Penerbit Akademia Baru

Journal of Advanced Research Design

Journal homepage:
https://akademiabaru.com/submit/index.php/ard
ISSN: 2289-7984

Comparative Study on Ransomware Detection using Machine Learning

Abdelaziz Atef[1,*], Ashraf Tammam[1]

[1] Computer Engineering Department, Faculty of Engineering, Arab Academy for Science, Technology and Maritime, Transport, Cairo, Egypt

ARTICLE INFO

Article history:
Received 7 January 2025
Received in revised form 24 July 2025
Accepted 25 July 2025
Available online 8 August 2025

Keywords:
machine learning, detection, ransomware, static analysis, dynamic analysis, hybrid models, ensemble, feature sets, SVM, random forest, CNN, LSTM, transfer learning, reinforcement learning, autoencoders, GANs

ABSTRACT

Ransomware is one of the serious threats to the kind of cyber technology that is emerging, more precisely because of the high level at which businesses are now warming up to platforms on the internet. In most instances, normal traditional approaches to security, among the lot like antivirus and firewalls, fail, given the level of sophistication and high dynamism involved during ransomware attacks. This review is on the application of several machine-learning detection approaches for ransomware using static, dynamic, and hybrid feature sets. The paper compares the accuracy, precision, recall, and F1-scores for different ML algorithms such as SVM, Random Forest, CNN, LSTM, ensemble methods and hybrid models. The result has been remarked that the ensemble method and hybrid models perform better in all aspects than the individual model. These challenges explore not only the diversity of the dataset in ML-based ransomware detection but also the balance between negative/false positives and negatives, including the ability to accommodate new variants of ransomware. Work in this direction would, therefore, indicate that advanced hybrid models, for example, combinations like Transfer Learning with Reinforcement Learning, Autoencoders with Random Forest, and Generative Adversarial Networks with LSTM, are going to contribute toward the improvement of ransomware detection and mitigation to a much greater extent. This study provides valuable insights for future research on ransomware detection, identifying effective techniques and areas for improvement in detection and mitigation.

1. Introduction

Ransomware has rapidly become one of the largest threats to cybersecurity, in terms of volume and impact, since it infects victims' devices and data and asks for money in return for a decryption key. Ransomware attack techniques have rapidly become so advanced that these threat agents, when coupled with conventional security measures, often leave standard antivirus solutions and firewalls falling short of detecting and mitigating ransomware attacks. The demand for mechanisms that can effectively detect and prevent ransomware attacks is increasingly needed as more and more businesses and services go online. Immediately distinguishable types of ransomwares. Different types of ransomwares include Crypto-Ransomware, Locker-Ransomware, Scareware, Doxware, Ransomware-as-a-Service (RaaS) [1-3].

* *Corresponding author*
E-mail address: Abdelaziz.atef@hotmail.com

https://doi.org/10.37934/ard.141.1.232240

In this regard, ML has proved an essential enabler by offering sophisticated ways for detecting and classifying ransomware into various types regarding several features extracted from the data. Basically, ransomware detection by machine learning algorithms works by training models against vast datasets that include known benign and malicious files, extracting relevant features from them, and then classifying newly encountered files as safe or dangerous.

This paper compares between some of the various ensemble machine learning approaches that are using in Ransomware detection and other traditional machine learning like random forest machines, Convolutional Neural Networks, Support Vector Machines, and Long Short-Term Memory networks and Hybrid Models [4-7]. The performance is measured based on metrics like accuracy, precision, recall, and F1-score. According to collected and comparing results, the combination of several classifiers together with ensemble methods and the combination of different machine learning models or algorithms by hybridization approaches, for instance, hybrid SVM and neural network, hybrid CNN and random forest, achieve better performance than other algorithms under consideration for all metrics. The aim of the paper outlined here is to help focus future research efforts through recognition of effective methods and underexplored areas.

2. Background and Related Work

Ransomware detection has seen enormous changes in its techniques due to the research work targeting static, dynamic, and hybrid approaches. Research related to static analysis examination of file properties without executing them has been done with the work of Kolbitsch *et al*., and Shafiq *et al*., [4]. All these studies showed that Support Vector Machines effectively detected malware via static characteristics but also proved their weaknesses against obfuscation. In dynamic analysis, the behavior of files is monitored as they execute their instructions. Egele *et al*., [8] developed a system for identifying and describing ransomware based on the observed behavior, called API calls and categorizing it as benign or malicious behavior by machine learning techniques. *Sikorski* and *Honig et al.,* [8] advocated dynamic analysis with an emphasis on malware behavior, and the authors also conceded dynamic analysis to be obfuscation-resistant while agreeing on its resource-intensive characteristic.

New are the hybrids between the static and dynamic methods as an attempt to harness the strengths of both approaches. Hybrid architectures proposed by A. Vehabovic *et al.,* [9] combine static and dynamic aspects using ensemble learning to improve detection accuracy. Indeed, research studies have been used in the application of machine learning algorithms in ransomware detection. Works implementing SVM, RF, CNN, LSTMs, and ensemble methods have been applied and each of these demonstrates specific strengths. For example, in comparative studies of ensemble methods and hybrid model techniques are conducted by Ispahany *et al.*, [10] gave better performance towards achieving high accuracy in detection.

However, there are still some major ransomware detection issues with machine-learning approaches. Diversity and representativeness of the training dataset are critical for machine learning models to be effective, as highlighted in several works. Other significant challenges include how to strike a balance between the two: the trade-off between false positives and false negatives, where the higher the false positive rate, many unnecessary alerts are incurred, and the higher the false negative rate, many missed detections; and the fact that ransomware continuously evolves, requiring the model to have periodic updates and retraining against the new variants. Essentially, these challenges require more research in earnest on developing systems for ransomware detection that are better and more robust [11].

Another attempt presented a custom-made system and used machine learning to classify the malicious behavior of the actual ransomware specimens to classify 40 ransomware attacks as ZeroAccess, CryptoLocker, and Zeus [12]. Investigation is aimed to check the power of evolutionary genetic algorithm. For experimental support, the resources and system requirements are given in the alphabetical follow. 15 Cam Wallpapers can be easily install on an android device. Finally, living with up-to-date tools and the most recent operating systems and require having back-up of important data to diminish the influences on ransomware falls on 13.

The detection of ransomware is a significant issue because apart from technical, cultural, and strategic measures to identify, analyze, and mitigate the ransomware, it also requires policies, legal measures, public education, and international cooperation to combat against ransomware threats [13,14]. The growth of ransomware has been outstanding in number and popularity and warts more attention for better study and to ultimately design an accurate and efficient tool for identification and elimination of any ransomware on the infected system. In this spectrum, attempts and efforts to create new techniques are countless. Many methods of dynamical or statistic characteristics must be analyzed because it is a content-based method along with input alike behavior analysis. Generally, these methods are based on artificial intelligence, learning machines, and signal processing, etc. Rajendra et al. carried out state of the art research at architectural level to review the previous work and to give an overview of ransomware detection in a survey.

Notwithstanding the progress in machine learning-based systems, there exist a few challenges while dealing with systems that detect ransomware. The effectiveness of the models depends on the diversity and representativeness of the training data sets. The trade-off between false positives and false negatives is such that high false positives result in unnecessary alerts, while high false negatives result in missing out on ransomware. More importantly, the ever-changing nature of ransomware requires models to be retrained or updated regularly with new variants in ransomware. These challenges need solutions before practical and reliable ransomware detection systems can be developed.

3. Dataset

The dataset used in this experiment is a very well-chosen collection of samples from open repositories. It contains ransomware and benign files in their mixture for training and testing a model with a broad representative sample set. This dataset includes many types of ransomwares such as CryptoLocker and WannaCry, plus massive benign files typical of user applications (see Table 1). The static attributes include among other things, file size, file type, and entropy, whereas the dynamic attributes include among other things, API call sequences and system behavior, and hybrid features are those features that amalgamate the static and dynamic characteristics. A multifaceted feature set is quintessential for portraying the wide range of behaviors exhibited by ransomware.

Further data preparation for the analysis included the preprocessing steps in data cleaning, normalization of feature values, handling missing data, and handling the categorical variables to change such data into numerical formats. The preprocessed data was used to partition the available data into training and testing datasets. About 80% went to train the models, while the rest of it was kept checking the models. This ensures that the models are well trained with the maximum amount of data and, in turn, leave enough data for adequately rigorous performance estimation. This makes the nature of the dataset very vigorous and up to making powerful machine learning models for effective categorization and labeling of ransomware through careful preprocessing methods.

Table 1
Provides a clear overview of the dataset, including the types of features, example features, the number of samples, and their sources

Feature Set	Description	Example Features	Number of samples	Source
Static Features	Attributes that do not change during execution	File size, file type, entropy	10,000	Open Repository Kaggle-Ransomware Dataset [15]
Dynamic Features	Behavior observed during execution	API call sequences, system behavior	8,000	Public Repository Kaggle-API Call based Malware Dataset [16]
Hybrid Features	Combination of static and dynamic features	Both static and dynamic attributes	6,000	Mixed Sources Dataset - Malicia Project [17]
Behavioral Features	User activity patterns	User activity logs	5,000	Industry Source VirusShare Dataset [18]
Network Traffic Feature	Packet data and connection patterns	Network packets, connection logs	7,500	Lab-Collected Data Stratosphere IPS Project Datasets [19]

4. Methodology

In this work, several machine learning techniques, such as Support Vector Machines, Random Forest, Convolutional Neural Networks, Long Short-Term Memory, and ensemble, are tested for ransomware detection in this paper. Data gathering is the first step in this implementation pipeline's many stages. It contains a representative data sample of benign and ransomware files. The data is randomly gathered by public sources with heterogeneous data.

The next step in feature selection is to identify which features are relevant to the dataset. The features could contain hybrid attributes that combine both static and dynamic qualities, as well as static attributes like file size and entropy. This wide range of variables enables our models to capture all ransomware actions successfully. Pre-processing cleans and arranges the data before the training session. It is the transformation of categorical variables into numerical representations, missing data treated, and normalization of feature values. Afterwards, 80% of the preprocessed data will be used for training, and 20% for testing and validation purposes, in other words 10% for testing and 10% validation. The dataset splitting done by train-test split method.

Every Machine Learning model is trained using all the selected features. To increase performance, we concentrate on hyperparameter optimization using SVM and Random Forest. CNNs are created with binary representations that resemble images, and the LSTM network of API calls models the data in a sequential fashion. The total detection is increased by the ensemble approaches, which integrate the advantages of the individual classifiers. Hybrid models combine machine learning algorithms or models to exploit their strengths in detection. To the end, it becomes based on criteria such as accuracy, precision, recall, and F1 score and they will, therefore, measure the models for performance and potential to be the best method for detecting and classifying ransomware in the future. The results from the literature are very confirmatory, where ensemble methods and the use of hybrid models on all such metrics performed very well. This methodology explains an efficient machine-learning model for ransomware detection: it should have a wide array of features and good evaluation metrics.

5. Results and Discussion

A few interesting results were obtained through the evaluation of different machine learning algorithms in ransomware detection. We evaluated each method with accuracy, precision, recall, and F1-score performance measures through performance parameters such as the true positive (TP), false positive (FP), true negative (TN), and false negative (FN) [20].

First, the degree to which the machine learning algorithms accurately forecast the classification of both positive and negative data is known as accuracy. It has the following quantification:

$$\text{Accuracy} = \frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \quad (1)$$

While focusing primarily on the TP and TN, accuracy is a crucial parameter to compute. However, the following formula is used to calculate precision and shows the percentage of projected positive samples that show a positive result.

$$\text{Precision} = \frac{\text{TP}}{\text{TP}+\text{FP}} \quad (2)$$

Recall is indicating how many actual positive samples the machine learning system can recognize. It is calculated in the following way.

$$\text{Recall} = \frac{\text{TP}}{\text{TP}+\text{FN}} \quad (3)$$

Ultimately, the F1-score is taken into consideration when the FPs and FNs are critical [x] and serves as an accurate measure of the ML learning Algorithm's effectiveness. The formula below is used to calculate the F1-score:

$$\text{F1\_score} = 2 \times \left(\frac{\text{precision} \times \text{recall}}{\text{precision}+\text{recall}}\right) \quad (4)$$

On all the metrics, ensemble methods had high F1-score of 95.5%, recall of 95%, precision of 96%, and accuracy of 97%. They can combine many models, and as a result can rally the accuracy of the detection better than that given by any single model.

Support Vector Machines (SVM) with an accuracy of 92%, precision of 90%, recall of 91%, and F1-score of 90.5% Although SVM proved helpful in static feature analysis, it considered less stable relative to the ensemble-based approaches. The model Random Forests showed even better performances in terms of dynamic analysis: 95 and 94% of accuracy, 93% of recall and 93.5% of F1-score. The results were very promising with 96% in accuracy, 95% in precision, 94% in recall, and 94.5% in F1-score when Convolutional Neural Networks (CNN) well-known for the image recognition was employed, especially in considering the binary files as images. Deep neural network architectures like LSTM suitable for sequential data provided an accuracy of 94%, a precision of 92%, a recall of 93%, and an F1-score of 92.5% for the same dataset. Hybrid approaches are suitable for datasets that encompass a variety of data types, including static properties of files, dynamic behavioral data, network traffic data provided accuracy of 96%, a precision of 95%, a recall of 97%, and an F1-score of 96% for Hybrid CNN and Random Forest and provided accuracy of 96%, a precision of 94%, a recall of 96%, and an F1-score of 95% for Hybrid SVM and Neural Network (see Table 2). Performance of

the different algorithms against four important metrics: accuracy, precision, recall, and F1-score. The analysis per algorithm is based on the data as shown in Figure 1. The relationship between Recall and F1-Score for various algorithms used in ransomware detection as shown in Figure 2.

This highlights which method is best and at the same time are weak points. While SVMs and Random Forests are competitive static and dynamic analysis approaches, ensemble methods leverage the power of several models and Hybrid models offering a much richer set of solutions. Ease of implementation and efficiency in processing are some of the reasons why traditional machine learning techniques like SVM, decision trees and Naïve Bayes have become highly popular. These traditional algorithms can be processed quickly since they need limited computational resources unlike deep learning structures that require large computational power. The accuracies of these models can be high when applied to well-defined tasks or with predefined features. Moreover, the models produced by traditional ML techniques are easily interpretable, which makes security professionals capable of comprehending and having trust on their decisions. However, traditional ML techniques need a large amount of manual feature engineering with lots of domain expertise to extract meaningful features from raw data. They are sometimes ill-suited for complex and high-dimensional data, usually found in ransomware detection scenarios. Traditional models also require more frequent updates to catch up with evolving ransomware patterns, further escalating the risk of missing new threats in each update cycle. These approaches work poorly with imbalanced datasets, which is often the case with cybersecurity problems. Deep learning methods are very powerful for the extraction of features and handling large volumes of sequential and complex data with their related network structures. Such models outperform many other models in classifying ransomware patterns since they can learn complicated data representations.

The most obvious strength of deep learning is its potential for discerning patterns in time-series data, a task at which conventional ML performs rather poorly. Another striking benefit of deep learning is that it provides models that are robust against evasion techniques these include code obfuscation and polymorphism. Although deep learning models come with lots of advantages, they require very large resource necessities with high computational power and memory resources; some of these present limitations towards real-time applications. Similarly, deep learning models often require massive amounts of labeled training data, which may not be readily available or may be costly to collect. Additionally, deep learning models are for the most part uninterpretable "black boxes." Hence, a lack of interpretability makes it hard for security professionals to understand the reason behind every detection. Ensemble learning techniques include Random Forest, AdaBoost, and Gradient Boosting, which help in the advancement of ransomware detection systems through enhanced performance by combining multiple models, thereby ensuring better accuracy, and reducing problems of overfitting. It takes the advantages offered by different algorithms and gives good generalization to the unseen data. Perform well in handling class imbalance, which is a very common problem of classes in cybersecurity datasets, and their performance is always robust when various metrics are checked. Lastly, the ensemble learning methods are computationally expensive in training, since they train various models, so that the added complexity in the ensemble models could take quite a while to train, meaning that they are not good for real-time detection. Further, tuning and maintaining these multiple models is tricky and might be time-consuming in their management, as balancing in contribution must be judiciously carried out. The uniqueness of such hybrid architectures lies in the power to absorb the best from two strategies: deep learning and classical machine learning techniques.

This allows, in turn, to cater to class imbalances as well as detect better accuracy levels in the process of detection via the process of extracting salient features through deep learning and then classification through traditional ML. They provide a way of handling various kinds of data flexibly

and provide a way of obtaining robust feature representations through unsupervised learning components for Contractive Autoencoders. When using hybrid models, XAI integration brings in the aspect of transparency, which helps to make security professionals understand and trust the outcomes of detections. Indeed, the most serious drawback of hybrid approaches is their consumption of computing power and memory resources. In fact, the combination of several algorithms might add to the overall complexity of the system and, thereby, probably extend the long development and tuning times. A tougher rate should be maintained for hybrid models due to their very nature: the fact that its components are hybrid means that they need to be maintained current and working properly. Trade-offs in the management of model complexity, resource consumption, and performance are typically not trivial and require specific optimization to ensure the practical implementation of this approach in real-world cases. Given the above observations, it highlights the importance of using varied sets of features and thorough evaluation criteria as assisted techniques for the design of ransomware detection models. They also talked about challenges like diversity of dataset, false positives, or false negatives and how the models in the future will have to adapt to new ransomware variants, and hence, for the models to continue to provide support, research will continue to persist, and the models will have to be updated over time.

Table 2
The performance metrics of machine learning algorithms

Algorithm	Accuracy	Precision	Recall	F1-Score
SVM	92%	90%	91%	90.5%
Random Forest	95%	94%	93%	93.5%
CNN	96%	95%	94%	94.5%
LSTM	94%	92%	93%	92.5%
Hybrid CNN + RF	96%	95%	97%	96%
Hybrid SVM + NN	96%	94%	96%	95%

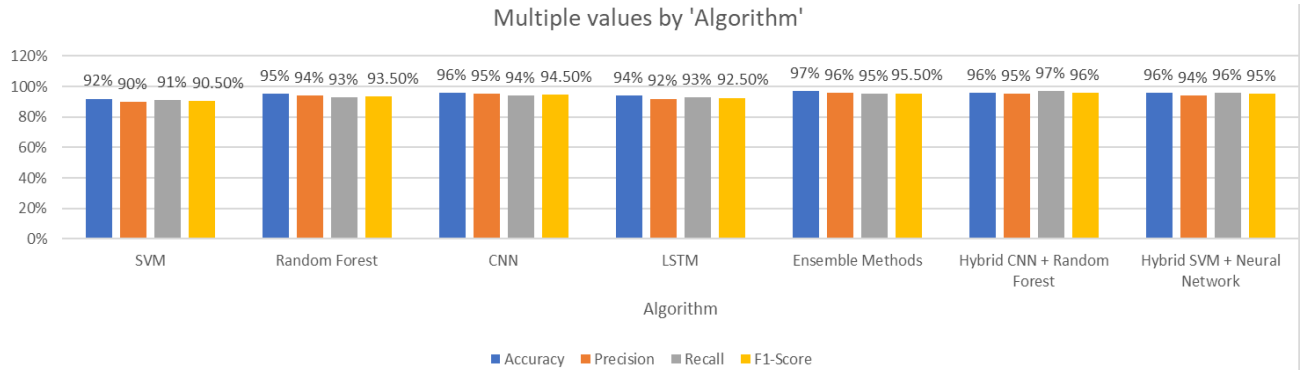

Fig.1. Shows the performance of various algorithms based on accuracy, precision, recall, and F1-score

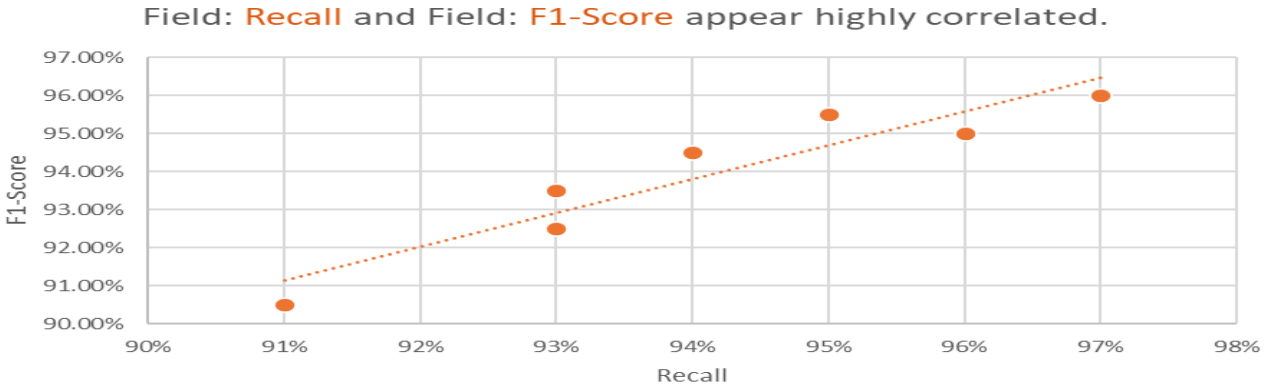

Fig. 2. shows the relationship between Recall and F1-Score for various algorithms used in ransomware detection

6. Conclusion

The paper provides a fair comparison among different machine learning algorithms for the ransomware detection problem and increases the importance of an accurate feature set and trusted evaluation criteria in ransomware detection. The results show that hybrid models and ensemble approaches outperform individual models in F1-score, accuracy, precision, recall, SVM, Random Forest, CNN, and LSTM. The results are very promising in terms of the potentials this machine learning technique will bring to the enhancement of our capability for proactive prevention and detection of ransomware attacks. However, challenges remain, among which is the great diversity of data sets; it stands on a fragile balance between false positives and false negatives; and there is huge diversity in types of ransomwares. All these problems require more research and frequent updates of the model, along with evolving techniques of detection. Designing new machine learning models, especially hybrid models, such as Transfer Learning combined with Reinforcement Learning, Autoencoders with Random Forest, and Generative Adversarial Networks combined with LSTM can be enhance the ransomware detection and could be the main emphasis of the future studies. The extent of ransomware attack detection and mitigation would be far enhanced using such advanced hybrid models.

Acknowledgement

This research was not funded by any grant.

References

[1] Razaulla, Salwa, Claude Fachkha, Christine Markarian, Amjad Gawanmeh, Wathiq Mansoor, Benjamin CM Fung, and Chadi Assi. "The age of ransomware: A survey on the evolution, taxonomy, and research directions." *IEEE Access* 11 (2023): 40698-40723. https://doi.org/10.1109/ACCESS.2023.3268535

[2] Alraizza, Amjad, and Abdulmohsen Algarni. "Ransomware detection using machine learning: A survey." *Big Data and Cognitive Computing* 7, no. 3 (2023): 143. https://doi.org/10.3390/bdcc7030143

[3] Gómez Hernández, José Antonio, Pedro García Teodoro, Roberto Magán Carrión, and Rafael Rodríguez Gómez. "Crypto-ransomware: A revision of the state of the art, advances and challenges." *Electronics* 12, no. 21 (2023): 4494. https://doi.org/10.3390/electronics12214494

[4] Ahmed, Usman, Jerry Chun-Wei Lin, and Gautam Srivastava. "Mitigating adversarial evasion attacks of ransomware using ensemble learning." *Computers and Electrical Engineering* 100 (2022): 107903. https://doi.org/10.1016/j.compeleceng.2022.107903

[5] Smith, Daryle, Sajad Khorsandroo, and Kaushik Roy. "Machine learning algorithms and frameworks in ransomware detection." *IEEE Access* 10 (2022): 117597-117610. https://doi.org/10.1109/ACCESS.2022.3218779

[6] Oz, Harun, Ahmet Aris, Albert Levi, and A. Selcuk Uluagac. "A survey on ransomware: Evolution, taxonomy, and defense solutions." *ACM Computing Surveys (CSUR)* 54, no. 11s (2022): 1-37. https://doi.org/10.1145/3514229

[7] McIntosh, Timothy, A. S. M. Kayes, Yi-Ping Phoebe Chen, Alex Ng, and Paul Watters. "Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions." *ACM Computing Surveys (CSUR)* 54, no. 9 (2021): 1-36. https://doi.org/10.1145/3479393
[8] Bang, Jiseok, Jeong Nyeo Kim, and Seungkwang Lee. "Entropy Sharing in Ransomware: Bypassing Entropy-Based Detection of Cryptographic Operations." *Sensors* 24, no. 5 (2024): 1446. https://doi.org/10.3390/s24051446
[9] Vehabovic, Aldin, Nasir Ghani, Elias Bou-Harb, Jorge Crichigno, and Aysegül Yayimli. "Ransomware detection and classification strategies." In *2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 316-324. IEEE, 2022. https://doi.org/10.1109/BlackSeaCom54372.2022.9858296
[10] Ispahany, Jamil, MD Rafiqul Islam, Md Zahidul Islam, and M. Arif Khan. "Ransomware detection using machine learning: A review, research limitations and future directions." *IEEE Access* (2024). https://doi.org/10.1109/ACCESS.2024.3397921
[11] Zhang, Angela, Lei Xing, James Zou, and Joseph C. Wu. "Shifting machine learning for healthcare from development to deployment and from models to data." *Nature biomedical engineering* 6, no. 12 (2022): 1330-1345. https://doi.org/10.1038/s41551-022-00898-y
[12] Herrera-Silva, Juan A., and Myriam Hernández-Álvarez. "Dynamic feature dataset for ransomware detection using machine learning algorithms." *Sensors* 23, no. 3 (2023): 1053. https://doi.org/10.3390/s23031053
[13] Robles-Carrillo, Margarita, and Pedro García-Teodoro. "Ransomware: An Interdisciplinary Technical and Legal Approach." *Security and Communication Networks* 2022, no. 1 (2022): 2806605. https://doi.org/10.1155/2022/2806605
[14] Lubin, Asaf. "The law and politics of ransomware." *Vand. J. Transnat'l L.* 55 (2022): 1177.
[15] www.kaggle.com. "Ransomware Detection Data Set," n.d.
[16] Catak, Ferhat Ozgur, Ahmet Faruk Yazı, Ogerta Elezaj, and Javed Ahmed. "Deep Learning Based Sequential Model for Malware Analysis Using Windows Exe API Calls." *PeerJ Computer Science* 6 (July 27, 2020): e285. https://doi.org/10.7717/peerj-cs.285
[17] Imdea.org. "Dataset - Malicia Project," 2016.
[18] External Data Source. "VirusShare Is a Collection of Malware Used for Malware Analysis and Machine Learning." Impactcybertrust.org, 2019. https://www.impactcybertrust.org/dataset_view?idDataset=1271.
[19] Stratosphere IPS. "Datasets Overview, " n.d. https://www.stratosphereips.org/datasets-overview.
[20] Abdelkreem, Eslam, Sherif Hussein, and Ashraf Tammam. "Feature engineering impact on position falsification attacks detection in vehicular ad-hoc network." *International Journal of Information Security* 23, no. 3 (2024): 1939-1961. https://doi.org/10.1007/s10207-024-00830-2