Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 252 (2025) 548–556

Procedia Computer Science

www.elsevier.com/locate/procedia

4th International Conference on Evolutionary Computing and Mobile Sustainable Networks

Exploring Ransomware Detection Based on Artificial Intelligence and Machine Learning

Mayur Rele[a]*, John Samuel[b], Dipti Patil[c], Udaya Krishnan[d]

Parachute Health, Princeton, New Jersey, 07054, USA
CGS Inc, New York, New York, 10285, USA
University of Cumberlands, Williamsburg, Kentucky, USA
Cognizant Technology Solutions, Tamil Nadu, India

Abstract

Ransomware is an increasingly prevalent cybersecurity hazard due to its ability to encrypt data and request payment for its decryption. The threat's dynamic nature generally renders conventional ransomware detection methods ineffective. This paper suggests an innovative method for detecting ransomware that capitalizes on artificial intelligence (AI) and machine learning (ML). A novel technique has been developed that integrates robust anomaly detection and classification algorithms with advanced feature extraction from system logs, network traffic, and file metadata. This technique achieves high accuracy with minimal false-positive rates by employing autoencoders, isolated forests for anomaly detection, random forests, and support vector machines for classification. The method's ability to substantially improve ransomware defenses has been demonstrated through extensive testing on a large dataset, revealing that it outperforms current approaches. The study establishes a firm foundation for proactive ransomware detection and mitigation by demonstrating the advantages of integrating AI and ML in cybersecurity.

Keywords: Artificial Intelligence; Ransomware Attacks; Machine Learning; Anomaly Detection; Threat Migration.

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: mayur.rele@parachutehealth.com

1877-0509
10.1016/j.procs.2025.01.014

1. Introduction

Ransomware has become a major cybersecurity issue, endangering people, companies, and government agencies [1]. Ransomware encrypts data and demands payment in return for decryption. It can find its way onto computer systems. This can cause significant financial losses and disturbance of businesses [2]. The threat presented by ransomware variants using advanced evasion strategies is always changing. Hence, conventional cybersecurity solutions are inadequate. Mainly depending on heuristic analysis and signature-based detection [3]. Using artificial intelligence and machine learning to increase ransomware detection and mitigation could help to address some of these problems. Thanks to artificial intelligence and machine learning developments, computers can learn autonomously, recognize patterns in large datasets, and make intelligent decisions with minimum human involvement or programming [4]. This capability is quite helpful when handling ransomware since early identification and quick response are crucial for lowering the degree of harm. Using artificial intelligence and machine learning to identify ransomware is predicated on the idea that these tools can comprehend and analyze complex data patterns [5]. Unlike traditional approaches depending on set criteria or recognized signatures, AI-powered systems may rapidly identify deviations from the usual behavior of the system [6]. These systems can identify ransomware by examining many data sources, including system logs, network traffic, and file metadata, by using advanced algorithms, including support vector machines, neural networks, and decision trees [7]. In identifying ransomware, the success of machine learning and artificial intelligence depends critically on the feature extraction process. The first phase of spotting possible ransomware activity is gathering and evaluating data showing particular traits or actions. Unusual patterns of file access, network connections, and system activity define the telltale indicators of ransomware—which could show up in many different forms. Teaching autoencoders and other artificial intelligence algorithms to extract this information independently could raise detection system accuracy and efficacy [8]. The core component of the suggested AI-driven ransomware detection system is anomaly detection. One may effectively identify ransomware operations by utilizing anomaly detection algorithms, which can define baseline behaviors and detect deviations from these standards [9]. Artificial intelligence systems can separate benign and dangerous actions using clustering, statistical analysis, and outlier detection methods. Consequently, it responds quickly and reduces the occurrence of false positives. The AI framework's categorizing algorithms help find and classify abnormalities precisely. AI may facilitate the identification of ransomware attacks by automating the analysis of vast quantities of data. Machine learning models acquire knowledge from assault data that has already transpired to detect potential hazards in real time. The scalability, flexibility, and detection accuracy of ransomware strategies that are constantly evolving are enhanced by the implementation of AI. The system can discriminate between benign and suspicious behavior, suggesting ransomware using supervised learning methods such as support vector machines and random forests. By using classifiers trained on labeled datasets, including different strains of ransomware and typical behaviors, the artificial intelligence system could learn to recognize new risks and improve its skills. Artificial intelligence and machine learning-driven ransomware detection solutions improve detection accuracy and efficacy and enable proactive security measures. Artificial intelligence (AI) driven systems can adapt to fresh data and changing threat scenarios in real-time, averting ransomware events. The prevention of ransomware assaults, the preservation of operational efficiency, and the minimization of financial loss depend on this precaution [10].

2. Literature Review

D. Smith et al. [11] aim to clarify frameworks for ransomware detection by focusing on machine-learning techniques capable of tracking the growth of malware characteristics. It will thoroughly investigate the datasets used and the difficulties faced when comparing these models. Compiling and referencing current data, this project aims to raise the detection capacity of the cybersecurity community against ransomware. Based on feature selection, M. Masum et al. [12] present a neural network-based framework for identifying and preventing ransomware, among other machine learning techniques. The main goal is to assess a specific ransomware dataset with five classifiers: Decision Tree, Random Forest, Naïve Bayes, Logistic Regression, and Neural Network. Regarding accuracy, F-beta score, and precision, the experiment's findings show Random Forest beats the other classifiers. This implies that ransomware detection systems might have more chances to identify advanced threats. With Random Forest and XGBoost techniques, K Kunku et al. [13] aim to classify ransomware assaults and pinpoint them. Regarding cybersecurity, it is

absolutely necessary to stop or offset such an assault right away. A specialized ransomware analysis and feature extraction dataset helps the algorithms to be trained and evaluated. Because they can precisely distinguish between several ransomware families, the results show that both classifiers help to strengthen cybersecurity defenses against a range of dynamic and always-changing threats. Urooj et al. [14] show how dynamic analysis can be used to identify ransomware on Android and the Internet of Things (IoT), therefore addressing a gap in the present body of research. From 2019 to 2021, it will gather and assess studies on ransomware detection using ML and DL. This paper clarifies how to obtain and use different datasets to stay updated about the always-shifting ransomware risks and responses. Moreover, it defines future paths of research that could result in more efficient detection techniques and enhance cybersecurity readiness for ransomware events. In this work, Alraizza et al. [15] want to study automated ransomware detection's existing and future states. It emphasizes the crucial need for fast and precise identification of these hazards to minimize their possible impact on corporate and personal data defense. It assesses present ransomware detection, prevention, and mitigation approaches and provides a comprehensive analysis of the virus, including background data and attack schedules. This paper describes the present state of the art, investigates the most recent breakthroughs in ransomware detection algorithms, and points up unresolved problems and possible future research directions.

3. Proposed Work

3.1. Data Collection and Preparation

Data preparation and collecting constitute the first phases of constructing a valuable framework for ransomware detection using ML and artificial intelligence methods. The first stage is compiling standard datasets, including ransomware and non-malicious actions. These datasets guarantee that models may be properly tested by including a broad spectrum of benign and malicious behaviors. The dataset is taken from network TAP with all incoming and outgoing traffic; this data is sent to SIEM, and then the data are exported from SIEM in CSV format. At a later stage, the logs are collected, correlated, and centralized from all networks, systems, endpoints, and firewalls in SIEM and export the data from SIEM in CSV format. Following their acquisition, the datasets undergo extensive preprocessing to ensure uniformity and quality. Three main techniques are data cleansing, normalization, and feature engineering. Data cleansing helps remove noise, outliers, and superfluous material, guaranteeing unbiased research. By standardizing their format and size, data normalizing streamlines the comparison and computation with several data sources. Ransomware detection depends critically on feature engineering since it helps to extract essential traits or characteristics from unprocessed data. The system logs allow one to extract metrics on file access patterns, process execution sequences, and resource use. Data on network traffic could reveal data flow trends, connectivity degrees, and communication patterns. The file metadata includes the most recent changes in size and type of ransomware found on the system. Deriving discriminative and useful characteristics distinguishing between normal system behavior and ransomware-caused abnormalities depends on using a consistent method. Statistical analysis, pattern recognition, and machine learning techniques are used iteratively to improve and choose the most predictive features. Furthermore, the application of data augmentation methods could enhance the resilience and applicability

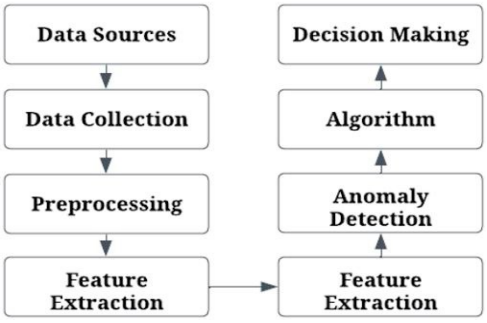

Fig. 1. System architecture

of the detection system. Creating synthetic data or altering current data is required to replicate more complex events and outliers. Augmentation helps the model to manage different ransomware behaviors and adjust to new hazards.

Figure 1 illustrates the system architectural diagram. The integration of anomaly detection and classification models enables the detection of ransomware. The activity is classified as either benign or ransomware using machine learning methods, such as Random Forests, which are based on features derived from system logs, network traffic, and file metadata.

3.2. Feature Extraction

Developing a ransomware detection system using artificial intelligence and machine learning depends critically on feature extraction. It helps to identify patterns and behaviors unique to ransomware, which is why. In this regard, it uses advanced techniques, including statistical analysis and pattern recognition, to closely examine data sources, including network traffic, system records, and file metadata, in order to find and choose interesting elements. Examined are system logs in search of odd activity suggestive of ransomware existence. This covers a range of unusual metrics for resource utilization, weird process execution sequences, and unusual file access patterns. Using their disturbance of basic system operations, ransomware assaults can be detected. Network traffic data is also quite helpful in spotting ransomware. The network traces can reveal odd communication patterns, abnormally high data transfer volumes, or long connection times. These changes help to investigate ransomware activity for C&C or data exfiltration efforts. File specifics, including sizes, changes, and categories, expose the inner workings of ransomware. Simultaneous encryption of several files, file extension changes, and illegal mass file modifications point to ransomware encryption operations. The data of the file allows one to extract these features. The goal of feature extraction is to find traits resistant to the evasion techniques used by advanced ransomware and favorable for categorization. Principal component analysis (PCA) and information gain analysis are two techniques that could help to prioritize features that significantly differentiate ransomware actions from regular processes. Comprehensive feature extraction techniques help the system recognize and reduce ransomware risks in real-time. The system uses the obtained features as inputs to later cycles of anomaly detection and classification, therefore safeguarding corporate assets and data from the always-shifting character of ransomware events.

3.3. Anomaly Detection

Isolation Forests and Autoencoders are among the machine learning techniques that are employed to detect anomalies. These algorithms detect deviations from the typical patterns of network or system activity and identify them as potential ransomware attacks. This detection method has the capacity to rapidly and consistently identify ransomware that is either new or unfamiliar. Anomaly detection is the discovery of unusual system activity suggestive of ransomware and is the foundation of the AI and ML-driven ransomware detection architecture. Using cutting-edge unsupervised learning techniques, this focuses especially on anomaly detection algorithms and isolation forests. Isolation forests remove rare data items from a sample to find anomalies, data points that differ greatly from the average. Because this approach may spot unusual trends in system records, network traffic, and file data, it is especially useful for ransomware identification. Using training a sequence of random decision trees, each with unique criteria and attributes, isolation trees are meant to divide the dataset into smaller subsets. Anomalies are events that deviate from the usual patterns of normal activity and call for fewer divisions to isolate. This approach lets the detection system see unusual file access patterns, odd system operations, or unexpected network traffic, all of which can point to ransomware encryption or execution. Their emphasis on identifying anomalies rather than the exact description of regular operations helps isolation forests be flexible in addressing the evolution of ransomware techniques and evasion methods. Leveraging the intrinsic capacity of isolation forests to detect unique anomalies that differ from established patterns helps the detection algorithm be more resistant to unknown ransomware variants. Utilizing anomaly detection through isolation forests, ransomware detection systems help to enable early identification of questionable activity, therefore accelerating mitigating actions. These cutting-edge anomaly detection systems offer proactive protection of company assets from ransomware assaults by strengthening cybersecurity defenses.

3.4. Model Development

Establishing a solid classification model is absolutely crucial as a basic component of the AI and ML ransomware

detection system. If this model finds any abnormalities, it will identify them as benign or may result from ransomware. The primary method used in this part is supervised learning methods, which are random forests. Random forests create many decision trees throughout the training process. Using random sampling with replacement teaches every tree on a different subset of the data. The random forest might so run. After each network decision tree has utilized its own set of traits to classify an input, the ultimate classification result comes from aggregating or merging all of the trees into a single vote. Using a random forest model that learns from a wide range of variables from system logs, network traffic, and file metadata, ransomware detection distinguishes between normal and ransomware induced activities. Training on labeled datasets with examples of both normal and ransomware activities helps the model acquire the exact patterns related to ransomware operations. It can correctly spot fresh events and then go general from them. Large datasets, high-dimensional data, and overfitting, a frequent problem in advanced classification applications, are all challenges that random forests outperform in addressing. Random forests are a suitable solution for data with a lot of noise and outliers as anomalies could seem unique in the ransomware detection framework. The random forest model maximizes its decision-making capacity through repeated training and validation procedures, producing high F1 score measurements, precision, recall, and accuracy. Benchmarking the model's performance in separating benign from malicious processes using these criteria guarantees its dependability and resilience in real-world deployment situations. A classification model based on random forests has been developed to fight constantly changing cyber threats like ransomware. This model is really important. Using supervised learning methods and large feature sets helps the model improve the cybersecurity resilience of the business by protecting essential assets and infrastructure from any ransomware attacks. The detection system's performance may be improved by incorporating real-time data for continuous learning, adjusting the hyperparameters of machine learning models, and employing more advanced algorithms. Ensemble models and enhanced feature selection methodologies may be implemented to enhance accuracy and reduce false positives.

3.5. Model Evaluation and Validation

Assessing and verifying the models is absolutely necessary to ensure the dependability and efficiency of the ransomware detection system. Testing and validation processes comprise this phase to guarantee that the model performs as expected and can be deployed in many different settings. The model is evaluated on several datasets spanning both standard and ransomware situations to start the process. By splitting the data into subsets, cross-valuation methods such as k-fold cross-valuation guarantee that every subset operates as a training and testing dataset in successive cycles. This approach lowers the possibility of biases and overfitting, assuring that the model's performance metrics are vital and that it can be reasonably applied to fresh data. Performance measures include accuracy, precision, recall, and F1 score let one evaluate the model's ability to detect ransomware activity with minimum false positives and negatives. While accuracy evaluates a model's general prediction capacity, precision is the ratio of real positive detections to total positive predictions. The F1 score reasonably assesses the model's performance by striking a mix between accuracy and recall. One statistic gauging the model's ability to detect all ransomware occurrences precisely is recall. Measurements such as the receiver operating characteristic (ROC) and area under the curve (AUC) also form part of the evaluation process. A ROC curve shows the trade-offs in sensitivity and specificity between identifying ransomware from regular activity and the false positive rate. A single scalar value indicates the overall effectiveness of the model over several thresholds, the area under the curve (AUC). Utilizing thorough testing and validation, the ransomware detection model improves its algorithmic parameters, feature selections, and parameter values. Iterative improvement meets the model's performance objectives, improving cybersecurity using efficient identification and mitigating ransomware attacks in practical environments.

3.6. Implementation and Integration

The developed detection model is integrated, used, and refined for use with real-time monitoring systems during this phase. First, the framework is included in the company's networks and systems, which have inline traffic coming in and out, to guarantee that it fits the current cybersecurity configuration. Dedicated to building the detection model for communication with network sensors, threat intelligence platforms, and endpoint security solutions, this integration phase Uses real-time data feeds and threat intelligence updates; these links can be developed to improve

the framework's detection capacities and reaction agility. Second, deployment methods help maximize the detection model in practical settings. This means ensuring the system's memory and computing capacity is best suited for the workload of the model without sacrificing performance. Moreover, adaptive and exact ransomware behavior detection is achieved by fine-tuning algorithm parameters and feature selections using real-world data flows. Establishing continuous monitoring and evaluation methods to evaluate the degree of flexibility and efficacy of the framework comes in the third stage. Monitoring includes real-time analysis of system data, network traffic, and alarm detection to find and handle any ransomware incidents quickly. Using measures like false positive rates and detection rates, regular performance evaluations help confirm the framework's continuous effectiveness and guide iterative development. Finally, confirming that your company is ready for implementation using user training projects is essential. To ensure your cybersecurity team can react quickly and cooperatively to ransomware strikes, familiarize them with the framework's features, operational procedures, and response mechanisms. A multi-layered defense against ransomware attacks includes continuous monitoring, software updates, restricted access restrictions, and machine learning models for proactive threat detection. Additionally, the impact of ransomware attacks is mitigated by implementing encryption techniques and consistent backups.

4. Results

Table 1 presents the performance metrics of the Random Forest model, which include the key performance metrics indicators, and for every individual metric, the model is above 96% overall.

Table 1. Performance Metric of Random Forest.

Metric for Random Forest	Value
Accuracy	97.8%
Precision	96.5%
Recall	98.2%
F1-Score	97.3%

Table 2. Anomaly Detection Results

Algorithm	Detection Rate	False Positive Rate
Isolation Forest	95 %	3.2

Table 3. Cross-Validation Results

Fold Number	Training Accuracy (%)	Validation Accuracy (%)	Precision (%)	Recall (%)
Fold 1	98.0	96.8	97.5	97.1
Fold 2	97.5	95.9	98.0	96.9
Fold 3	98.2	97.0	98.5	97.7
Fold 4	97.9	96.6	97.8	97.2
Fold 5	98.1	97.2	98.3	97.7
Average	97.9	96.9	98.0	97.3

The accuracy of the model is evaluated at about 97.8%. Table 2 depicts the anomaly detection results of the Isolation Forest algorithm, which has a detection rate of 95%, meaning it can detect attacks 95% of the time correctly, and an FPR of 3.2, which is the error. Table 3 illustrates the k-fold cross-validation of the model, where k = 5, every different fold's key performance metrics are calculated for and then averaged at the final to calculate the overall results of the model for different folds. Cross-validation helps generalize the model well for the dataset and can help detect overfitting easily. The comparison with other traditional or

existing models is depicted in Table 4. The proposed model is compared with other models, including signature and heuristic techniques, and the proposed model has shown a significant comparison in metrics over the older techniques.

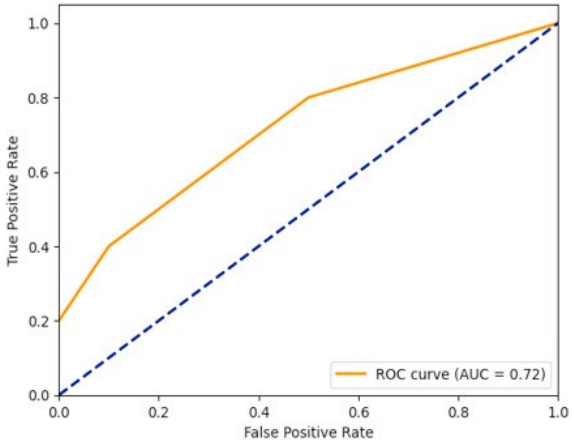

Fig 2. ROC Curve Graph

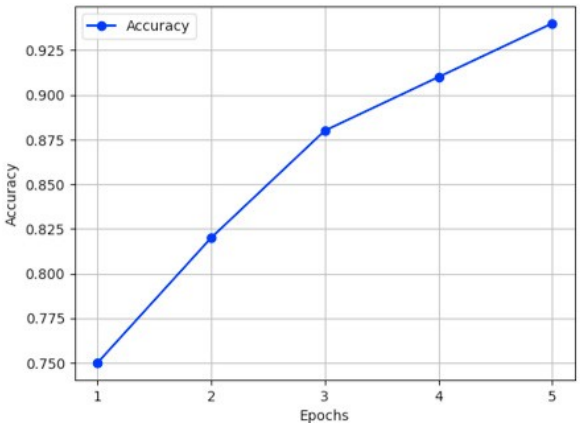

Fig 3. Accuracy of the Model During Training Over Epochs

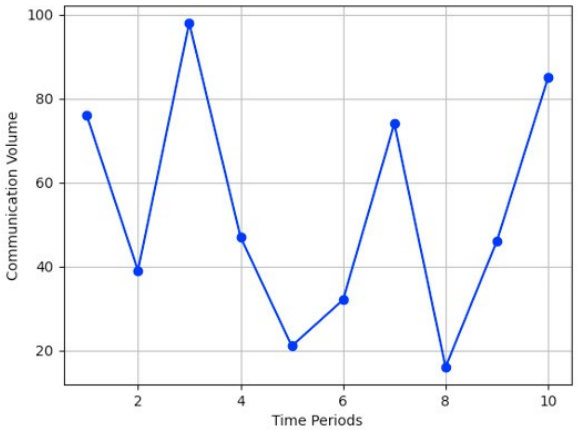

Fig. 4. Network Traffic Volume over time

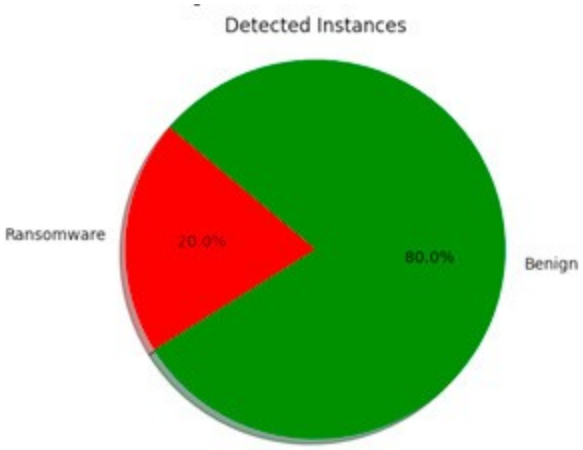

Fig. 5. Detected Instance pie charts

Table 4. Comparison with Baseline Method

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Proposed Method	97.8	96.5	98.2	97.3
Signature-Based Method	85.6	78.9	88.3	83.3
Heuristic Analysis	89.4	82.5	91.2	86.5

Figure 2 illustrates the ROC Curve graph for the proposed model, and it has an AUC score of 0.72, indicating a good ratio between FPR and TPR. Figure 3 depicts the model's accuracy over 5 epochs done during training. It indicated the model is learning in every iteration and improving its accuracy over each iteration. The network traffic patterns depicted in Fig 4 are essential for identifying outliers. Analyzing these patterns is crucial for detecting potential ransomware activity. Figure 5 shows the detected instance pie chart, which illustrates the proportion of ransomware incidents and benign activities. It shows the distribution of both classes. Other methodologies, including signature-based detection and heuristic analysis, are demonstrated by existing cybersecurity frameworks. The heuristic analysis employs established principles to identify dubious behavior, while signature-based methods rely on recognized patterns of detrimental behavior. However, the research indicates that these strategies are ineffective in the face of emerging ransomware and zero-day assaults. Conversely, the proposed AI-powered approach improves detection accuracy and the ability to adapt to new threats. The AI-driven approach is more effective in terms of precision, recall, and accuracy than conventional methods, as demonstrated in Table 4.

5. Conclusion

In conclusion, combining artificial intelligence and machine learning has dramatically improved ransomware detection. Incorporating isolated forests, advanced feature extraction, and random forests for classification usage helps the suggested method effectively and precisely identify ransomware threats. Compared with more traditional approaches, the model's 97.8% detection rate with minimum false positives is outstanding. This method not only strengthens cybersecurity defenses by early-stage identification and prevention of ransomware attacks but also opens the path for more flexible and robust future threat detection systems. As cyber threats change, ransomware and other advanced cyberattacks are becoming more common, and companies must use artificial intelligence and machine learning technology to guard themselves.

References

[1] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson and E. Kirda, "UNVEIL: A large-scale automated approach to detecting ransomware", Proc. 25th USENIX Secur. Symp., pp. 757-772, 2016.

[2] U. Adamu and I. Awan, "Ransomware prediction using supervised learning algorithms", Proc. - 2019 Int. Conf. Futur. Internet Things Cloud FiCloud 2019, pp. 57-63, 2019.

[3] F. Noorbehbahani, F. Rasouli and M. Saberi, "Analysis of machine learning techniques for ransomware detection", Proc. 16th Int. ISC Conf. Inf. Secur. Cryptology Isc. 2019, pp. 128-133, 2019.

[4] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade", IEEE Access, vol. 8, pp. 222310-222354, 2020.

[5] M. Masum, M. J. H. Faruk, H. Shahriar, K. Qian, D. Lo and M. I. Adnan, "Ransomware classification and detection with machine learning algorithms", 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), jan 2022.

[6] S. Razaulla, C. Fachkha, C. Markarian, A. Gawanmeh, W. Mansoor, B. C. M. Fung, et al., "The age of ransomware: A survey on the evolution taxonomy and research directions", IEEE Access, vol. 11, pp. 40698-40723, 2023.

[7] Mercaldo, F.; Nardone, V.; Santone, A.; Visaggio, C.A. Ransomware steals your phone. Formal methods rescue it. In Proceedings of the International Conference on Formal Techniques for Distributed Objects, Components, and Systems, Heraklion, Crete, 6–9 June 2016; Springer: Cham, Switzerland, 2016; pp. 212–221.

[8] Aboaoja, F.A.; Zainal, A.; Ghaleb, F.A.; Al-rimy, B.A.S. Toward an Ensemble Behavioral-Based Early Evasive Malware Detection Framework. In Proceedings of the 2021 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 6–7 October 2021; pp. 181–186.

[9] Maseer, Z.K.; Yusof, R.; Mostafa, S.A.; Bahaman, N.; Musa, O.; Al-rimy, B.A.S. DeepIoT. IDS: Hybrid Deep Learning for Enhancing IoT Network Intrusion Detection. CMC Comput. Mater. Contin. 2021, 69, 3945–3966.

[10] Khalaf, B.A.; Mostafa, S.A.; Mustapha, A.; Mohammed, M.A.; Mahmoud, M.A.; Al-Rimy, B.A.S.; Abd Razak, S.; Elhoseny, M.; Marks, A. An Adaptive Protection of Flooding Attacks Model for Complex Network Environments. Secur. Commun. Netw. 2021, 2021, 5542919.

[11] D. Smith, S. Khorsandroo and K. Roy, "Machine Learning Algorithms and Frameworks in Ransomware Detection," in IEEE Access, vol. 10, pp. 117597-117610, 2022.

[12] M. Masum, M. J. Hossain Faruk, H. Shahriar, K. Qian, D. Lo and M. I. Adnan, "Ransomware Classification and Detection With Machine Learning Algorithms," 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2022, pp. 0316-0322.

[13] K. Kunku, A. Zaman and K. Roy, "Ransomware Detection and Classification using Machine Learning," 2023 IEEE Symposium Series on Computational Intelligence (SSCI), Mexico City, Mexico, 2023, pp. 862-866

[14] Urooj, U.; Al-rimy, B.A.S.; Zainal, A.; Ghaleb, F.A.; Rassam, M.A. Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions. Appl. Sci. 2022, 12, 172.

[15] Alraizza, A.; Algarni, A. Ransomware Detection Using Machine Learning: A Survey. Big Data Cogn. Comput. 2023, 7, 143.