**Transactions on Engineering and Computing Sciences - Vol. 11, No. 1**
**Publication Date: February 25, 2023**
**DOI**:10.14738/tecs.111.13973.
Ba'abbad, I., & Batarfi, O. (2023). A Short Criteria-Based Review of High-Performance Proactive Ransomware Analysis Models. Transactions on Engineering and Computing Sciences, 11(1). 168-179.




# A Short Criteria-Based Review of High-Performance Proactive Ransomware Analysis Models

**Ibrahim Ba'abbad**
Department of Information Technology,
King Abdulaziz University, Jeddah, Saudi Arabia

**Omar Batarfi**
Department of Information Technology,
King Abdulaziz University, Jeddah, Saudi Arabia.

**Abstract**

**The Software that contains destructive commands intended to damage user data and systems is known as malware. The malware's objective is to take over the system without authorization, access private information, or even corrupt it. Over the past few years, several malware threats have been reintroduced. To demand a ransom, malicious software known as ransomware locks the victim's system or encrypts important data. Numerous studies have been conducted to stop and quickly recognize ransomware attacks. Therefore, detecting ransomware attacks as early as possible avoids the execution of malicious instructions that would otherwise damage user data and the system. In this study, we examine eight criteria across several aspects of the suggested solution to evaluate six state-of-the-art high-performance proactive ransomware detection models. Depending on how well each requirement is met, points are given to it. The evaluation results are compared with the claimed accuracy results. The ranking outcomes and potential areas for future improvement outlined by each model will then be presented. To the best of our knowledge, researchers in the field of proactive ransomware detection are more interested in increasing classification accuracy than they are in reducing latency. One crucial factor in defining a model as high-performance is latency. Model 5 (M5, Zhang et al. model) thus receives the highest score of 14 points. With only 2.44 seconds, the model minimized the classification latency. After comparison, it is strongly advised to look beyond the capabilities of machine learning algorithms to quickly identify and stop ransomware attacks.**

**Keywords:** Ransomware Detection; Proactive Analysis; Machine Learning; Classification Accuracy; Classification Latency.

## INTRODUCTION

The community of internet security researchers is very concerned about internet security. Malware is constantly being created by cybercriminals on the dark web to harm legitimate operations. The user's system and data are immediately impacted by ransomware. The attacker can lock the system and encrypt important data to demand a ransom in exchange for the decryption key needed to decrypt encrypted data. The two primary categories of ransomware are described here: locker ransomware and crypto-ransomware. Due to the complexity of the

decryption technique required for recovery, crypto-ransomware has received a lot of attention in recent literature. To create a stronger cipher, a hybrid encryption system that uses both symmetric and asymmetric encryption can be used. The victim's data is encrypted using effective block symmetric encryption techniques. The symmetric key is then encrypted using the public key, and it will be decrypted using the private key [1].

However, since the end of the 1980s, other ransomware families have emerged. Trojan AIDS, which was created in 1989, was the first known case of ransomware. Floppy disks were speared, and a ransom of $189 was requested [2,3]. Additionally, WannaCry is one of the most recent ransomware attacks, which in 2017 [1] destroyed more than 200 000 systems across 150 countries. At the end of 2015, $352 million was paid in ransom payments worldwide due to Cryptowall, another ransomware outbreak [4]. Therefore, the average ransom requested from an individual victim is $300, whereas the amount increases to $10,000 for a business victim [5]. With more than 64% of all internet ransomware activations coming from email, this method is the most infectious. A phishing email is sent to the victim along with a harmful attachment or link. As soon as the victim responds to this email, the ransomware encrypts their data and displays screen messages asking them to pay a ransom in cryptocurrency (such as bitcoin) [1].

Numerous studies have been conducted as remedies to stop and quickly recognize ransomware attacks. Analysis of network activity is required for ransomware detection. Analysis of ransomware might be static or dynamic. Researchers who used static analysis concluded that it is not useful for the early detection of emerging ransomware families [1]. On the other hand, a closed platform known as a sandbox is used for dynamic analysis of active ransomware behaviors. However, while being examined, the ransomware may react against the victim system [4].

Nowadays, proactive monitoring utilizing artificial intelligence (AI) techniques is used for proactive forecasting more effectively in addition to static and dynamic analysis methods [6]. The systematic extraction of features using standard machine learning (ML) algorithms, however, consumes time and reduces the proactive nature of network monitoring [7]. As a result, ML is not fully investigated because results from current studies on classification latency indicate that there is still room for improvement. Therefore, proactive network monitoring approaches must be developed to attain the highest possible levels of classification accuracy and latency [8].

The following sections make up this document: recent studies for the improvement of proactive detection models for ransomware are presented in Section 2. The methodology for evaluating and comparing the reviewed models is shown in Section 3. The claimed accuracy results in comparison to the evaluation results are discussed and displayed in Section 4. The conclusions and scope for future improvement highlighted by each model are summarized in Section 5.

## RELATED WORK

One of the most well-known cyber hazards is ransomware because of the catastrophic effects it has on the resources of its victims. The fact that ransomware is transmitted globally, much like electronic mail systems, is one factor in such effects [1]. The advent of the Ransomware as a

Service (RaaS) model is another factor. Criminals and ransomware developers have used RaaS to target the victim's computer system.

Network monitoring is a remedy that is crucial to intrusion detection in general. System administrators should continue to monitor network activity for unusual activity. A series of proactive prevention commands are carried out if it is discovered [6]. Analysis of network activity is required for ransomware detection. Analysis of ransomware might be static or dynamic. The ransomware operation code (opcode) is extracted via static analysis to create an n-gram code pattern that may be used to train ML/DL algorithms. The ransomware does not have to be activated by static analysis. It is therefore a safe operation. It will not, however, aid in the early detection of new ransomware families [1]. On the other hand, a closed platform known as a sandbox is used for dynamic analysis of active ransomware behaviors. However, while being examined, the ransomware might react against the target machine. The operating system's I/O operations and application programming interface (API) calls are watched carefully, particularly the encryption procedures. The accuracy of early ransomware detection may be improved by proactive monitoring of critical directories as a preventative measure. Finally, while the hybrid technique is now undesirable due to implementation difficulties, it is far more accurate. Figure 1 illustrates a hierarchical structure of ransomware analysis approaches.

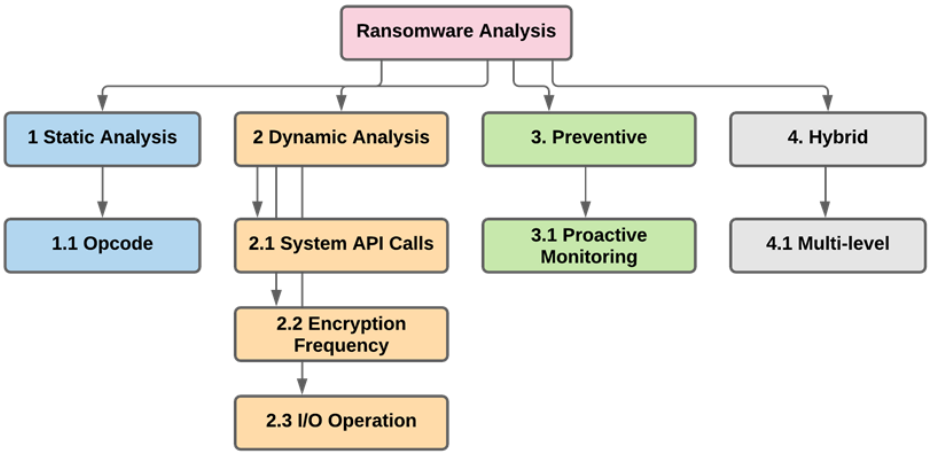



**Figure 1: Hierarchical structure of ransomware analysis approaches**

Recent research has focused on the early detection and prevention of ransomware attacks. Since it makes use of the network edge rather than conventional faraway servers, network edge computing aids in boosting the I/O operations rate between network users and resources. Devices used for edge computing, however, have security flaws. One of the most prevalent types of malware in network edge computing is ransomware. A deep neural network model with an autoencoder was suggested by Abdulsalam et al. [7] to monitor ransomware actions without the requirement for the feature extraction procedure. 942 good-ware samples and 582 ransomware samples are utilized in an open-source dataset. MATLAB software is employed as a simulation tool. The true positive rate for the suggested model is 99.7 percent. The accuracy of the model will be improved in the future to detect threats other than ransomware attacks using a de-noising autoencoder based on dropout training.

Detecting encrypted ransomware attacks through secure socket layer/ transport layer security (SSL/TLS) protocol is a crucial task. Zhang et al. in [9] proposed a system based on dual generative adversarial networks (GAN) for encrypted ransomware detection. The system is named a transferred-generating adversarial network intrusion detection system (TGAN-IDS). Deep convolutional GAN (DCGAN) and transferred GAN (TGAN) are the two primary parts of TGAN-IDS. DCGAN is based on a convolutional neural network (CNN) deep learning algorithm. DCGAN optimizes the performance of its generator (GD) while TGAN is used to optimize its discriminator (DT) performance. TGAN is the core component of the system since its discriminator (DT) reacts as the final detector of anomaly behavior. Three websites—Malware-Traffic-Analysis.net, PacketTotal, and Interactive Online Malware Analysis Sandbox—are used to gather 8175 ransomware instances from seven different families that are all encrypted with the TLS protocol. A random sample of 20,000 normal instances is chosen from the CIC-IDS2017 dataset. A computer running the Ubuntu 18.04 operating system and Python 2.7 as a software development tool are utilized as the testing environment. According to tests, TGAN-IDS increases classification accuracy for all seven families of ransomware by an average of 93.8 percent in 2.44 seconds. Improvement to the system is considered in the future to detect more malicious attacks with enhanced performance.

Homayoun et al. [10] offer the deep ransomware threat hunting and intelligence system (DRTHIS) as a novel idea to quickly and effectively detect and hunt the ransomware threat. Long short-term memory (LSTM) concept and convolutional neural network (CNN) are utilized as the system's primary classifiers. Within the first 10 seconds of an application's operation, DRTHIS can identify ransomware and its family. The suggested model is assessed using a dataset of 204 good-ware samples and 660 ransomware samples. Results indicate that the true positive rate for DRTHIS is 97.2 percent. Future research for detecting a wide range of malware involves using a variety of deep learning training techniques.

A deep learning model based on a neural network algorithm was proposed by Berrueta et al. [11] as an additional effort. In a client-server architecture, all crucial files are saved on the servers, and the client only has access to them via a networked file-sharing service. However, if a crypto-ransomware attack were to target only one client accessing the shared file server, it might infect all the workgroup files. The suggested model tracks file-sharing traffic to look for unusual actions taken by a crypto-ransomware attack, like reading files, writing the encrypted version of files, and deleting files. A dataset is created using 70 samples of crypto-ransomware and 50 hours of benign applications from users who accessed file-sharing servers during 2528 working hours. 80 percent of the formed dataset is used for training and the remaining 20 percent is used for testing. Ten additional undiscovered crypto-ransomware samples are exclusively utilized for validation. Among the three algorithms that were looked at—decision trees, ensemble trees, and artificial neural networks—a neural network algorithm with three hidden layers was chosen. According to the results, the model has a false positive rate of 0.004 percent with more than 2400 hours of user working traffic. 99.9 percent of crypto-ransomware attacks can be detected in an average of 30.2 seconds. Only Microsoft Windows desktop and laptop operating systems are considered as client computers in this study; operating systems for mobile phones are not. Since the current version of the model exclusively addresses crypto-ransomware threats, an adaptive version is needed to expand the model's usability.

Additionally, Adamu and Awan [4] analyze ransomware behaviors across 5 selected features out of 30.000 features using machine learning algorithms. The ransomware dataset from the Resilient Information Systems Security research group (RISS), which includes 942 examples of good-ware and 582 examples of ransomware from 11 different families, is used. As a result, the support vector machine (SVM) classifier achieves an accuracy of 88.2 percent. The next improvement step is believed to be network behavior prediction utilizing machine learning and agent-based approaches.

Homayoun et al. [12] suggest a model with a sequence pattern mining (SPM) technique for detecting crypto-ransomware activities in the network in 2020. The dataset consists of 220 Windows Portable Executable (PE32) benign applications from the website (portableapps.com) and 1,624 (PE32) ransomware samples from the website (virustotal.com). The model is trained using the J48, Random Forest, Bagging, and Multilayer Perceptron (MLP) algorithms. Results reveal a 99 percent accuracy rate in separating ransomware from legitimate software. For more research, considering stream data mining techniques can be a great alternative. The model work for ransomware detection only. It would be interesting to research the model in the fields of IoT platforms and mobile malware detection. Figure 2 illustrates the claimed accuracy of reviewed ransomware analysis models.

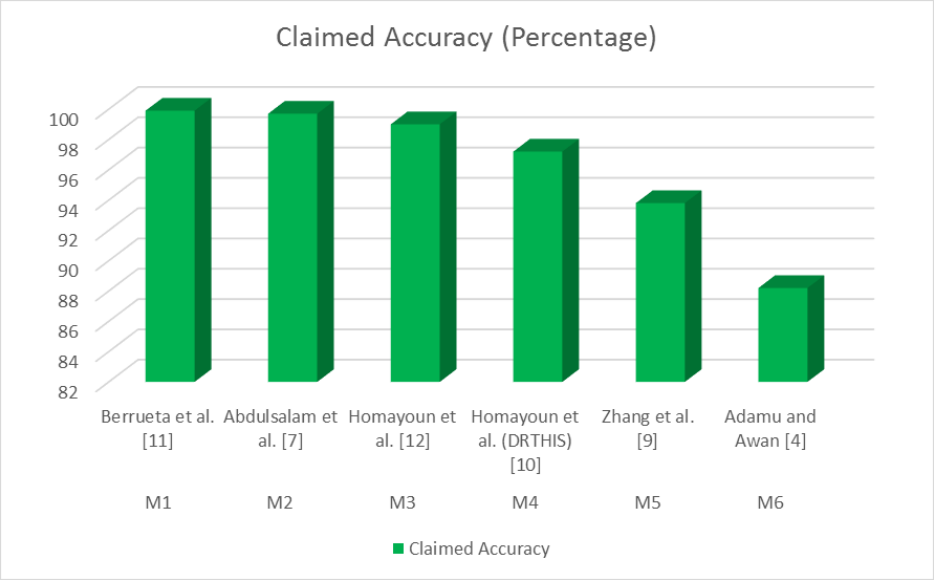



**Figure 2: Claimed accuracy of ransomware analysis models**

## METHODOLOGY

We searched reputable journals and conferences in general digital libraries, including but not limited to IEEE Xplore, ScienceDirect, and research gate, to perform this brief review. The articles are the most recent from 2019 to 2022. After searching, 70 papers met the specified area expectations. After that, we started looking at each paper's abstract and the authors' suggested solutions. The twenty-two most relevant articles in the field of ransomware detection models overall are picked. The analysis of a few chosen publications is then continued. The six articles that best meet the focused research topic of high-performance proactive ransomware analysis models are then chosen.

Six models are compared using eight criteria that relate to various aspects of the suggested solution. The criteria examine each model based on the ransomware sample quantity, ransomware families variety, feature selection process, model hybridity, processing phases multiplicity, malware detection capabilities, latency minimization, and results validation. The accuracy results get crisper and the model detection capabilities of that variety of instances are increased as malware samples in datasets grow in size and have a wide range of instances. Model detection techniques become novel when they are hybrid coupled with several processing stages, especially if the model latency is controlled. The process of feature selection reduces model latency, resulting in faster detection. Finally, the model conclusion is based on trustworthy outcomes as a result of the results being validated. These factors determine how the six models are rated in terms of points subject to the degrees of criterion fulfillment.

Each criterion has a set number of points that can be used to evaluate each model. Depending on whether the expectations of the criteria were met, points were assigned in increments of 3 to 1 or 2 to 1. Expectations can be binary in some cases. Therefore, there will be a choice between the greatest rank and zero. The eight criteria are shown in table 1, along with a description and points. In order to represent the review results visually, MS Excel is employed as a data visualization tool.

**Table 1: Evaluation criteria for reviewed ransomware analysis models**

| C# | Criterion | Criterion Description | Points | Ref |
|---|---|---|---|---|
| C1 | Ransomware samples quantity | If # ransomware samples > 1000 | 3 | [9] |
| | | If # ransomware samples > 100 and < 1000 | 2 | |
| | | If # ransomware samples < 100 | 1 | |
| C2 | Ransomware families variety | If # ransomware families > 3 | 2 | [4] |
| | | If # ransomware families <= 3 | 1 | |
| C3 | Feature selection process | Feature selection is performed | 2 | [4] |
| | | Feature selection is not performed | 0 | |
| C4 | Model hybridity | The model uses more than one technique | 2 | [10] |
| | | The model uses only one technique | 1 | |
| C5 | Processing phases multiplicity | If # processing phases >= 2 | 2 | [9] |
| | | The model has only one phase | 1 | |
| C6 | Multiple malware detection capabilities | The model can be used to detect other malware types | 3 | [4] |
| | | The model can be used to detect other ransomware families | 2 | |
| | | The model can be used to detect only experimented ransomware | 1 | |
| C7 | Latency minimization | The model is interested in minimizing latency | 3 | [10] |
| | | The model is not interested in minimizing latency | 0 | |
| C8 | Results validation | Results are validated | 2 | [11] |
| | | Results are not validated | 0 | |

## DISCUSSION AND RESULTS

Eight criteria were used to evaluate six ransomware analysis models, and the findings are described in table 2 with total points and ranking. They are then shown in figure 3. Model 5 (M5, [9]) receives a score of fourteen. The data set used included 20000 normal samples from CIC-IDS2017 coupled with 8175 ransomware samples organized into seven families. Additionally, the model combines a convolutional neural network (CNN) technique with dual generative adversarial networks (GAN). There are two stages to the detection procedure. Since Ubuntu 18.04, an open-source operating system, was utilized in the testing environment, which is more configurable than Windows OS, the model reduced latency. As a result, it can be altered until the classification latency is reduced to only 2.44 seconds. However, the future challenge for this model is to figure out how to make the system more effective at detecting malicious attacks while maintaining classification accuracy.

Model 4 (M4, [10]) comes in second place with thirteen points. Since the model achieves a true positive rate of 97.2 percent, the results are validated. The latency was reduced to a level of 10 seconds. Even yet, it appears to take a while for the LSTM approach to detect malware. Since it needs four linear layers per cell, LSTM requires more time to train.

Meanwhile, model 2 (M2, [7]) has a moderate score of 11 points. The latency was not minimized by the model. However, the authors claimed that the model gets 99.7 percent accuracy. MATLAB is a simulation tool used in a testing environment that is rapidly evolving with new editions every year. The algorithms are continually being improved. In an average of 30.2 seconds, the model 1 (M1, [11]) proposal can detect crypto-ransomware attacks. The proposal is based on a deep neural network with three hidden layers, whose classification takes time due to their level of complexity. The model may become faster as future recommendations are made because mobile operating systems are less sophisticated than the Windows OS used in desktop and laptop computers. Furthermore, the model only considers crypto-ransomware attacks, thus there are fewer features to examine than there would be for a model that considers a variety of attack types. As a result, it receives a medium score of ten points. For model 6 (M6, [4]), selecting five features appears to be a smart decision in terms of analysis time. The writers, however, made no mention of decreasing latency. Additionally, it may reduce the precision of ransomware detection. Feature selection with various combinations can improve the performance of the model.

Model 3 (M3, [12]), on the other hand, receives seven points for being in the lowest position. Instead of being able to recognize different ransomware families, the model can only detect experimental ransomware. Additionally, the model did not reduce the latency. However, the dataset utilized in separating the ransomware from the good software is specified with high accuracy through the ransomware pattern used by SPM. Since then, the authors claimed that the model gets 99 percent accuracy. Figure 4 displays the ransomware analysis models' available latency durations. Table 3 provides a comprehensive summary of ransomware analysis models testing environments, claimed results, evaluation results, and future improvements.

**Table 2: Evaluation results of reviewed ransomware analysis models**

| Models | | Criteria | | | | | | | | Total Points (19) | Raking |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | | |
| M1 | Berrueta et al. 2022, [11] | 1 | 1 | 0 | 1 | 1 | 1 | 3 | 2 | 10 | 4 |
| M2 | Abdulsalam et al. 2020, [7] | 2 | 2 | 0 | 2 | 1 | 2 | 0 | 2 | 11 | 3 |
| M3 | Homayoun et al. 2020, [12] | 3 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 7 | 6 |
| M4 | Homayoun et al. 2019, [10] | 2 | 1 | 0 | 2 | 1 | 2 | 3 | 2 | 13 | 2 |
| M5 | Zhang et al. 2022, [9] | 3 | 2 | 0 | 2 | 2 | 2 | 3 | 0 | 14 | 1 |
| M6 | Adamu and Awan, 2019, [4] | 2 | 2 | 2 | 1 | 1 | 2 | 0 | 0 | 10 | 5 |

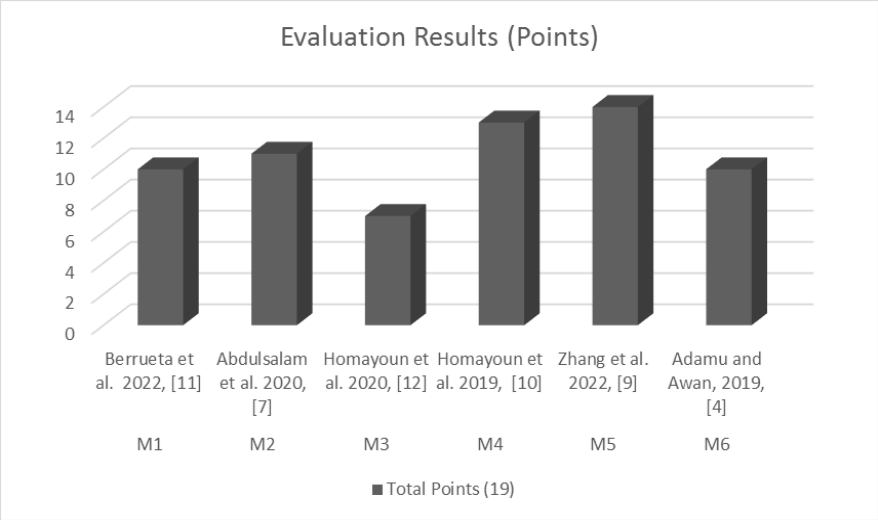



**Figure 3: Evaluation results of reviewed ransomware analysis models**

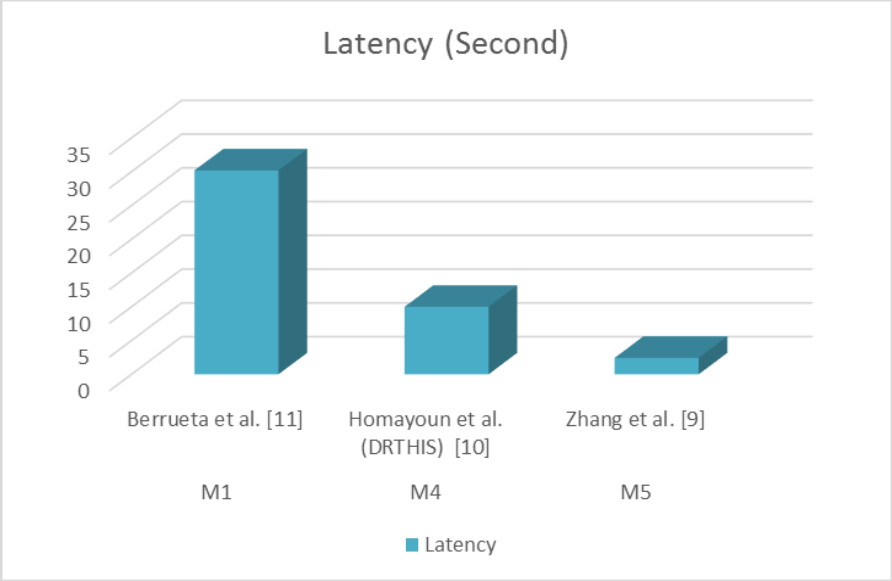



**Figure 4: Available latency durations of ransomware analysis models**

## CONCLUSION AND FUTURE WORK

Ransomware is malware that affects the user's system and data harmfully. With more than 64 percent, electronic mail is the most common infectious source on the internet used to activate ransomware. A phishing email is sent to the victim along with a harmful attachment or link. Numerous studies have been conducted to stop and quickly recognize ransomware attacks. According to the studied literature, the best ransomware analysis model would have accurate results, the shortest latency, and be able to distinguish ransomware from legitimate software early on. Therefore, novel techniques are still required to provide the best performance in terms of both accuracy and latency. Consequently, these models can handle the ransomware attacks' rapid evolution.

In this study, we assessed six cutting-edge, high-performance proactive ransomware detection models. Eight criteria covering various aspects of the suggested solution provide the basis for the evaluation. The evaluation results are compared with the claimed accuracy results. The rankings were then displayed, along with each model's recommendations for potential future improvements.

To the best of our knowledge, researchers in the field of proactive ransomware detection are more interested in increasing classification accuracy than they are in reducing latency. One crucial factor in classifying a model as high-performance is latency. Model 5 (M5, Zhang et al. model) thus receives the highest score of 14 points. With only 2.44 seconds, the model minimized the classification latency.

After comparison, it is strongly advised to look beyond the capabilities of machine learning algorithms to quickly identify and stop ransomware attacks. This will open up new opportunities for the research community in the fields of intrusion detection systems and ransomware detection and prevention systems.

**Table 3: Ransomware analysis models testing environments, claimed results, evaluation results, and future improvements.**

| Model Ref | Experiments | | | Claimed Res. | | Evaluation Res. | |
|---|---|---|---|---|---|---|---|
| | Dataset | Algorithms | Testing Tools | Accuracy (percent) | Latency (sec) | Points (19) | Rank |
| **M1 [11]** | 80 crypto-ransomware (10 for validation) with 50 working hours of benign traffic. | Decision Trees Ensemble Trees Artificial Neural Networks | N/A | 99.9 (Artificial Neural Networks) | 30.2 | 10 | 4 |
| **Potential areas for future improvement** | Win. OS desktops are only considered while mobile phones are not. An adaptive version is required to detect not only crypto-ransomware. | | | | | | |
| **M2 [7]** | Resilient Information Systems Security (RISS) research group`s dataset | Deep neural network model with an autoencoder | MATLAB software | 99.7 | N/A | 11 | 3 |
| **Potential areas for future improvement** | De-noising autoencoder based on dropout training will be used as a new training method to detect threats other than ransomware. | | | | | | |
| **M3 [12]** | 1,624 ransomware from virustotal.com 220 benign applications from portableapps.com | A model with sequence pattern mining (SPM) technique | N/A | 99 | N/A | 7 | 6 |
| **Potential areas for future improvement** | Stream data mining techniques may decrease the latency. IoT platforms and mobile malware detection are interesting areas to investigate. | | | | | | |
| **M4 [10]** | 660 ransomware and 204 good-ware | Long short-term memory (LSTM) and convolutional neural network (CNN) under the “DRTHIS” model | Keras deep learning framework | 97.2 | 10 | 13 | 2 |
| **Potential areas for future improvement** | Ensemble Deep Neural Network (DNN)/ CNN/ RNN techniques deployment is required to hunt a wide range of malware. | | | | | | |
| **M5 [9]** | 8175 ransomware from websites. | Deep Convolutional | Ubuntu 18.04 OS | 93.8 | 2.44 | 14 | 1 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 20000 normal samples from CIC-IDS2017. | GAN (DCGAN) is based on Convolutional Neural Network (CNN) | with Python 2.7 | | | | |
| **Potential areas for future improvement** | | Improvement to the system is considered in the future to detect more malicious attacks with enhanced performance. | | | | | |
| **M6 [4]** | Resilient Information Systems Security (RISS) research group`s dataset | Support Vector Machines Random Forest Decision Trees Bayesian Network Artificial Neural Network Logistic Regression | N/A | 88.2 (SVM) | N/A | 10 | 5 |
| **Potential areas for future improvement** | | Prediction of network behavior using machine learning and agent-based is considered. | | | | | |

## References


[1]. S. H. Kok, A. Abdullah, and N. Jhanjhi, *Early detection of crypto-ransomware using pre-encryption detection algorithm*. Journal of King Saud University - Computer and Information Sciences, p. S1319157820304122, Jul. 2020, doi: 10.1016/j.jksuci.2020.06.012.

[2]. Y. A. Ahmed, B. Koçer, S. Huda, B. A. Saleh Al-rimy, and M. M. Hassan, *A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection*. Journal of Network and Computer Applications, vol. 167, p. 102753, Oct. 2020, doi: 10.1016/j.jnca.2020.102753.

[3]. S. Mohurle and P. Manisha, *A brief study of Wannacry Threat: Ransomware Attack 2017*. ijarcs, 2017.

[4]. U. Adamu and I. Awan, *Ransomware Prediction Using Supervised Learning Algorithms*. in 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), Istanbul, Turkey, Aug. 2019, pp. 57–63. doi: 10.1109/FiCloud.2019.00016.

[5]. R. Richardson, *Ransomware: Evolution, Mitigation and Prevention*. vol. 13, no. 1, p. 13, 2017.

[6]. G. Nguyen, S. Dlugolinsky, V. Tran, and A. Lopez Garcia, *Deep Learning for Proactive Network Monitoring and Security Protection*. IEEE Access, vol. 8, pp. 19696–19716, 2020, doi: 10.1109/ACCESS.2020.2968718.

[7]. G. AbdulsalamYa'u, G. K. Job, S. M. Waziri, B. Jaafar, N. A. SabonGari, and I. Z. Yakubu, *Deep Learning for Detecting Ransomware in Edge Computing Devices Based On Autoencoder Classifier*. in 2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization

Techniques (ICEECCOT), Mysuru, India, Dec. 2019, pp. 240–243. doi: 10.1109/ICEECCOT46775.2019.9114576.

[8]. H. Hindy et al., *A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems*. IEEE Access, vol. 8, pp. 104650–104675, 2020, doi: 10.1109/ACCESS.2020.3000179.

[9]. X. Zhang, J. Wang, and S. Zhu, *Dual Generative Adversarial Networks Based Unknown Encryption Ransomware Attack Detection*. IEEE Access, vol. 10, pp. 900–913, 2022, doi: 10.1109/ACCESS.2021.3128024.

[10]. S. Homayoun et al., *DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer*. Future Generation Computer Systems, vol. 90, pp. 94–104, Jan. 2019, doi: 10.1016/j.future.2018.07.045.

[11]. E. Berrueta, D. Morato, E. Magaña, and M. Izal, *Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic*. Expert Systems with Applications, vol. 209, p. 118299, Dec. 2022, doi: 10.1016/j.eswa.2022.118299.

[12]. S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, and R. Khayami, "*Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence*. IEEE Trans. Emerg. Topics Comput., vol. 8, no. 2, pp. 341–351, Apr. 2020, doi: 10.1109/TETC.2017.2756908.