ISSN: 2182-2069 / E-ISSN: 2182-2077

Ransomware Detection with Machine Learning: Techniques, Challenges, and Future Directions - A Systematic Review

Jonathan Ismael Zapata Sandoval[1*], Elian Garcés[2], and Walter Fuertes[3]

[1*]Department of Computer Science, Universidad de las Fuerzas Armadas (ESPE), Av. General Rumiñahui 171103, Quito, Ecuador. jizapata3@espe.edu.ec, https://orcid.org/0000-0002-2929-9953

[2]Department of Computer Science, Universidad de las Fuerzas Armadas (ESPE), Av. General Rumiñahui 171103, Quito, Ecuador. eigarces1@espe.edu.ec, https://orcid.org/0009-0003-4924-9229

[3]Department of Computer Science, Universidad de las Fuerzas Armadas (ESPE), Av. General Rumiñahui 171103, Quito, Ecuador. wmfuertes@espe.edu.ec, https://orcid.org/0000-0001-9427-5766

Received: November 30, 2024; Revised: January 12, 2025; Accepted: January 27, 2025; Published: February 28, 2025

Abstract

Ransomware attacks are one of the most common and dangerous threats in cybersecurity. It prevents users from accessing their systems or personal files and extorts them by demanding a ransom payment. This study aims to identify the most effective machine-learning methods and techniques for detecting and mitigating ransomware attacks. Furthermore, it seeks to determine which features are essential to locate ransomware and which attributes are most effective in achieving this goal. To do so, we conducted a systematic literature review using the PRISMA methodological guide. We focused on selecting only primary empirical studies that will evaluate their effectiveness. The main findings revealed that the studies focus on the analysis of existing datasets, followed by API calls and executable file analysis. Dynamic, static, and network traffic analysis are the most used methods. Furthermore, we found that techniques such as hybrid analysis, digital DNA sequencing, and supervised learning, although less frequently, show their potential in ransomware detection. This research also indicates the limitations of their application, challenges, and future research directions. The results can be beneficial for researchers to learn about the variety of ransomware detection methods to identify ransomware infection at an earlier stage before an attack occurs and develop highly effective solutions.

Keywords: Machine Learning, PICOS, PRISMA, Ransomware, Systematic Review.

1 Introduction

Cyberspace is an exposed area where cybercriminals interact and try to exploit every opportunity to make fraudulent financial gains (Seyedan et al., 2023). Cybercriminals use sophisticated methods like ransomware to target users and businesses. Ransomware is one of the most devastating recent attacks

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 1 (February), pp. 271-287. DOI: *10.58346/JISIS.2025.I1.017*

*Corresponding author: Department of Computer Science, Universidad de las Fuerzas Armadas (ESPE), Av. General Rumiñahui 171103, Quito, Ecuador.

due to its extortionate potential to access a person or business's data, disrupt partial or complete operations, put information into code, and demand illegal recovery payments (Bae et al., 2020).

Detecting and diminishing ransomware attacks is a complex task that industry and academia continue to grapple with. Ransomware cyber attackers continuously develop new variants and new cybercriminal weapons to avoid existing security methods (Akash et al., 2022). Early identification of ransomware attacks at different stages of their lifecycle is critical for prevention and reaction. However, cybercriminals use increasingly sophisticated techniques to hide their immoral activities, making avoiding and detecting such attacks even more challenging (Cao & Jiang, 2024).

To address this issue, researchers conducted several studies to survey and analyze the most applied algorithms and methods in ransomware detection. For example, (Beaman et al., 2021) provide a comprehensive discussion of current advances, opportunities, and future research lines. Similarly, (Alraizza & Algarni, 2023) investigated ransomware detection using machine learning methods, emphasizing the most effective algorithms and their weaknesses (Biswas 2024). Finally, (Razaulla et al., 2023) afford an ordered overview of the ransomware era's evolution, classification, and research directions and significantly contribute to recognizing recent and future tendencies in this subject. These studies demonstrate the scientific and industrial interest in combating these attacks.

Ransomware is an extortion malware from the social engineering attack group that retains data and information on devices hostage until the victim pays a ransom (Aljabri et al., 2024). It prevents access to the information attackers are trying to steal by encrypting files with symmetric or asymmetric cryptographic algorithms. Victims face pressure and demands and choose to pay the ransom. However, perpetrators do not always comply with the offer to restore access (Rakesh et al., 2024). This failure puts the company in a desperate situation, forcing it to restore its processes or operations on its own, resulting in losses in productivity, revenue, customers, and operations, which affects its reputation (Beaman et al., 2021).

The present study aims to identify the methods, techniques, trends, challenges, and future research directions of machine learning models for ransomware detection and prevention (Anny Leema et al., 2024). To achieve this, we use the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodological guide, which allows us to perform a systematic literature review (Haddaway et al., 2022). Using this approach, we systematically evaluate state-of-the-art ML tools and learning models, assessing their effectiveness in detecting ransomware and mitigating its impact.

PRISMA provides a standardized guideline for rigorous systematic reviews that ensures that study selection, data extraction, and analysis are transparent and replicable (Haddaway et al., 2022). In the context of ransomware cyberattacks, several studies employed PRISMA to examine different types of attacks and mitigation techniques to ensure quality in collecting reviewed articles (Kavibharathi et al., 2021). Indeed, researchers used it to identify detection techniques, providing a detailed and structured assessment of existing studies; explore methods of attack detection, prevention, and mitigation, providing a critical view of trends in the literature; and eventually, identify defense mechanisms to ensure a comprehensive and well-structured review of relevant publications worldwide (Cheng et al., 2021).

The main contribution of this study is to make available to the researcher the current state, new variants, and techniques for using machine learning models to detect and prevent ransomware (Park et al., 2019). It also seeks to determine which features are essential to identify ransomware and which attributes are most effective in achieving this goal. In addition, this study presents its challenges, future research directions, and limitations.

The remainder of the article is structured as follows: Section 2 details the procedure used in this bibliographic research, following the PRISMA guidelines. Section 3 presents the evaluation of results and discussion based on the results obtained during the execution of the PRISMA phases. Here, we highlight the 36 primary studies found, performing analysis and interpretation by research question in such a way that we show the most relevant findings. Finally, in section 4, we highlight the most important conclusions, challenges, limitations, and opportunities for future lines of research.

2 Methodology

This section focuses on the process well-known by PRISMA, a methodological framework widely used in scientific research to ensure the rigor of systematic literature reviews and synthesize evidence from available studies (Haddaway et al., 2022). PRISMA delivers a complete protocol covering various essential elements of the research process, such as objectives, research questions, selection of scientific databases, study inclusion and exclusion criteria, search strategies, methods for selecting primary studies, data extraction and cleaning techniques, and analysis procedures.

The PRISMA procedure also facilitates the quality assessment of included studies, allowing researchers to filter and blend consistent data. This process is fundamental to synthesizing scientific evidence, especially when considering trends, challenges, and future directions of machine learning methods in ransomware detection. By evaluating the quality of individual studies, scientists ensure that reliable and convincing bases support the conclusions formulated.

Additionally, PRISMA's emphasis on replicability is crucial. Within this study, replicability or reproducibility refers to the ability to repeat a procedure in different situations with different subjects and researchers. In cybersecurity research, findings could be replicated, allowing other researchers to corroborate the results and build on already-established knowledge (Cheng et al., 2021). The systematic documentation of the research process, which PRISMA promotes, including inclusion and exclusion criteria, search methodologies, and data extraction techniques, ensures that future studies can replicate and verify the presented findings.

The PRISMA methodological guide within the present research was essential, as it offers a detailed process and a checklist that ensures severe and accurate searches, resulting in valid findings (Haddaway et al., 2022). In addition, it allowed us to identify and assess the quality of the included studies, which in turn allows for a more robust synthesis of the available scientific evidence. There is also a notable amount of evidence that the scientific community has applied this methodology in systematic reviews on ransomware and cybersecurity attacks. Figure 1 presents a flowchart visually illustrating the selection process and preliminary results, providing a clear perspective of how the studies were filtered and analyzed. These visual tools improve the process's clarity and facilitate its understanding during the systematic review.

Research Questions

The process began with the problem statement, at which stage we formulated the research questions, which we drafted technically based on the works of (Beaman et al., 2021; Alraizza & Algarni, 2023; Razaulla et al., 2023):

RQ 1: What are the most used machine learning methods and techniques for detecting ransomware, and what features and attributes are essential and effective in achieving this goal?

RQ 2: What tools are used by ransomware to implement machine learning methods and techniques in detecting and mitigating?

RQ 3: Which machine learning algorithms have proven most effective in detecting and preventing ransomware?

RQ 4: What are the main challenges, future research lines, and limitations of detecting using machine learning?

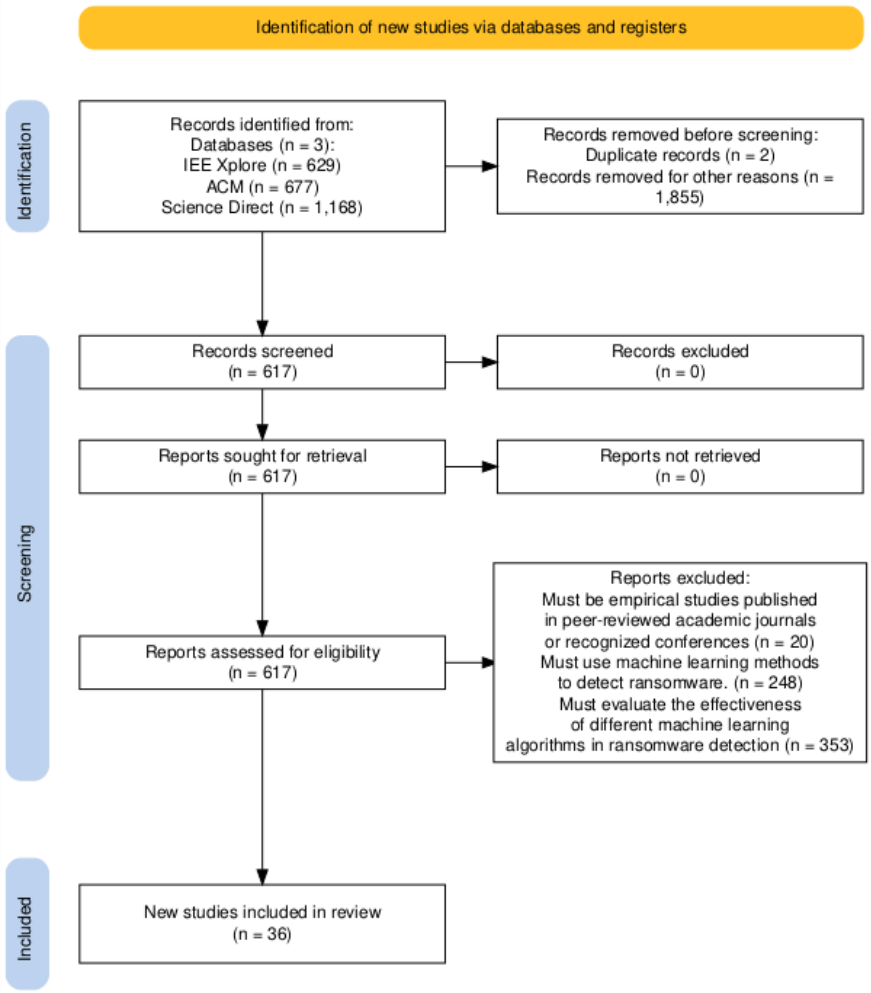


Figure 1: PRISMA 2020 Flowchart Illustrates this Research's Procedure and Preliminary Results.

Source: Haddaway 2022

Eligibility Criteria

We only included studies that use machine learning algorithms for ransomware detection with accurate measurements, published in the last five years.

Information Sources

We used IEEE Xplore, ACM Digital Library, and ScienceDirect, which are crucial digital databases offering access to relevant engineering and computing research.

Search Strategy

We use the PICOS method to define the Search Strategy (Methley et al., 2014). This strategy allows us to conduct a more sensitive search and identify relevant studies for systematic reviews in technology and science contexts. This method helps formulate precise research search strings and ensures the review is comprehensive and appropriate. Each component of the process is detailed below. Once we explain the method, we apply it to our study:

- **P** (Population): Specifies the subject group or population of interest for the study.
  - "Ransomware", "Ransomware families", "Locky-ransomware", "Crypto-ransomware", "WannaCry Ransomware"
- **I** (Intervention): Specifies the type of intervention or exposure that researchers evaluate.
  - "Machine Learning", "Machine Learning Algorithms", "Neural Networks", "Classification ", "Methods", "Techniques", "Deep Learning"
- **C** (Comparison): Identifies the group or intervention with which researchers will compare the central intervention.
  - "Dynamic Detection Algorithms vs. Static Detection Algorithms"
- **O** (Outcome): Describes the results or effects that researchers intend to measure.
  - "Detection Rate", "Precision", "False Positive Rate".
- **S** (Study Design): Specifies the type of study design to include in the review, such as clinical trials or cohort studies.
  - "Empirical Studies", "Comparative Analyses"

Once the search strings and their variants were defined using PICOS, we combined these terms with Boolean operators. We applied the following search strings to each digital database. Table 1 lists the results found.

Table 1: Articles Found According to Applied Search Strings

Database	Search String	Number of articles
IEEE Xplore	("Ransomware" OR "Crypto ransomware") AND ("Machine Learning" OR "Machine Learning Techniques" OR "ML") AND ("Algorithms" OR "Methods" OR "Techniques" OR "Classification" OR "Dynamic Analysis" OR "Static Analysis")	629
ACM	("Ransomware" OR "Crypto ransomware") AND ("Machine Learning" OR "Machine Learning Techniques" OR "ML") AND ("Algorithms" OR "Methods" OR "Techniques" OR "Classification" OR "Dynamic Analysis" OR "Static Analysis")	677
Science Direct	("Ransomware" OR "Crypto ransomware") AND ("Machine Learning") AND ("Algorithms" OR "Dynamic Analysis" OR "Static Analysis")	1168

The first searches began in May 2024 in the abovementioned databases, which we selected for their availability and access. Subsequently, we expanded the search strategy by identifying keywords related to the PICOS method and combining them with Boolean operators “AND” and “OR”, as illustrated in Table 1. Specifically, we obtained 629 articles in IEEE Xplore, 677 in ACM, and 1168 in Science-Direct. Before selecting articles, we defined the inclusion and exclusion criteria, which we list below.

Inclusion Criteria

- Studies must be empirical research published in peer-reviewed academic journals or presented at recognized conferences.
- Articles must use machine learning methods to detect ransomware.
- Studies should evaluate the effectiveness of different machine-learning algorithms in detecting ransomware.
- Articles published between 2020 and May 2024, both inclusive.

Exclusion Criteria

- Studies that do not provide empirical results relevant to ransomware detection.
- Studies that use non-representative or irrelevant data sets for ransomware detection.
- Research that lacks a precise and reproducible methodology for evaluating ransomware detection.
- Studies that focus solely on theoretical or conceptual aspects of ransomware detection without providing practical, measurable, or applicable results.

Classification of Information

We extracted data on algorithms and methods, validation techniques, data sets, software tools, and performance metrics from the selected articles.

3 Evaluation of Results and Discussion

According to the PRISMA methodological guide and the search strategy, we considered 617 suitable articles from IEEE Xplore, ACM, and Science Direct, as shown in Figure 1. After applying the inclusion and exclusion criteria, we discarded 581 articles that did not focus on ransomware detection using machine learning, were not empirical studies, did not include quantitative results, or went out of context by offering only theoretical concepts about ransomware. Finally, we selected 36 primary articles to continue with the respective analysis. Then, we read, revise, and analyze deeply the information provided in each article. The purpose was to resolve the research questions individually and then classify the information correspondingly. The findings we describe are below:

RQ 1: *What are the most used machine learning methods and techniques for detecting ransomware, and what features and attributes are essential and effective in achieving this goal?*

The most prominent methods are Dynamic Analysis and Static Analysis, each with considerable use in the selected articles (12 and 18 studies, respectively). In addition, network traffic analysis emerges as a critical aspect of ransomware detection, with five studies. Though less commonly used, methods such as Hybrid Analysis, Digital DNA Sequencing, and Supervised Learning demonstrate their potential value in ransomware detection. However, effective implementation requires further exploration and development (Figure 2).

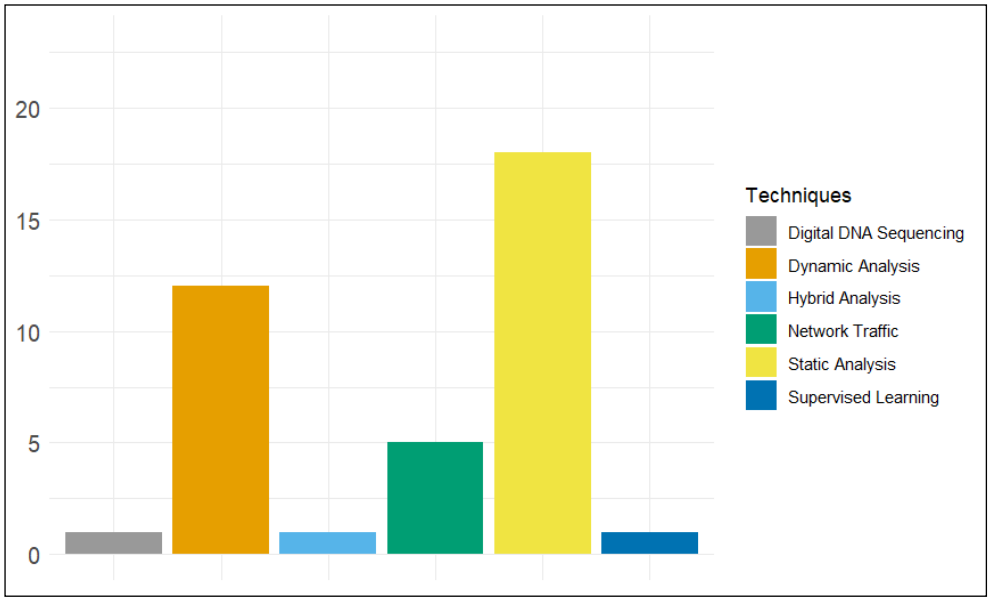


Figure 2: Most Notable Techniques in Ransomware Detection

The data in Table 2 indicates that the combination of the application of static, dynamic, hybrid, and network traffic analysis techniques favors ransomware detection. The high frequency with which these methods and techniques characterize ransomware detection in the literature determines that these techniques are widely accepted and effective. Numerous articles support extracting and selecting features from portable executable (PE) files. Its relevance in static analysis is notable since it achieves an accuracy of 99.98% using an unsupervised machine learning technique with Weight of Evidence (WoE) analysis (Shrimal et al., 2023). Similarly, analyzing ransomware behavior and extracting key features are crucial in dynamic analysis, with a True Positive Rate (TPR) of up to 99.4% (Gulmez et al., 2024). On the other hand, the study of network traffic and communication with servers achieved high accuracy percentages of 99.83% with Decision Tree and 99.61% with Random Forests algorithms (Almousa et al., 2021b). The information on these techniques and characteristics demonstrates their importance and effectiveness in identifying and mitigating ransomware cyber-attacks.

Table 2: Comparative Analysis of Features and Effective Attributes for Ransomware Detection

Techniques	**Features**	**Effective attributes and infected file characteristics**
Static Analysis	Binary classification (Schoenbachler et al., 2023)	Import/Export tables: unusual section names, High entropy sections
	PE Executable File Feature Extraction (Masum et al., 2022; Majd & Mazumdar, 2023; Moreira et al., 2023; Shrimal et al., 2023; Surendran et al., 2021; Usharani & Sandhya, 2020; Vehabovic et al., 2023)	PE headers, Section names, Entropy, API calls, Strings: Suspicious API calls, Anomalous byte patterns
	Bitcoin Address (Hassan et al., 2023)	Presence of Bitcoin addresses: Indicators of ransom demands
	Headers, Footers, File Extensions (Duignan et al., 2023)	Unusual headers/footers, Malicious file extensions
	Encrypted File Formats (Hsu et al., 2021)	Encrypted file patterns: Unrecognized encryption schemes

Dynamic Analysis	Ransomware Behavior (Gulmez et al., 2024; Hirano et al., 2022; Khan & Sharma, 2023; Kunku et al., 2023; Usha et al., 2021)	System calls, File operations, Registry changes: unusual file modifications, Registry key alterations
	Memory Access Patterns (Hirano et al., 2022)	Memory access patterns: Abnormal process behavior
	Resource Monitoring (Celdrán et al., 2023)	CPU and memory usage: High resource usage
Hybrid Analysis	System and Network Activities (Ahmed et al., 2022; Almousa et al., 2021a; Khurana, 2023)	Combined static and dynamic features: Indicators of malicious activity
	DLL, Function Call, Assembly (Poudyal & Dasgupta, 2021)	DLL interactions, Function calls: Unusual DLL loads, Suspicious function calls
Network Traffic Analysis	Traffic Analysis (Almousa et al., 2021b; Ghazi & Raghava, 2022; Srivastava et al., 2023; Teymourlouei & Harris, 2021; Zhuravchak & Dudykevych, 2023)	IP addresses, Domain names: Connections to malicious IPs/domains
		Packet size and frequency: unusual packet sizes, Anomalous protocol usage
	Packet Authentication (Khan & Sharma, 2023)	Server communication: Unexpected outbound traffic, Abnormal communication frequency

RQ 2: *What tools are used by ransomware to implement machine learning methods and techniques in detecting and mitigating?*

We identified various machine learning tools for ransomware detection and their characteristics, listing their article references in Table 3.

Table 3: Most Used Tools of Machine Learning Used in Detection Ransomware

Tools	Articles
Datasets	(Ahmed et al., 2022; Asaju et al., 2021; Hiran & Kobayashi, 2022; Hsu et al., 2021; Khan & Sharma, 2023; Khammas, 2020; Kunku et al., 2023; Mansor et al., 2020; Schoenbachler et al., 2023; Teymourlouei & Harris, 2021; Victoriano, 2019)
API Calls	(Almousa et al., 2021a; Gulmez et al., 2024; Hirano et al., 2022; Masum et al., 2022; Poudyal & Dasgupta, 2021; Rahman et al., 2024; Usha et al., 2021)
Executable Files	(Majd & Mazumdar, 2023; Moreira et al., 2023; Shrimal et al., 2023; Surendran et al., 2021; Usharani & Sandhya, 2020; Vehabovic et al., 2023)
Ransomware Samples	(Ahmed et al., 2022; Aljabri et al., 2024; Almousa et al., 2021a; Gulmez et al., 2024; Hassan et al., 2023; Hirano et al., 2022; Celdrán et al., 2023; Sharma et al., 2023)

The analysis of the percentages of tools used in ransomware detection, shown in Figure 3, reveals a dominance of existing data sets, representing almost 32.4% of the total. This prevalence underscores the need for quality data to train and evaluate ransomware detection algorithms quickly, safely, and effectively. In addition, ransomware samples with 26.5%, API Calls, and the analysis of executable files (Executable Files) also stand out as fundamental tools, occupying 20.6% and 17.6% of use, respectively. These results reflect a trend toward real-time monitoring of system behavior and deep analysis of suspicious files. Therefore, managing a multidisciplinary approach in the fight against ransomware that takes advantage of static and dynamic data is necessary.

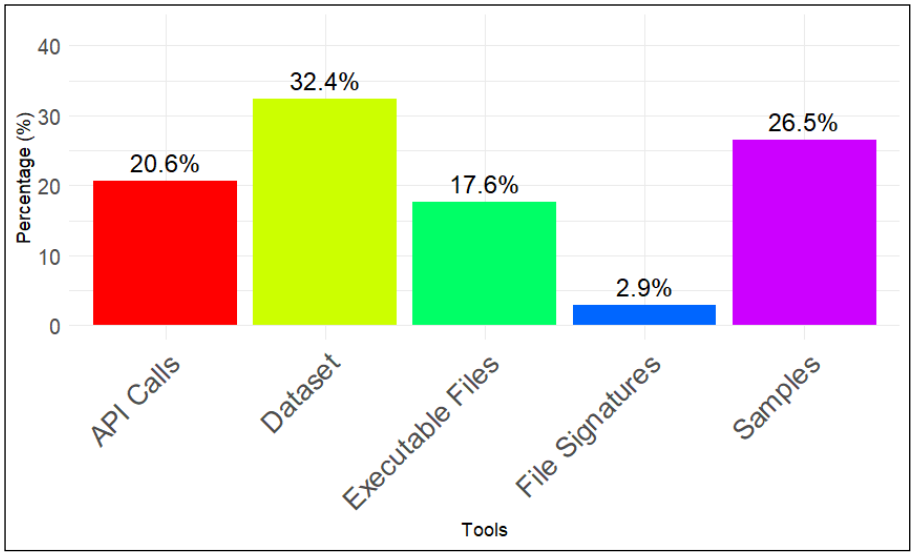


Figure 3: Most Notable Tools in Ransomware Detection

On the other hand, although less prevalent, Samples and File Signatures also play essential roles, representing 17.6% and 2.9% of usage, respectively. These findings underscore the diversity of approaches and tools in ransomware detection and the need for a comprehensive strategy that employs a wide range of resources to address this cyber threat effectively.

RQ 3: *Which machine learning algorithms have proven most effective in detecting and preventing ransomware?*

Several machine learning algorithms have proven to be highly effective in detecting ransomware. The most notable are Random Forests, Decision Tree, Support Vector Machines (SVM), Neural Networks, and Naïve Bayes (see Table 4 and Figure 4). Below is a brief explanation of these findings:

Table 4: Algorithm Effectiveness in Ransomware Detection

Article	Random Forest	Decision Tree	Support Vector Machine	Neural Networks	Naïve Bayes
Mansor et al., (2020)	99.32%				
Schoenbachler et al., (2023)	90.51%	88.32%			
Victoriano, (2019)	98.05%	98.05%			97.6%
Rahman et al., (2024)	99.7%	99.5%	78.7%		
Srivastava et al., (2023)		99.9%			
Masum et al., (2022)	99%	98%		97%	35%
Asaju et al., (2021)		97.60%			83.40%
Almousa et al., (2021b)	99.61%	99.83%			
Surendran et al., (2021)	99.42%	99.05%			69.43%
Poudyal & Dasgupta, (2021)	98.99%	99.54%		99.69%	
Usharani & Sandhya, (2020)		98.98%			98.44%
Khan & Sharma, (2023)					78.5%

As shown in Figure 4, the Random Forest algorithm is the most popular, used in 21.7% of cases. This preference may be due to its ability to handle large and complex data sets and its effectiveness in classification tasks. Support Vector Machine (SVM) and Decision Tree are prominent algorithms used in 12.5% of the studies. SVM is particularly effective in high-dimensional spaces. The "Others" category, which includes a variety of algorithms such as CNN, JRIP, LightGBM, Extra Trees, Gaussian

NB, and Linear Discriminant Analysis, among others, represents 13.3% of usage. Thus, we infer that although there is a core of preferred algorithms, researchers also explore various techniques to find optimal solutions. This diverse approach reflects the complexity of the ransomware detection problem and the need to adapt methods to different data types and scenarios.

In Addition, Assembly techniques such as XGBoost and AdaBoost have moderate usage, with 4.2% and 6.7%, respectively. These methods are valuable for improving prediction accuracy by combining multiple simpler models. Other classic classification algorithms, such as Gradient Boosting, KNN, Naïve Bayes, and Logistic Regression, are frequently used, each with a 5-6% share. Likewise, neural networks and Long-Short-Term Memory (LSTM) models have a lower presence, with 1.7% and 5%, respectively.

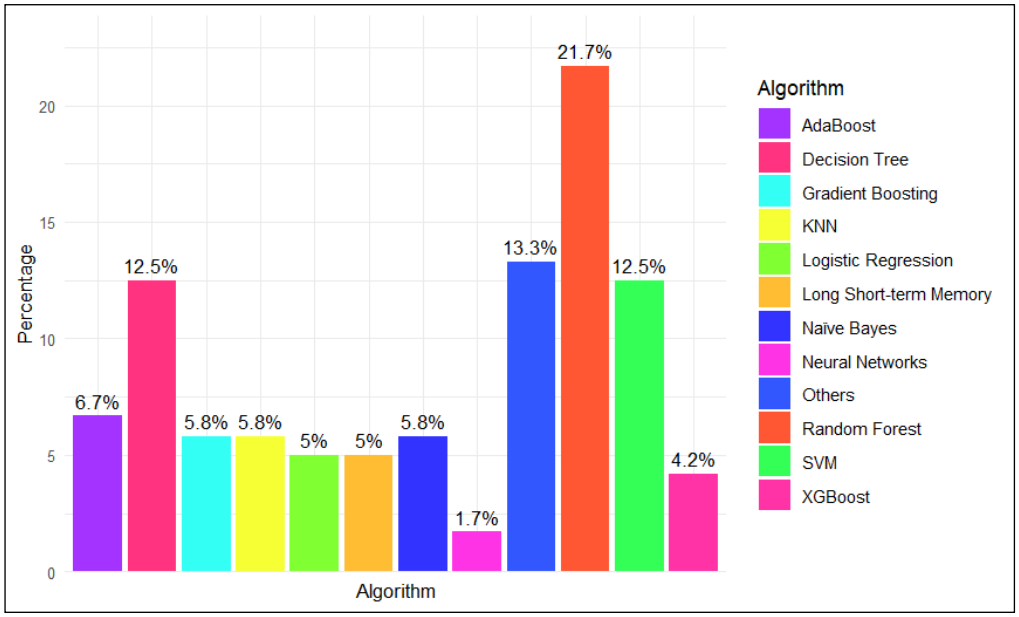


Figure 4: Identification of the Most used Machine Learning Algorithms in Ransomware Detection

In summary, Figure 4 reveals that Random Forest, Decision Tree, and Neural Networks are the most consistent and practical algorithms for ransomware detection, with Random Forest and Neural Networks achieving effectiveness rates exceeding 99% in several studies. Decision Tree also performs well, though with slightly more variability, ranging from 88.32% to 99.9%. Support Vector Machine (SVM) is effective, particularly with high effectiveness in some studies (e.g., 99.69%), but shows more significant variability, with a minimum of 78.7%. Naïve Bayes exhibits significant variability, with effectiveness ranging from 35% to 97.6%, making it less reliable than the other algorithms. Random Forests, Decision Trees, and Neural Networks are the most reliable options. At the same time, SVM remains a strong contender despite its variability, and Naïve Bayes may require careful adjustment for optimal performance.

The systematic review of existing articles highlights RF, DT, and NN as the most reliable algorithms for ransomware detection. Despite its variability, SVM remains a viable option, while NB and other traditional methods can be effective under specific circumstances. The diversity of techniques reflects ransomware detection research's dynamic and evolving nature, emphasizing the need for continued exploration of ML approaches tailored to ransomware's unique challenges.

RQ 4: *What are the main challenges, future research lines, and limitations of detecting using machine learning?*

To answer this question, we tried to classify the primary articles considering the country of origin of the study, which, knowing their technological development, would serve us for inferences. Figure 5 shows the country where researchers published their articles. The presence of countries such as the United States, India, and the United Kingdom among the main contributors to the research suggests greater awareness and concern about cybersecurity in these regions due to having more developed digital infrastructures and greater susceptibility to attacks. Also, international collaboration in this field is evident, indicating an exchange of knowledge and creating more effective solutions. Therefore, this highlights the need to address cybersecurity globally and the importance of working together to protect organizations and users against ransomware.

One of the main challenges in ransomware detection using machine learning is the ability of more advanced variants to evade such detection. Duignan et al., (2023) noted that it is essential to conduct broader research covering various ransomware strains and file types, especially those that do not alter their extensions. Moreover, Poudyal & Dasgupta, (2021) underline the importance of leveraging cloud computing with parallel processing capabilities and having labeled and representative data sets. They also insist on the need to balance accuracy and performance in real-time environments to optimize the effectiveness of machine learning.

Future research tendencies in ransomware detection and control through machine learning methods include developing models to analyze anomalous behavior and classify suspicious files. Likewise, creating predictive models that allow the anticipation of attacks, and the dynamic adaptation of security policies is envisioned (Beaman et al., 2021). In addition, future research focuses on the automation of incident responses and continuous adaptation to new ransomware variants (Razaulla et al., 2023).

Regarding certain limitations in the application of machine learning for ransomware detection, several authors summarize them in two key aspects. First, detection models depend on specific data sets that focus on ransomware and relatively small executable files, which can restrict the ability of these models to generalize their results to other malware variants (Khammas, 2020; Celdrán et al., 2023; Moreira et al., 2023). Second, both the computational processing requirements and the analysis duration are insufficient to detect ransomware in real-time effectively (Aljabri et al., 2024).

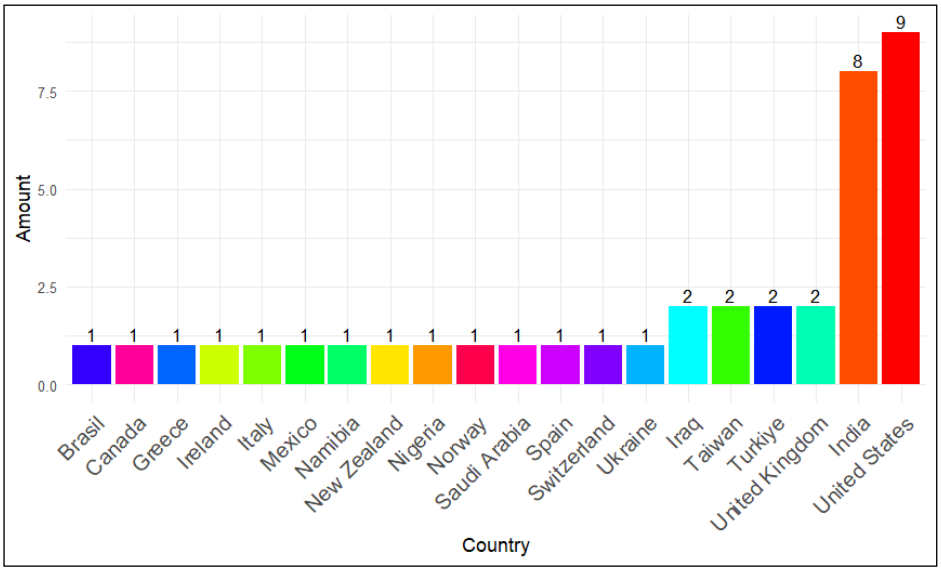


Figure 5: The number of Articles on Ransomware Detection using Machine Learning in our Study and Published in different Countries where India, the United States, and the United Kingdom Stand Out

4 Discussion

The study provides a detailed analysis of the literature related to ransomware detection using machine learning methods. We meticulously address each aspect, from the methodology used to the results obtained and the discussions that arise from them. Through a selective search process and an exhaustive review of the publications available in IEEE Xplore, ACM, and Science Direct, the study identified 617 articles, of which we selected 36 as relevant primary studies.

The articles' collection, choice, and analysis emphasize several essential aspects. Firstly, we observed that the Random Forest algorithm is the most widely used in ransomware detection, closely followed by the Decision Tree and Support Vector Machine (SVM) algorithms. This finding underlines the effectiveness of these tools in the field of cybersecurity, especially in identifying attacks such as ransomware.

Various methods and techniques illustrate the problem's complexity and the need for flexible solutions. Researchers are exploring a broad spectrum of approaches, ranging from dynamic and static analysis to network traffic analysis, to improve the accuracy of ransomware detection.

Moreover, international collaboration in this area is clearly palpable, with notable contributions from countries such as the United States, India, and the United Kingdom. This cooperation emphasizes the relevance of addressing cybersecurity worldwide and accentuates the need to exchange knowledge and resources to confront emergent cyber-attacks.

This study identified six key machine-learning methods for ransomware detection: Random Forest, Naïve Bayes, Decision Tree, Support Vector Machine, Ada Boost, and Gradian Boosting, the properties of infected files and attributes that would facilitate their identification. We considered four key factors: static analysis, dynamic analysis, hybrid analysis, and network traffic analysis. This conclusion is relevant, as algorithms could focus on these aspects to improve their accuracy.

Nonetheless, the research also reveals various challenges and restrictions in ransomware detection exploiting machine learning. The scarcity of representative datasets and the ability of advanced ransomware variants to evade detection are just some of the obstacles that researchers must face in this field; this highlights the need for further research and the development of innovative solutions to address these issues.

This study provides a comprehensive and up-to-date overview of ransomware detection through machine learning techniques. Recent advances and remaining challenges and areas requiring future research are highlighted. This analysis is essential to strengthen cybersecurity and safeguard organizations and users from the growing threats ransomware poses.

5 Conclusions

This study used the PRISMA methodological guide to systematically review the literature, highlighting the importance of machine learning in detecting ransomware. Among the 36 primary articles analyzed, machine learning techniques are of great help, as they allow identifying patterns to detect ransomware attacks; among them, we find static, dynamic, and hybrid analysis with the characteristics and attributes of the files most effective for detecting them. Also, we found that the most used algorithms for ransomware detection include the Random Forest algorithm. The results reveal the diversity of approaches and methodologies employed, emphasizing the analysis of system behavior, API calls, and file analysis using ransomware datasets and samples as critical research areas. Finally, the variety of

tools and techniques employed highlights the complexity of this challenge. It underlines the importance of adopting comprehensive approaches to detect and prevent this type of malware.

As future work, we plan to combine Principal Component Analysis (PCA) for dimensionality reduction of data sets with the development of a robust hybrid model combining supervised ML methods and the results of this research.

References

[1] Ahmed, U., Lin, J. C. W., & Srivastava, G. (2022). Mitigating adversarial evasion attacks of ransomware using ensemble learning. *Computers and Electrical Engineering*, *100*, 107903. https://doi.org/10.1016/j.compeleceng.2022.107903

[2] Akash, Kaviya, Nithish, Sethupathi, & Balamurugan. (2022). Traffic Flow Prediction Using RF Algorithm in Machine Learning. *International Academic Journal of Innovative Research*, *9*(1), 37–41. https://doi.org/10.9756/IAJIR/V9I1/IAJIR0906

[3] Aljabri, M., Alhaidari, F., Albuainain, A., Alrashidi, S., Alansari, J., Alqahtani, W., & Alshaya, J. (2024). Ransomware detection based on machine learning using memory features. *Egyptian Informatics Journal*, *25*, 100445. https://doi.org/10.1016/j.eij.2024.100445

[4] Almousa, M., Basavaraju, S., & Anwar, M. (2021, December). Api-based ransomware detection using machine learning-based threat detection models. In *2021 18th International Conference on Privacy, Security and Trust (PST)* (pp. 1-7). IEEE. https://doi.org/10.1109/PST52912.2021.9647816

[5] Almousa, M., Osawere, J., & Anwar, M. (2021, September). Identification of ransomware families by analyzing network traffic using machine learning techniques. In *2021 Third international conference on transdisciplinary AI (TransAI)* (pp. 19-24). IEEE. https://doi.org/10.1109/TransAI51903.2021.00012

[6] Alraizza, A., & Algarni, A. (2023). Ransomware detection using machine learning: A survey. *Big Data and Cognitive Computing*, *7*(3), 143. https://doi.org/10.3390/bdcc7030143

[7] Anny Leema, A., Balakrishnan, P., & Jothiaruna, N. (2024). Harnessing the Power of Web Scraping and Machine Learning to Uncover Customer Empathy from Online Reviews. *Indian Journal of Information Sources and Services*, *14*(3), 52–63. https://doi.org/10.51983/ijiss-2024.14.3.08

[8] Asaju, C. B., Otoo-Arthur, D., Orah, R. O., & Sekyi-Dadson, F. (2021, July). Development of a machine learning model for detecting and classifying ransomware. In *2021 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICMEAS52683.2021.9692402

[9] Bae, S. I., Lee, G. B., & Im, E. G. (2020). Ransomware detection using machine learning algorithms. *Concurrency and Computation: Practice and Experience*, *32*(18), e5422. https://doi.org/10.1002/cpe.5422

[10] Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security*, *111*, 102490. https://doi.org/10.1016/j.cose.2021.102490

[11] Biswas, A. (2024). Modelling an Innovative Machine Learning Model for Student Stress Forecasting. *Global Perspectives in Management*, *2*(2), 22-30

[12] Cao, Y., & Jiang, L. (2024). Machine Learning based Suggestion Method for Land Suitability Assessment and Production Sustainability. *Natural and Engineering Sciences*, *9*(2), 55-72. https://doi.org/10.28978/nesciences.1569166

[13] Celdrán, A. H., Sánchez, P. M. S., Von der Assen, J., Shushack, D., Gómez, A. L. P., Bovet, G., ... & Stiller, B. (2023). Behavioral fingerprinting to detect ransomware in resource-constrained devices. *Computers & Security*, *135*, 103510. https://doi.org/10.1016/j.cose.2023.103510

[14] Cheng, H., Zhang, M., & Zhang, Y. (2021). A systematic review of ransomware detection techniques. *Journal of Computer Science and Technology, 36*(4), 659-674. https://doi.org/10.1007/s11390-021-1460.

[15] Duignan, M., Schukat, M., & Barrett, E. (2023, June). Detecting Ransomware Encryption with File Signatures and Machine Learning Models. In *2023 34th Irish Signals and Systems Conference (ISSC)* (pp. 1-5). IEEE. https://doi.org/10.1109/ISSC59246.2023.10162047

[16] Ghazi, M. R., & Raghava, N. S. (2022, December). Detecting ransomware attacks in cloud environment using machine learning-based intelligence system in COVID-19 chaos. In *2022 IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)* (pp. 1-6). IEEE. https://doi.org/10.1109/IATMSI56455.2022.10119441

[17] Gulmez, S., Kakisim, A. G., & Sogukpinar, I. (2024). XRan: Explainable deep learning-based ransomware detection using dynamic analysis. *Computers & Security, 139*, 103703. https://doi.org/10.1016/j.cose.2024.103703

[18] Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis. *Campbell systematic reviews*, *18*(2), e1230. https://doi.org/10.1002/cl2.1230

[19] Hassan, N., Sood, K., & Suzuki, G. (2023, July). Machine Learning with Bitcoin Heist Ransomware. In *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)* (pp. 1-6). IEEE. https://doi.org/10.1109/SmartNets58706.2023.10215732

[20] Hirano, M., & Kobayashi, R. (2022, July). Machine learning-based ransomware detection using low-level memory access patterns obtained from live-forensic hypervisor. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 323-330). IEEE. https://doi.org/10.1109/CSR54599.2022.9850340

[21] Hirano, M., Hodota, R., & Kobayashi, R. (2022). RanSAP: An open dataset of ransomware storage access patterns for training machine learning models. *Forensic Science International: Digital Investigation*, *40*, 301314. https://doi.org/10.1016/j.fsidi.2021.301314

[22] Hsu, C. M., Yang, C. C., Cheng, H. H., Setiasabda, P. E., & Leu, J. S. (2021). Enhancing file entropy analysis to improve machine learning detection rate of ransomware. *IEEE Access*, *9*, 138345-138351. https://doi.org/10.1109/ACCESS.2021.3114148

[23] Kavibharathi, S., Lakshmi Priyankaa, S., Kaviya, M. S., & Vasanthi, S. (2021). Live Chat Analysis Using Machine Learning. *International Academic Journal of Science and Engineering*, *8*(1), 39–44. https://doi.org/10.9756/IAJSE/V8I1/IAJSE0805

[24] Khammas, B. M. (2020). Ransomware detection using random forest technique. *ICT Express*, *6*(4), 325-331. https://doi.org/10.1016/j.icte.2020.11.001

[25] Khan, A., & Sharma, I. (2023, November). Machine learning-based methodology for preventing ransomware attacks on healthcare sector. In *2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)* (pp. 1-5). IEEE. https://doi.org/10.1109/RMKMATE59243.2023.10368971

[26] Khurana, S. (2023, December). Ransomware Threat Detection and Mitigation using Machine Learning Models. In *2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICTBIG59752.2023.10456343

[27] Kunku, K., Zaman, A. N. K., & Roy, K. (2023, December). Ransomware detection and classification using machine learning. In *2023 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 862-866). IEEE. https://doi.org/10.1109/SSCI52147.2023.10371924

[28] Majd, N. E., & Mazumdar, T. (2023, July). Ransomware classification using machine learning. In *2023 32nd International Conference on Computer Communications and Networks (ICCCN)* (pp. 1-7). IEEE. https://doi.org/10.1109/ICCCN58024.2023.10230176

[29] Mansor, W. N. A. B. W., Ahmad, A., Zainudin, W. S., Saudi, M. M., & Kama, M. N. (2020, April). Crytojacking Classification based on Machine Learning Algorithm. In *Proceedings of the 2020 8th International Conference on Communications and Broadband Networking* (pp. 73-76). https://doi.org/10.1145/3390525.3390537

[30] Masum, M., Faruk, M. J. H., Shahriar, H., Qian, K., Lo, D., & Adnan, M. I. (2022, January). Ransomware classification and detection with machine learning algorithms. In *2022 IEEE 12th annual computing and communication workshop and conference (CCWC)* (pp. 0316-0322). IEEE. https://doi.org/10.1109/CCWC54503.2022.9720869

[31] Methley, A. M., Campbell, S., Chew-Graham, C., McNally, R., & Cheraghi-Sohi, S. (2014). PICO, PICOS and SPIDER: a comparison study of specificity and sensitivity in three search tools for qualitative systematic reviews. *BMC health services research*, *14*(1), 1-10. https://doi.org/10.1186/s12913-014-0579-0

[32] Moreira, C. C., Moreira, D. C., & de Sales Jr, C. D. S. (2023). Improving ransomware detection based on portable executable header using xception convolutional neural network. *Computers & Security*, *130*, 103265. https://doi.org/10.1016/j.cose.2023.103265

[33] Park, M., You, G., Cho, S.J., Park, M., & Han, S. (2019). A Framework for Identifying Obfuscation Techniques applied to Android Apps using Machine Learning. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *10*(4), 22-30. https://doi.org/10.22667/JOWUA.2019.12.31.022

[34] Poudyal, S., & Dasgupta, D. (2021). Analysis of crypto-ransomware using ML-based multi-level profiling. *Ieee Access*, *9*, 122532-122547. https://doi.org/10.1109/ACCESS.2021.3109260

[35] Rahman, M. S., Sabbir, M. S. A., & Ghosh, S. (2024, March). Ransomware Attack Detection using Machine Learning Approaches. In *2024 3rd International Conference for Innovation in Technology (INOCON)* (pp. 1-7). IEEE. https://doi.org/10.1109/INOCON60754.2024.10512276

[36] Rakesh, N., Mohan, B. A., Kumaran, U., Prakash, G. L., Arul, R., & Thirugnanasambandam, K. (2024). Machine learning-driven strategies for customer retention and financial improvement. *Archives for Technical Sciences*, 2(31), 269–283. https://doi.org/10.70102/afts.2024.1631.269

[37] Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B. C., & Assi, C. (2023). The age of ransomware: A survey on the evolution, taxonomy, and research directions. *IEEE Access*, *11*, 40698-40723. https://doi.org/10.1109/ACCESS.2023.3268535

[38] Schoenbachler, J., Krishnan, V., Agarwal, G., & Li, F. (2023, October). Sorting ransomware from malware utilizing machine learning methods with dynamic analysis. In *Proceedings of the Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing* (pp. 516-521). https://doi.org/10.1145/3565287.3617632

[39] Seyedan, A., Soroushpour, S., & Gholamrezazadeh, S. (2023). Family and its changes in Cyberspace and the explanation of its future perspectives in the communication era. *International Academic Journal of Organizational Behavior and Human Resource Management*, *2*(2), 01–06.

[40] Sharma, A., Babbar, H., & Vats, A. K. (2023, May). Ransomware attack detection in the internet of things using machine learning approaches. In *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)* (pp. 553-559). IEEE. https://doi.org/10.1109/ICAAIC56838.2023.10141036

[41] Shrimal, R. S., Gajrani, J., Jain, V. K., Tripathi, M., & Jat, D. S. (2023, August). Detection of Ransomware Attacks Using Weight of Evidence Technique. In *2023 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)* (pp. 76-81). IEEE. https://doi.org/10.1109/ETNCC59188.2023.10284928

[42] Srivastava, A., Kumar, N., Handa, A., & Shukla, S. K. (2023, July). Ransomware detection based on network behavior using machine learning and hidden markov model with gaussian emission. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 227-233). IEEE. https://doi.org/10.1109/CSR57506.2023.10225001

[43] Surendran, R., Karthika, R., & Jayalakshmi, B. (2021, August). Implementation of dynamic scanner to protect the documents from ransomware using machine learning algorithms. In *2021 International Conference on Computing, Electronics & Communications Engineering (iCCECE)* (pp. 65-70). IEEE. https://doi.org/10.1109/iCCECE52344.2021.9534855

[44] Teymourlouei, H., & Harris, V. E. (2021, December). Detecting ransomware automated based on network behavior by using machine learning. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 728-734). IEEE. https://doi.org/10.1109/CSCI54926.2021.00186

[45] Usha, G., Madhavan, P., Cruz, M. V., Vinoth, N. A. S., & Nancy, M. (2021, December). Enhanced ransomware detection techniques using machine learning algorithms. In *2021 4th International Conference on Computing and Communications Technologies (ICCCT)* (pp. 52-58). IEEE. https://doi.org/10.1109/ICCCT53315.2021.9711906

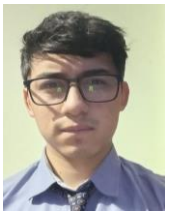
[46] Usharani, S., & Sandhya, S. G. (2020, July). Detection of ransomware in static analysis by using Gradient Tree Boosting Algorithm. In *2020 International Conference on System, Computation, Automation and Networking (ICSCAN)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICSCAN49426.2020.9262315

[47] Vehabovic, A., Zanddizari, H., Ghani, N., Shaikh, F., Bou-Harb, E., Pour, M. S., & Crichigno, J. (2023, May). Data-centric machine learning approach for early ransomware detection and attribution. In *NOMS 2023-2023 IEEE/iFIP network operations and management symposium* (pp. 1-6). IEEE. https://doi.org/10.1109/NOMS56928.2023.10154378

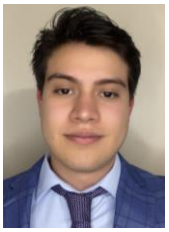
[48] Victoriano, O. B. (2019, October). Exposing android ransomware using machine learning. In *Proceedings of the 2019 International Conference on Information System and System Management* (pp. 32-37). https://doi.org/10.1145/3394788.3394923

[49] Zhuravchak, D., & Dudykevych, V. (2023, November). Real-time ransomware detection by using eBPF and natural language processing and machine learning. In *2023 IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT)* (pp. 1-4). IEEE. https://doi.org/10.1109/AICT61584.2023.10452697

Authors Biography



Jonathan Ismael Zapata Sandoval is a software engineer graduating from Universidad de las Fuerzas Armadas (ESPE). His areas of interest include cybersecurity, web development, and machine learning research. He has worked on projects combining these disciplines throughout his academic background, focusing on threat detection and computer security improvement. Jonathan is committed to applying innovative technologies to solve complex problems in computer science.



Elian Israel Garcés Aguila is a software engineer who graduated from the University of the Armed Forces (ESPE). His passion is cybersecurity, web development, and artificial intelligence research. During his academic career, he has participated in various projects combining these areas, specially creating innovative solutions and optimizing computer systems. Elian is committed to using advanced technologies to face the complex challenges software engineering presents.

Walter Fuertes is a senior research professor at the Department of Computer Science at the Universidad de las Fuerzas Armadas ESPE in Sangolquí-Ecuador. He currently serves as Coordinator of the Research Group on Distributed Systems, Cybersecurity and Content (RACKLY) at the same University. He graduated as a Systems and Computer Engineer from the Escuela Politécnica del Ejército ESPE. He then obtained his master's degree in computer science with a mention in Networks Computers from the Escuela Politécnica Nacional of Quito-Ecuador (EPN), his master's degree in University Teaching from ESPE, and his Doctorate (PhD) degree with honors in Computer and Telecommunications Engineering from the Polytechnic School of Computer Science of the Autonomous University of Madrid, Spain. Since 2006, he has actively participated in around 15 research projects focused on applying Virtualization technologies, Distributed Systems, Performance Evaluation, Security in Computer Systems, Cybersecurity, Data Analytics, Artificial Intelligence, Cognitive Security, Internet of Things, and Business Intelligence. He has spoken at several national and international conferences and written for national and international journals. He has published around 120 scientific and technical articles in different countries.