware detection. We examine the underlying mechanisms of various deep learning architectures, such as convolutional neural networks(CNN), Artificial neural networks(ANN), and their variants, and explore how these models can be tailored to effectively discern ransomware activity from benign system behavior. Additionally, we investigate the integration of advanced features, such as anomaly detection and behavioral analysis, into deep learning frameworks to bolster the resilience of ransomware detection systems against emerging threats.

In the subsequent sections, we will talk about the existing work that has been carried out by the researchers in the past and what path was chosen by them along with the techniques used in the research work, which is discussed in the Related Work section of the paper.

In the Methodology section of the paper, we have discussed how we have carried out our research work and what techniques and methods we have to use to carry out our findings in the field of ransomware.

Then the section Experiments and Results, talks about the dataset taken for the work that is carried out. It talks about, How the prominent features were identified to work upon and what were the steps and framework for the expirement. Along with different models that are being used in the research and showcasing the findings and results in the paper, with the help of graphs and charts we can differentiate between the final findings how differently each model is working, and what are the findings of the particular model that is mentioned in the result section of the Experiments and Result.

Followed, by the conclusion where we concluded the findings of the research paper, along with a current scenario explanation in regards to how ransomware has evolved in the past time and also how the threats raised by ransomware can be dealt with using deep learning technology.

II. Related Work

Ransomware, a pernicious form of malware engineered to hold computer systems or file storage until some ransom is paid, presents a pervasive threat across individuals, organizations, and governmental bodies globally. A spectrum of methodology has been devised to combat ransomware with a recent emphasis on harnessing the power of machine learning for enhanced detection and accuracy.

Researcher Fakhroddin Noorbehbahani et al. [1] share their research ideas on the same their paper investigates the efficiency of machine learning in detecting ransomware threats, a pressing issue in cybersecurity research said that there is a scarcity of studies specifically targeting ransomware detection using machine learning methods throughout their research they have used dataset named CICAndMAL2017.

Other researchers Nanda Rani et al. [2] discussed in their paper a comprehensive review of machine learning techniques that are useful for the classification of ransomware. Some traditional tools are struggling to detect ransomware and early machine learning techniques offer more promising avenues for enhanced detection capabilities. According to the author, some machine learning techniques that are useful in the detection of various applications such as spam detection, text classification, and pattern recognition research aim to throw light on ransomware detection efforts.

One traditional method that is being used for the detection of ransomware is Signature-based Detection this method involves creating signatures or patterns of known ransomware strains [3]. many antiviruses and (IDS) intrusion detection systems use these methods to scan files or network traffic for matches. But, the main disadvantage to using such a system is that they can only detect the known items but the manipulated strings or viruses will not be identified by them.

Researcher Hawawreh et al. [4] provides a comprehensive analysis of the landscape of ransomware detection methods, focusing primarily on machine learning (ML) techniques. Existing studies employ various parameters and matrics, including file encryption convergence, CPU utilization, True Positive Rates (TPR), False Positive Rate (FPR), accuracy, and recovery matrices, among others. While some efforts leverage sophisticated ML algorithms such as Convolutional Neural Networks (CNN), and Bi-directional Long-short-term Memory (BI-LSTM) others utilize supervised algorithms like support vector matrices (SVM) and decision trees (DT) However a notable limitation across these studies is the lack of comprehensive dynamic feature datasets obtained from running ransomware in an isolated environment. This absence hinders the development of robust detection and prevention solutions, particularly rapidly evolving ransomware variants. Therefore this research aims to address these gaps by generating a relevant feature dataset and leveraging it to produce an ML model capable of distinguishing ransomware from benign software, thereby enhancing detection efficacy and resilience against emerging threats.

Researchers YAP L. DION et al. [5] explored the use of machine learning algorithms in ransomware detection, addressing the scarcity of study in this area through an experimental platform constructed with the help of ransomware dataset, various machine learning algorithms including Random Forest, Gradient Boosting Decision Tree(GBDT), Neural Network Multilayer Perception, and three types of Support Vector Machine(SVM) kernels were evaluated. By analyzing opcodes and their frequencies from complete executable files, the study aimed to identify algorithms suitable for developing an effective ransomware detection model. The research was motivated by the significant impact of cyber ransomware, particularly highlighted by the WannaCry attack [6] in May 2017, and the limitations of existing commercial solutions in detecting evolving ransomware threats. The experiment focused on detecting ransomware from goodware using machine learning algorithms and feature selection methods, drawing inspiration from previous studies on automatic labeling of malware samples and analysis of ransomware samples in executable files. The findings of this research are expected to inform the design and development of a more robust ransomware detection system and model, benefiting both industries and research in the domain, the paper concludes with discussions on existing research, research methodology, experimental factors, results, and future directions.

III. Methodology

We applied traditional ML classifiers such as Random Forest Classifies, Support Vector Units, XG-boost, ANN, and CNN to detect ransomware. Figure. 1 shows the framework of our model first data was normalized to its new form so that we could use it for further processing. Feature selection models were applied so that the important features could be selected, then the data was divided for further classification and used in different types of models.

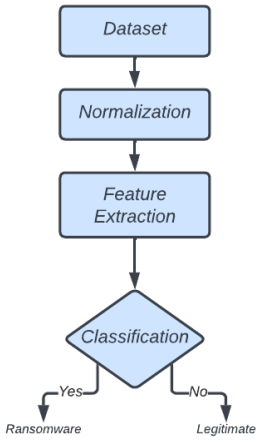

Fig. 1. Data Framework

IV. Experiments And Result

A. *Dataset Specification*

The dataset we are using contains 62486 samples with 18 features where 43.4% were ransomware and 56.6% were legitimate observations fig-2 which displays the distribution of the dataset

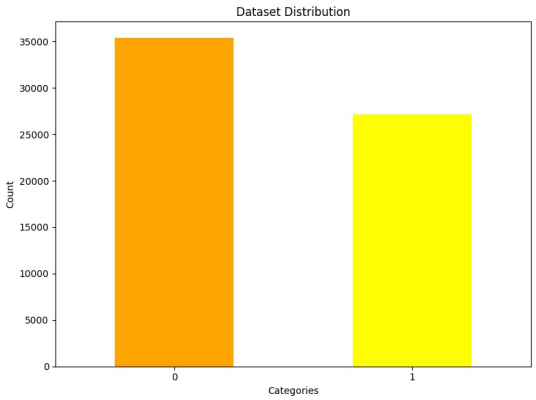

Fig. 2. Distributed Datay

B. *Selection of Features*

Selection of features in machine learning involves choosing a subset of relevant features (variables, predictors) to use in model construction. The aim of feature selection is to reduce overfitting, improve interoperability, and decrease computational cost in the model.
There are many ways for feature scaling to be performed for this dataset we have selected the most used and basic scaling process i.e. Standard Scaling. In this, every feature is based on its mean and standard deviation the formula for standard deviation is

$$X_{\text{std}} = \frac{X - \mu}{\sigma}$$

This is a normalization process in which the mean(μ) is subtracted from each feature from its value and after divided by the standard deviation (σ). It ensures features that have different scales and values come to the same scale and this step can be very crucial for many machine learning algorithms by bringing all the features on a common scale this algorithm will help to converge faster during training and prevent features with large scale to dominate over feature with low scale.

Now, we'll see the steps on how Feature scaling was performed:

1. Data Preparation: The dataset is initially prepared with the independent variable ('x') and the target variable ('y').
2. The dataset is split in training and testing set using the function 'train-test split' this function was imported from 'sklearn.model selection. This step ensures that the model is trained on one subset of data and evaluated on another subset to assess its performance

3. Feature Scaling: After splitting the dataset, feature scaling is applied. fig-3 shows the difference before and after feature scaling

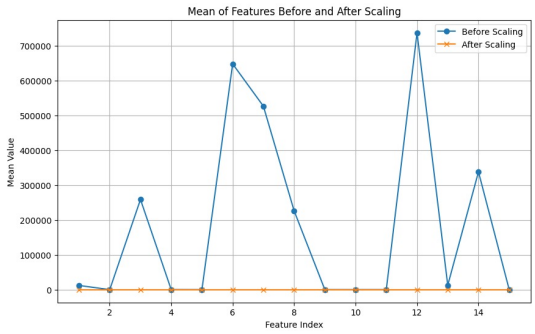

Fig. 3. Feature scaling

C. *Confusion Matrices*

The confusion Matrix serves as a tabular representation that assesses or measure the performance of the designated dataset. It provides a concise breakdown of correct and incorrect predictions made by the model across different classes and categories. The analytical tool is particularly valuable in evaluating classification models, which endeavor to assign categorical labels to input data instances. The matrix presents the count of predictions generated by the model on the test dataset

True positives(TP): Denotes instances where the model correctly predicts positive data points
True negative(TN): Signify instances where the model incorrectly predicts negative data points.
False positives(FP): Represent cases where the model incorrectly predicts positive data points
True positives(FN): Indicate instances where the model erroneously predicts negative data points.

Data based on confusion matrix

1. *Accuracy:* It measures the model's performance as the ratio of correctly predicted instances to the total instances.

$$Accuracy = \frac{CorrectPredictions}{TotalNumberofPrediction}$$

2. *Precision:* It is used to measure how accurate a model's positive predictions are. It is defined as the ratio of TP predictions to the total number of positive predictions made by the model

$$Precision = \frac{T\_P}{T\_P + F\_P}$$

3. *Recall:* It is used to measure the effectiveness of a classification model in identifying all relevant instances from

a dataset. It is the ratio of the number of TP instances to the sum of positive and FN instances

$$Recall = \frac{T\_P}{T\_P + F\_N}$$

Model Name	Truly Positive	Truly Negative	False Positive	False Negative
RandomForest	2154	4253	35	10
Support Vector Classification	2190	4164	124	55
ANN	2803	2639	351	207
XG-Boost	3183	6421	33	40
CNN	2803	2639	351	207

Fig. 4. Confusion Matrix Outputs

D. *Experimental Settings*

We have used different types of models like RandomForest, SVC, ANN, XG-Boost, and CNN on this dataset which is split in the ratio of 7:3 for testing and training data while maintaining the value of benign which will be considered as the dependent variable for classification Trained data was used to train each model all the models discussed above were trained on the dataset.
If we discuss CNN in that model we Keras is used for importing the main convolution layers and sci-kit learn lib is used to support major hyperparameter options.
The neural network was based on 6 layers in total, including one input layer, 4 hidden layers (2 convolution layers and 2 dense layers), and 1 output layer. In dense layers 'ReLU(Rectified Linear Unit)' is used

$$f(x) = \max(0, x)$$

and the 'Sigmoid' activation function is used for the output layer

$$f(x) = \frac{1}{1 + e^{-x}}$$

after that 'Adam' and binary 'cross-entropy' were used as optimizer and loss respectively

E. *Results*

We applied our different models on the dataset to classify the right and legitimate samples in fig-5 we can see the values like f1-beta, recall, precision, and accuracy in the derived table so that we can find whether the model is accurate or not Here we have also displayed the ROC curve for all the classification models ROC(Receiver Operating Characteristic Curve) is a Graph showing the performance of different classifications this graph plots on 2 parameters i.e.
1. True positive rate
2. False positive rate

Model Name	Accuracy	F-Beta	Recall	Precision
RandomForest	0.993	0.995	0.991	0.997
SVC	0.972	.0978	0.971	0.986
ANN	0.972	0.978	0.971	0.986
XG-Boost	0.972	0.978	0.971	0.986
CNN	0.972	0.978	0.971	0.986

Fig. 5. Experimental results and analysis of different models

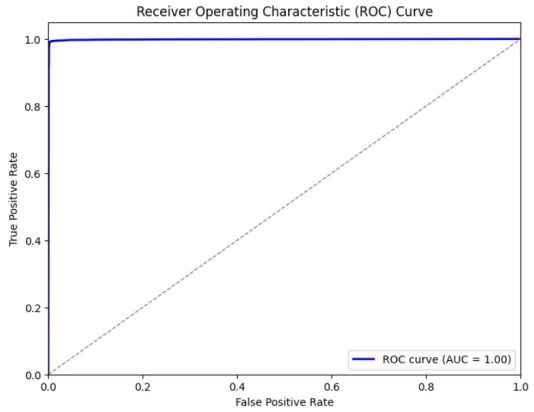

Fig. 6. ROC curve for: RandomForest

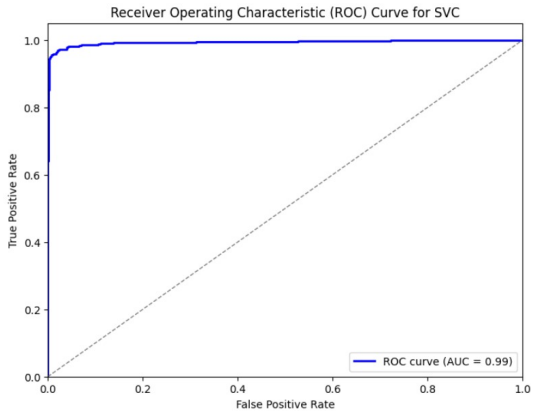

Fig. 7. ROC curve for: Support Vector Classification

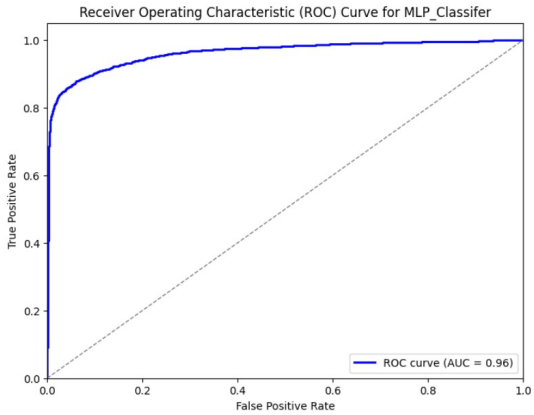

Fig. 8. ROC curve for: ANN

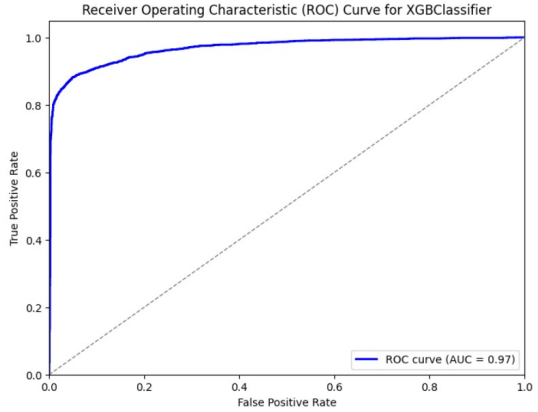

Fig. 9. ROC curve for: XGB-Classifier

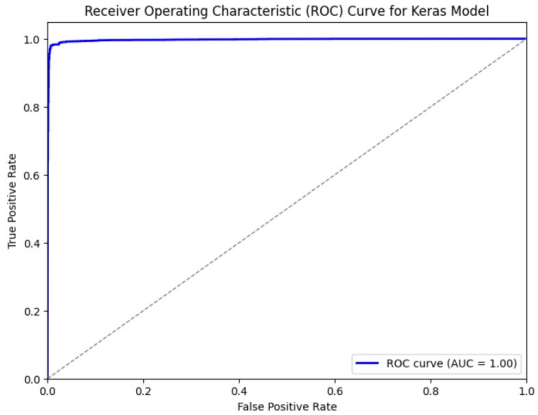

Fig. 10. ROC curve for: CNN

V. Conclusion

Ransomware and viruses are now more dangerous threat to the society so we should go for better alternative for detection of such a malicious software like using AI which we are already doing and we wish this will help us the wayout to solve the problem like this in this paper we have applied some classification models like RandomForest, CNN, ANN, Xg-Boost, SVC which help us to classify the ransomware or legitimate file and accuracy and results we got were good although we can say that Randomforest give much better results than other classifier and we are not satisfied here only we strongly believe that the results can be enhanced on different datasets contain different values and by using hyper-tuning and different algorithms.

References

[1] Noorbehbahani, F., Rasouli, F., & Saberi, M. (2019, August). Analysis of machine learning techniques for ransomware detection. In 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC) (pp. 128-133). IEEE.

[2] Rani, N., Dhavale, S. V., Singh, A., & Mehra, A. (2022, March). A survey on machine learning-based ransomware detection. In Proceedings of the Seventh International Conference on Mathematics and Computing: ICMC 2021 (pp. 171-186). Singapore: Springer Singapore.

[3] Bhattacharjee, S., & Dakhane, D. (2024, January). A Combined Utilization of Machine Learning and Pre-Attack Analysis to Provide a Protection Framework for Ransomware Attack. In 2024 14th International Conference on Cloud Computing, Data Science Engineering (Confluence) (pp. 599-604). IEEE.

[4] Al-Hawawreh, M., Alazab, M., Ferrag, M. A., & Hossain, M. S. (2023). Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms. Journal of Network and Computer Applications, 103809.

[5] Dion, Y., & Brohi, S. N. (2020). An experimental study to evaluate the performance of machine learning algorithms in ransomware detection. Journal of Engineering Science and Technology, 15(2), 967-981.

[6] Algarni, S. (2021). Cybersecurity attacks: Analysis of "wannacry" attacks and proposing methods for reducing or preventing such attacks in the future. In ICT Systems and Sustainability: Proceedings of ICT4SD 2020, Volume 1 (pp. 763-770). Springer Singapore.