Pre-Encryption Ransomware Detection (PERD) Taxonomy, and Research Directions: Systematic Literature Review

Mujeeb ur Rehman Shaikh[1]*, Mohd Fadzil Hassan[2], Rehan Akbar[3],
Rafi Ullah[4], K.S. Savita[5], Ubaid Rehman[6], Jameel Shehu Yalli[7]
Computer and Information Sciences Department, Universiti Teknologi PETRONAS, Seri Iskandar, 32610, Perak, Malaysia[1, 7]
Centre for Research in Data Science (CeRDaS), Universiti Teknologi PETRONAS,
32610 Seri Iskandar, Perak Darul Ridzuan, Malaysia[2]
School of Computing and Information Sciences, Florida International University, Miami, United States of America[3]
Positive Computing Research Centre, Universiti Teknologi PETRONAS, Seri Iskandar, 32610, Perak, Malaysia[4, 5]
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), Karachi, Pakistan[6]

***Abstract*—Today's era is witnessing an alarming surge in ransomware attacks, propelled by the increasingly sophisticated obfuscation tools deployed by cybercriminals to evade conventional antivirus defenses. Therefore, there is a need to better detect and obfuscate viruses. This analysis embarks on a comprehensive exploration of the intricate landscape of ransomware threats, which will become even more problematic in the upcoming era. Attackers may practice new encryption approaches or obfuscation methods to create ransomware that is more difficult to detect and analyze. The damage caused by ransomware ranges from financial losses, at best paid for ransom, to the loss of human life. We presented a Systematic Literature Review and quality analysis of published research papers on the topic. We investigated 30 articles published between the year 2018 to the year 2023(H1). The outline of what has been published thus far is reflected in the 30 papers that were chosen and explained in this article. One of our main conclusions was that machine learning ML-based detection models performed better than others. Additionally, we discovered that only a small number of papers were able to receive excellent ratings based on the standards for quality assessment. To identify past research practices and provide insight into potential future guidelines in the pre-encryption ransomware detection (PERD) space, we summarized and synthesized the existing machine learning studies for this SLR. Future researchers will use this study as a roadmap and assistance to investigate the preexisting literature efficiently and effectively.**

***Keywords*—Cybersecurity; ransomware detection; static and dynamic analysis; machine learning; cyber-attacks; security**

I. Introduction

One of the most prominent cyberattacks that has impacted businesses worldwide in the past five years is ransomware. According to the Verizon Data Breach Investigation Report (DBIR) 2021, ransomware has damaged 37% of organizations globally, including those in the healthcare sector [1]. By mid-2023, ransomware attacks had multiplied significantly globally in comparison to the previous year [2]. Ransomware gained traction again in 2017 with the WannaCry incident [3]. The incident not only emphasized the risks associated with ransomware but also its efficiency in terms of cost. The primary goals of the WannaCry to implement additional measures to prevent and minimize further harm and data loss within systems in cases where warning mechanisms fail during the initial detection phase. As businesses transition to remote work models, employees are increasingly susceptible to phishing emails, thereby creating security vulnerabilities that counteract the organization's defense against cyberattacks. Attacks were to sow chaos and instill fear rather than solely seeking financial profit. Despite requesting a ransom of only $300, the potential financial damages were far greater. The increase in ransomware attacks, along with their various forms, has been significant. This surge in recent cyberattacks is attributed to the impact of the COVID-19 pandemic [4], [5]. One of the reasons it has become increasingly difficult to identify cybercriminals is the use of virtual currencies, such as Bitcoin, in transactions, which are impossible to trace. This method continues because victims often succumb to pressure and are willing to pay any amount to recover their data. Additionally, evasion technologies are advancing rapidly, making it challenging for antivirus software to keep up with the evolution of ransomware.

The global economy benefits cybercriminals due to the lack of sufficient intelligence on spam messages and other methods used to spread highly potent ransomware. In the fight against ransomware, a key objective is to minimize file losses when early detection fails. Current detection techniques focus on limiting the number of encrypted files by blocking processes that exhibit ransomware-like behavior, such as API calls, registry key modifications, or embedded binary strings. However, it is crucial to provide a comprehensive assessment of ransomware trends from 1989 to 2023, as illustrated in Fig. 1.

Given the increasing sophistication and frequency of ransomware attacks, there is an urgent imperative to develop robust pre-encryption detection methods to thwart these threats before they unleash irreparable damage. This research article seeks to offer a comprehensive insight into pre-encryption detection methodologies tailored for ransomware, emphasizing their pivotal role in early threat identification and mitigation. Such strategies are indispensable for curtailing both the

*Corresponding Author.

financial losses and operational disruptions caused by ransomware incidents, enabling proactive incident responses and fortifying defenses against encryption and potential breaches of sensitive data. By fortifying cybersecurity measures and remaining vigilant against evolving ransomware tactics, organizations can safeguard the integrity of their systems and data, ensuring seamless business continuity. The study will initiate by categorizing pre-encryption detection methods based on the approaches employed for early ransomware detection, subsequently analyzing existing literature to pinpoint gaps, evaluate the current knowledge landscape, and delineate future research directions.

As technology continues to advance, ransomware evolves into more focused and precise attacks on networks, employing sophisticated techniques despite changes in technology and defensive tactics. Unlike other types of malicious software, cryptographic ransomware stands out due to its unique ability to encrypt victims' data, making decryption possible only by the malicious actors upon payment of ransom [6]. The results outlined in this research article stem from a thorough examination of existing literature, encompassing scholarly articles, conference papers, and industry reports up to our knowledge cutoff in May 2023, representing the most recent developments in the field. Through a comprehensive analysis of pre-encryption detection methods, their classification, and future research trajectories, this study aims to contribute to the advancement of more robust strategies in combating ransomware. The insights and findings presented herein offer a valuable resource for researchers, practitioners, and policymakers seeking to devise and deploy enhanced defense mechanisms against ransomware attacks. Table I shows Comparison of Legacy Ransomware vs. Advanced Ransomware.

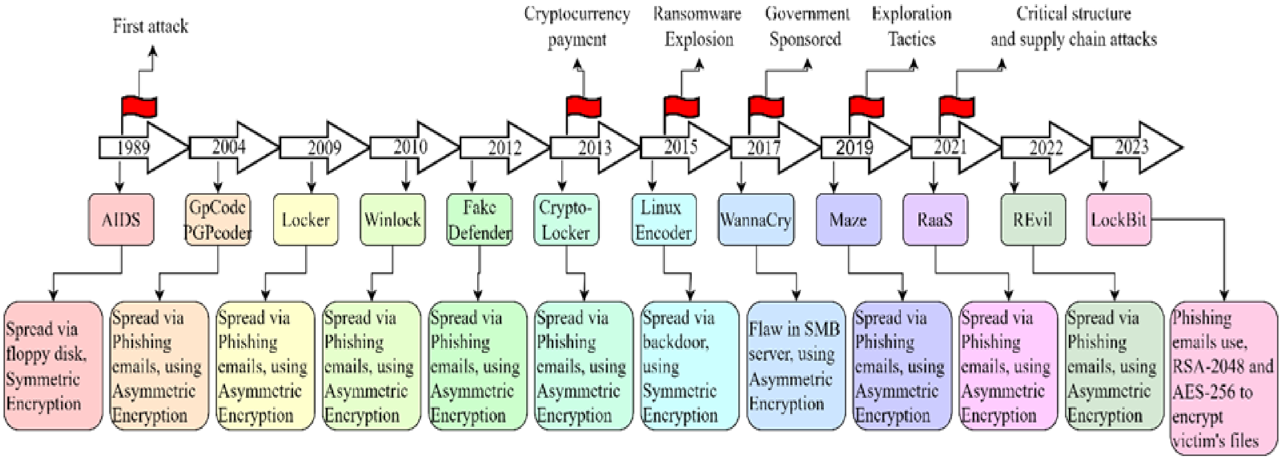
First attack
Cryptocurrency payment
Ransomware Explosion
Government Sponsored
Exploration Tactics
Critical structure and supply chain attacks
1989
2004
2009
2010
2012
2013
2015
2017
2019
2021
2022
2023
AIDS
GpCode PGPcoder
Locker
Winlock
Fake Defender
Crypto-Locker
Linux Encoder
WannaCry
Maze
RaaS
REvil
LockBit
Spread via floppy disk, Symmetric Encryption
Spread via Phishing emails, using Asymmetric Encryption
Spread via Phishing emails, using Asymmetric Encryption
Spread via Phishing emails, using Asymmetric Encryption
Spread via Phishing emails, using Asymmetric Encryption
Spread via Phishing emails, using Asymmetric Encryption
Spread via backdoor, using Symmetric Encryption
Flaw in SMB server, using Asymmetric Encryption
Spread via Phishing emails, using Asymmetric Encryption
Spread via Phishing emails, using Asymmetric Encryption
Spread via Phishing emails, using Asymmetric Encryption
Phishing emails use, RSA-2048 and AES-256 to encrypt victim's files

Fig. 1. Timeline for ransomware from 1989 to 2023.

TABLE I. LEGACY RANSOMWARE VS ADVANCE RANSOMWARE [13]

Aspect	Attack Method	Encryption	Targets	Ransom Payment	Data Exfiltration	Detection Evasion
Legacy Ransomware	Phishing, malicious attachments	Single-layer (AES)	Individuals, small businesses	Bitcoin, common cryptocurrencies	Rare, focus on encryption	Simple obfuscation
Advanced Ransomware	Vulnerability exploitation, RaaS	Multi-layer, often asymmetric	Large organizations, critical	Privacy-focused (Monero), extortion	Common, double/triple extortion	Fileless attacks, AI-based evasion

Cybercrime affects not only large corporations but also small and medium-sized enterprises, often leading to severe financial losses. These criminal activities have wide-ranging negative consequences, including data destruction, financial theft, reduced productivity, intellectual property violations, and other indirect costs. The growing incidence of cybercrime presents a major risk to the global economy, highlighting the urgent need for strong preventive measures [7]. Despite numerous reports and instances of ransomware attacks, organizations continue to adapt, strengthening their resilience and response to such threats. According to a study conducted in 2021 study revealed that 96% of businesses previously targeted by ransomware successfully survived and made improvements following the attacks.

According to Fig. 2, ransomware attacks constitute 35%, 33%, and 28% of all cyberattacks targeting industries such as professional services, government, and healthcare, respectively, indicating their prevalence as the most generic form of attack However, there is a notable shift in ransomware trends as observed in Sophos' research. Malicious actors behind ransomware attacks have transitioned from large-scale, indiscriminate attacks to more targeted and persistent approaches [8]. Researchers have recently observed striking parallels between the methods used by ransomware groups and those employed by highly sophisticated hackers known as Advanced Persistent Threats (APTs). This realization has ignited a wave of research, driving a comprehensive review of pre-encryption ransomware. Through this review, the aim is to gain a clear understanding of how both static and dynamic analysis techniques have been utilized over the past few years to detect ransomware before it encrypts data. This exploration of existing research will provide valuable insights into how to effectively identify and prevent these ever-evolving cyber threats. As Table II indicates, importance of the current and comparison with traditional methods.

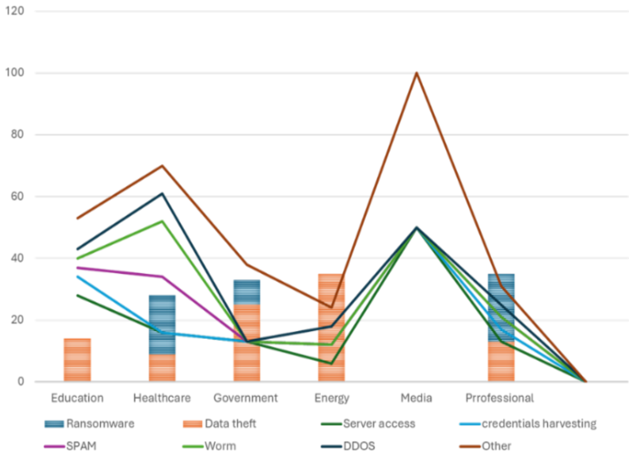

Fig. 2. Types of attacks per industry.

TABLE II. Comparison with Traditional Methods

Importance of the Current Method	Comparison with Traditional Methods
Potential to enhance ransomware detection accuracy.	Detection capabilities (e.g., pre-encryption vs. post-encryption)
Ability to detect novel or evolving ransomware strains.	Accuracy and false positive rates
Potential for early prevention of attacks	Computational overhead and resource requirements
Reduced impact on system performance or user experience	Resilience to evasion techniques Adaptability to detect new ransomware variants

A. Motivation of the Research

The harmful behavior of crypto-ransomware attacks makes it challenging to manage when developing a model for detecting such attacks [6]. If the model does not effectively differentiate between benign programs and crypto-ransomware attacks, there is a high likelihood of false alarms [8] [9]. The behavior of malicious software, coupled with the irreversible nature of ransomware attacks, makes detection even more difficult. Due to the ongoing development of ransomware variants, there is a lack of detection solutions capable of distinguishing between legitimate processes and malicious code [10]. Existing studies have used a fixed threshold to extract data from crypto-ransomware attacks. However, the use of cryptographic APIs presents challenges since these APIs are also employed by legitimate programs, leading to an increased rate of false alarms. This reliance on cryptographic APIs complicates the detection process. When a system struggles to classify processes as legitimate, harmless, or malicious, the accuracy of the detection is compromised. Models tend to be less accurate when they fail to identify zero-day attacks or adapt to the evolving behavior of crypto-ransomware attacks [11]. Crypto-ransomware attacks are particularly destructive and pose a significant threat to cybersecurity. Without a decryption key, recovering user files attacked by crypto-ransomware is impossible. Previous research has focused on detecting ransomware attacks at an early stage, prior to encryption. However, these solutions have not adequately addressed the dynamic nature of ransomware behavior [12]. The effectiveness of early detection in zero-day attacks has been improved through the development of Adaptive Crypto-Ransomware detection techniques, utilizing adaptive online classifiers to enhance the accuracy and responsiveness of ransomware detection. Currently, existing solutions do not deal with adaptation with pre-encryption detection. The main difference between the proposed model and the available solution is the adaptive detection of early zero-day encryption. The ability to efficiently detect new zero-day and new variants of crypto-ransomware while maintaining adaptability with limited amounts of data is crucial[13]. These attacks are difficult to detect due to limited data, redundant and variable properties, early detection, and adaptation [14], [15]. The existing solutions do not deal with the limited number of pre-encryption data and do not provide adaptation to the evolution of crypto-ransomware variants and do not provide adaptation to the evolution of crypto-ransomware variants [16].

B. Ransomware Pre-Encryption Detection

Some researchers are currently researching some methods of pre-encryption detection. Windows Defender and other virus protection also take steps to prevent attacks before work begins. However, attackers can circumvent these security firewalls [17]. For this reason, WannaCry ransomware attacked more than 200,000 PCs [18]. One of their contributions is based on the Windows Application Programming Interface (API) of an unreliable program and is recorded and examined by the learning algorithm [19]. Additionally, this phase includes a real-time detection system for Windows-based computers and makes use of API pattern recognition to determine whether the learning algorithm is a suspect program. To identify zero-day ransomware variations, their approach employs a hybrid method that incorporates the naïve Bayes and decision tree machine learning techniques. To identify malware that uses encryption methods to block files known as crypto-ransomware, the so-called pre-encryption detection algorithm (PEDA) has been suggested.

II. Research Contribution

This systematic literature review (SLR) aims to make significant contributions to the field of ransomware detection by providing a comprehensive analysis of existing methodologies, taxonomy, and future research directions for pre-encryption detection. Our study synthesizes current knowledge and identifies gaps in understanding, thereby offering valuable insights to researchers, practitioners, and policymakers. By categorizing and evaluating pre-encryption detection techniques and their effectiveness, this review serves as a foundation for developing more robust strategies to combat ransomware threats. Additionally, our identification of research directions paves the way for future investigations aimed at enhancing detection capabilities and mitigating the impact of new ransomware attacks on individuals, organizations, and society. A review may provide significant and helpful contributions to the realm of cybersecurity and ransomware detection. The most recent research on machine-learning techniques for ransomware detection is from 2018 to 2023. It is distinguished from prior work by extensively examining machine learning methods for spotting ransomware using an SLR technique. Additionally, the study explores current constraints and potential future directions in machine learning for pre-encryption ransomware detection at an early stage and includes innovative machine-learning algorithms. Overall, this

SLR contributes to advancing knowledge in the field of cybersecurity and provides actionable recommendations for improving new ransomware detection and prevention measures. Table III Shows List of all abbreviations used in this study.

1) A complete review of pre-encryption ransomware creation and novel approaches to detect ransomware was provided.

2) Ransomware attack techniques and taxonomy will be created.

3) Need to develop heuristic-based detection model so, that new ransomware can be detected.

4) Parameters used for the evaluation of ransomware attack, defense, and detection mechanisms.

5) Summary of the existing studies on pre-encryption ransomware detection

6) Explain ML and non-ML-based detection techniques.

7) Presenting a summary of the results and giving the researcher recommendations for future work to solve the issues.

TABLE III. LIST OF ABBREVIATIONS FOR THE ML ALGORITHMS

Abbreviation	Explanation
ML	Machine Learning
PERD	Pre-Encryption Ransomware Detection
SVM	Support Vector Machine
DT	Decision Tree
GB	Gradient Boosting
XGB	Xtreme Gradient Boosting
RF	Random Forest
LR	Logistic Regression
TPR	True Positive Rate
FNR	False Negative Rate
FPR	False Positive Rate
IOC	Indications of Compromise
DNS-Based	Domain Name System
API	Application program Interface
IRP	Incident Response Platform
C&C	Command and Control
ROC	Receiver Characteristic Operator

The remaining parts of the article are structured as follows: Section II presents a detailed analysis of previous related surveys. Section III details the research methodology, whereas Section IV presents the taxonomy of ransomware attacks. In Section V, Results, and future directions. Conclusion of the paper in Section VI.

A. Prior Research

Ransomware must be identified to keep genuine users and businesses safe from it. Finding out whether a given program has malicious intent is the process of ransomware detection. Before this, it was frequent practice to identify ransomware using signature-based detection techniques. However, this approach has certain drawbacks, such as the inability to identify fresh ransomware and undetected malware. Anomaly-based detection, heuristic-based detection, behavioral-based detection, and model-based detection are some of the novel techniques the researchers suggested at the same time. Algorithms for machine learning and data extraction are also frequently utilized for ransomware detection with these techniques. New strategies, such as deep learning, file tracking, cloud, mobile, and IoT-based detection, have recently been presented [20]. For unknown and innovative ransomware, on the other hand, behavior, model verification, and cloud-based methods are preferable. To better identify certain known and undiscovered ransomware and its families, deep learning, mobile devices, and IoT-based techniques have also been developed [21], [22]. This is because each approach has pros and cons of its own and under some circumstances, one method can be more effectively recognized than the other.

With an emphasis on tracking file systems and kernel activity, the majority of pre-encryption and encryption detection systems operate in host-based contexts. However, certain discovery methods prioritize communication with the command-and-control server and the target local network. The latter approach employs deep packet inspection to identify the delivery and exfiltration of encryption keys as well as network metadata to identify DNS-based indications of compromise (IOC) [23]. A wide range of algorithms and methods for pre-encryption and encryption detection range from simple spoofing and file integrity monitoring to sophisticated machine learning (ML) models trained to monitor system behavior during encryption-related operations such as encryption and key generation. This study also focuses on the detection of encryption-related crypto-ransomware, and additional references to ransomware refer to attackers encrypting victims' data for extortion purposes.

B. Ransomware Kill Chain Steps

The life cycle of ransomware begins with the spread of the malicious code and continues until the victim is presented with a demand for payment. Several procedures are followed throughout this lifecycle to successfully seize the files and resources of the user. According to Fig. 3, the summary below, there are many critical stages that ransomware assaults are supposed to go through [24], [25], [26], [27].

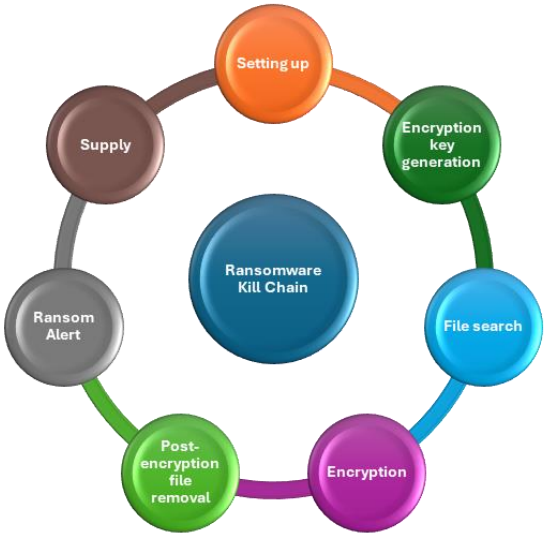

Fig. 3. Ransomware kill chain steps.

1) Setting up: Crypto-ransomware installed on the victim's computer, gathering information about the device's platform type, and OS version, and installed programs by exploring the running environment.

2) Encryption key generation/recovery: Crypto-ransomware either instantly generates the encryption key or requests it from the C&C servers.

3) Files search: The ransomware begins looking for the targeted files.

4) Encryption: According to the attack strategy, the crypto-ransomware either begins encrypting the targeted files one at a time while conducting a file search or waits until it has a list of all the files before encrypting them all at once.

5) Post-encryption original files removal: After encryption is finished, the original files are either erased or relocated to a new place with new names.

6) Pop-up target/ extortion: After all data have been relocated, erased, or encrypted, the victim receives an extortion message with payment instructions. The following actions are part of the ransomware attack lifecycle's pre-encryption stage: (a) creation of the encryption key; (b) installation; and (c) file search.

7) Supply: Ransomware is packaged and delivered via exploitation techniques, such as email attachments or drive-by downloads.

Three main streams make up most of the recent research on ransomware threats. Based on static and dynamic analysis created by the scientific community, the first stream focuses on identifying recent ransomware threats. The second stream focuses on categorizing ransomware threats rather than necessarily concentrating on detection algorithms [28], [29], [30].

- Prepare: “Identifying all active assets”
- Prevent: “Blocking common ransomware spread methods”
- Detect: “Alert an unauthorized access attempt”
- Remediate: “Initiate quarantine upon attack detection”
- Recover: “Visualization for phased recovery strategies”

The third stream engages with comprehensive strategies for countering ransomware techniques and tactics. Despite the title and the general subject of the paper, this survey addresses both crypto and locking ransomware types and includes some Android ransomware incidents. Since data from different papers cannot be compared because of different metrics and approaches to ransomware, the existing surveys strictly focus on crypto ransomware while noting the challenges of surveying this novel topic [31].

Despite efforts to identify ransomware early in the pre-encryption stage, existing solutions do not consider the dynamic nature of ransomware attacks. The evolution of zero-day attacks makes detection work more difficult [32], [33] . An adaptive pre-encryption detection system is therefore needed to identify crypto-ransomware attacks before they cause extortion [34]. Studying all the APIs before any encryption function was called, also known as pre-encryption APIs, was the data of interest in this research.

General ransomware detection and analysis system. First, a ransomware dataset sample is provided for pre-encryption, and then a feature extraction module that generates a feature representation vector. A feature reduction/selection process is conducted on the feature representation vector to obtain fixed dimensionality despite the length of the input sample for increased performance. Classification/clustering approach is trained using ransomware and benign samples that are currently available. Unseen samples are reported as ransomware or not during detection and analysis by the classification/clustering approaches to warn the user. Sometimes further analysis is conducted, such as outlining any suspicious (or advantageous) traits found in the sample. Ransomware detection analysis system is a cybersecurity tool designed to detect and prevent ransomware attacks in advance.

It uses signature- and behavior-based detection techniques to identify and stop known ransomware versions. Behavior-based detection observes program and process behavior to detect ransomware-like behaviors, such as widespread file-encrypting or shady network activity. Based on ransomware-specific patterns and qualities, machine learning algorithms may also be utilized to recognize fresh and developing ransomware outbreaks, as illustrated in Fig. 4.

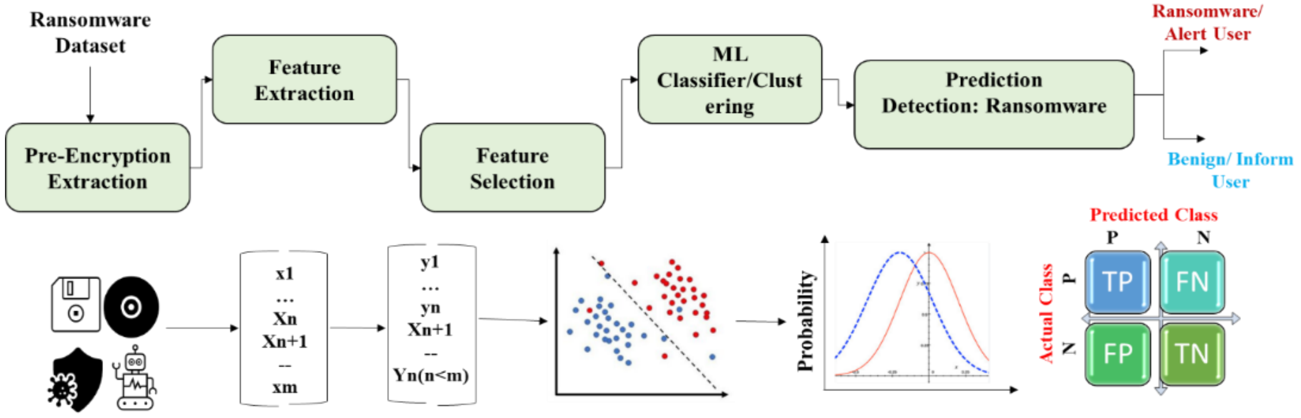

Fig. 4. Ransomware detection analysis system.

III. Research Methodology

The measures taken to examine earlier studies about ransomware attacks and detection systems are described in the methodology section. Also, inclusion and exclusion criteria were utilized to select the available research. The details of each phase of this investigation are provided in the sections that follows.

A. *Systematic Literature Review*

The PRISMA standards were used for the selection procedure, and the SLR guidelines were taken directly from [35]. The creation of review questions is the primary step. The next stage is to develop and evaluate a review technique, and then we will use the review protocol's criteria to look for primary screen studies as shown in Fig. 5. As Table IV shows different ransomware analysis tools.

TABLE IV. Ransomware Analysis Tools

Tools	Functions	Platform	Key Features	Pricing
IDA Pro	Disassembling and analysis	Win OS, Linux, macOS	Advanced disassembly and debugging capabilities	Contact for pricing
Cuckoo Sandbox	Automated malware analysis	Win OS, Linux	Dynamic behavioral analysis, threat intelligence integration	Open source
YARA	Pattern matching and detection	Win OS, Linux, macOS	Rule-based detection, custom signature creation	Open source
Wireshark	Network traffic analysis	Win OS, Linux, macOS	Packet-level analysis, protocol dissectors	Open source
Volatility	Memory forensics	Win OS, Linux	Memory image analysis, process, and DLL extraction	Open source
PEStudio	Static analysis of PE files	Win OS	Analysis of portable executable files	Free, Contact for advanced pricing
Ghidra	Reverse engineering and analysis	Win, Linux, macOS	Decomplication, the scriptable analysis environment	Open source
Procmon	Process monitoring and analysis	Win OS	Real-time process monitoring, event logging	Open source

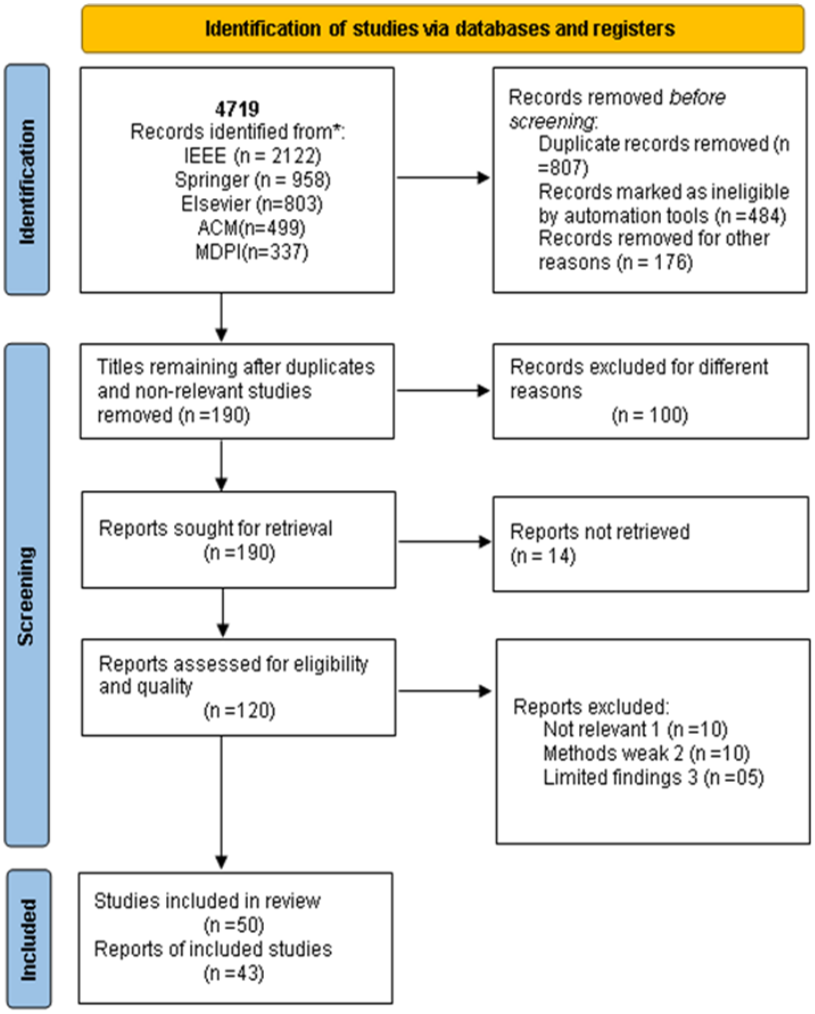
Identification of studies via databases and registers
Identification
4719
Records identified from*:
IEEE (n = 2122)
Springer (n = 958)
Elsevier (n=803)
ACM(n=499)
MDPI(n=337)
Records removed before screening:
Duplicate records removed (n =807)
Records marked as ineligible by automation tools (n =484)
Records removed for other reasons (n = 176)
Screening
Titles remaining after duplicates and non-relevant studies removed (n =190)
Records excluded for different reasons (n = 100)
Reports sought for retrieval (n =190)
Reports not retrieved (n = 14)
Reports assessed for eligibility and quality (n =120)
Reports excluded:
Not relevant 1 (n =10)
Methods weak 2 (n =10)
Limited findings 3 (n =05)
Included
Studies included in review (n =50)
Reports of included studies (n =43)

Fig. 5. Scoping literature review PRISMA.

B. Data Sources Information

The data sources utilized for the implementation of this article include IEEE Explore, ACM's digital library, Springer, Elsevier, MDPI, and online libraries. A search string is used to browse the code by the recommendations [36], [37]. The information sources that are mentioned in this review have been picked because they have high-quality, high-impact articles. Data sources were looked up in May 2023 utilizing sophisticated search tools. Table V illustrates searched databases sources.

TABLE V. SEARCH DATABASE SOURCES

Electronic Database	URLs
IEEE Xplore	(http://ieeexplore.ieee.org)
ACM Digital Library	(http://dl.acm.org/)
ScienceDirect	(http://www.sciencedirect.com)
Springer	(http://www.springer.com)
MDPI	https://www.mdpi.com/journal/futureinternet/special issues/SEO

IV. RESEARCH QUESTIONS

The goal of this study is to examine and assess several machine-learning algorithms for new ransomware detection. Research questions and research objectives (RQs and ROs) have been made to be emphasized in this SLR in Table VI.

TABLE VI. FORMULATED RQS AND ROS

No	Research Questions	Objectives
RQ1	State the current limitations in existing ransomware detection techniques that affect during the early phases.	RO1 To analyze and identify the current limitations and challenges in existing ransomware detection techniques, with a specific focus on their impact on the early phases of new ransomware attacks.
RQ2	What factors contribute to the improvement of pre-encryption for new-ransomware detection?	RO2 To Explore machine learning algorithms to detect unusual pre-encryption ransomware activities.
RQ3	How can the pre-encryption of ransomware be improved using machine learning and non-machine learning?	RO3 To identify the recent advances and techniques to overcome and improve the issue in new-ransomware pre-encryption prevention, and detection.

A. Review Protocol

The SLR metrics produced by [35] search strategy, inclusion and exclusion criteria, quality assessment, data extraction, and data analysis serve as the foundation for the review procedures.

B. Search Strategy

The most pertinent keywords and their variants were used to create the search string by the main goals of this study. Boolean operators and the keywords that were specified were used to create the search query. The search parameters and query strings are shown below in Fig. 6.

- TITLE-ABS-KEY "pre-encryption" OR "ransomware" OR "ransom" OR "malware" AND "security" ((‘‘cybersecurity’’ OR ‘‘security’’ OR ‘‘pre-encryption’’ OR ‘‘ransomware’’ OR ‘‘ransom’’) AND (‘‘ransomware detection’’ OR ‘‘ransom-ware’’ OR ‘‘malware’’ OR ‘‘encryption’’) AND (‘‘machine learning’’ OR ‘‘deep learning’’ OR ‘‘information security’’))
- The timespan to collect the studies is from 2018 to 2023 H1.
- The survey is in the English language medium.
- After finalizing the search terms, the appropriate digital repositories were chosen. We conducted searches across five electronic databases, which are listed below.
    - IEEE Xplore
    - ACM Digital Library
    - MDPI
    - Springer
    - ScienceDirect

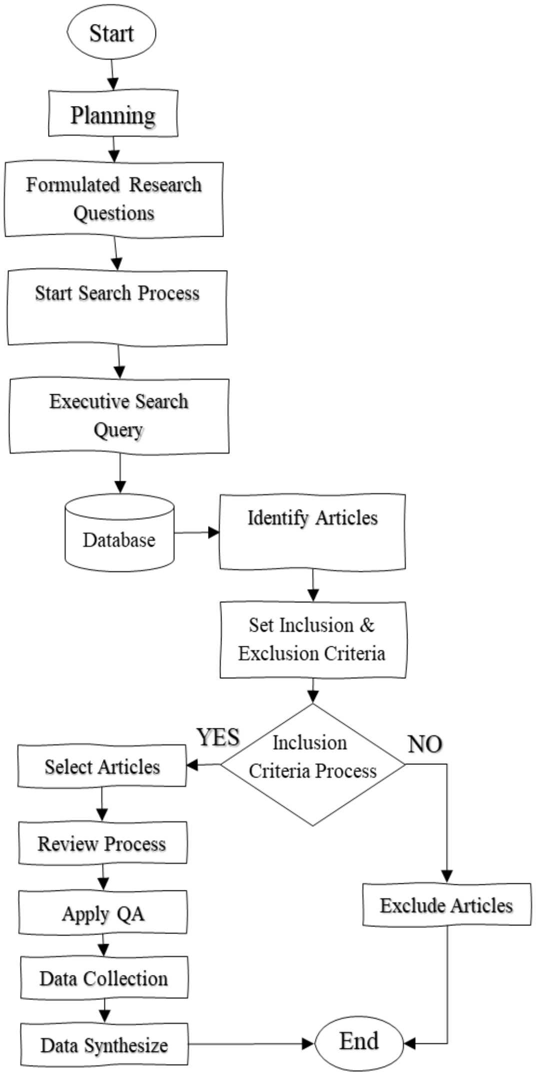

Fig. 6. Scoping review process.

The previously listed five electronic databases, which include the major publications and conferences, are searched. Second, while studies only make up just a small portion of the major research, we also compile the studies that are connected to pre-encryption ransomware detection using static analysis in the reference section. The search period covers from January 2018 to April 2023, and all research related to search phrases has been considered.

C. Inclusion and Exclusion Criteria

For the inclusion and exclusion criteria for this research, to focus on the most important criteria, scholarly works for this SLR. The shortlist is shown in Table VII. According to their capacities, studies are used to determine whether inclusion and exclusion satisfy the requirements.

TABLE VII. INCLUSION AND EXCLUSION CRITERIA

No	Inclusion Criteria	Exclusion Criteria
1	A research article published in English that focuses on the activities, assaults, defenses, and detection methods of ransomware in the Windows operating system, as well as data from peer-reviewed, reputable publications or conference papers included in the above-mentioned databases.	Analyze information from news and magazine publications, non-English articles, and information on the latest ransomware variants and vulnerabilities in other operating systems and mobile devices.
2	The article offers insights and practical advice to protect against ransomware attacks and other cyber threats and the early stage.	The article should discuss papers that investigate the impact of ransomware attacks on businesses or the legal system.
3	The document should provide an in-depth examination of ransomware or any other relevant technological advancement in your writing.	Governmental documents and blogs should not be included in the article.

Three steps made up the selection process. The first step was to look for any possible primary studies. The next step involved examining and reading the titles. Abstracts of all the papers that were returned by the search. So, we discovered every piece of research that met the requirements for inclusion and exclusion. After that every study that had been found was read already being selected for final selection.

Diagram illustrating the preferred reporting items for systematic reviews and Meta-Analysis (PRISMA) flow process showing the ultimate number of studies included in the systematic review and meta-analysis as well as the inclusion and exclusion of studies. Fig. 7 shows selection criteria for this study.

D. Quality Assessment Criteria

We screen the chosen studies following the quality assessment criteria and Score listed in Table VIII, Table IX to evaluate their quality. We determine whether the chosen studies meet these requirements using the cross-checking method to guarantee the reliability of the results. The final studies, which include, are obtained following the stage of quality assessment criteria, concerning the detection of ransomware, there are 103 studies and 2 SLRs related to this.

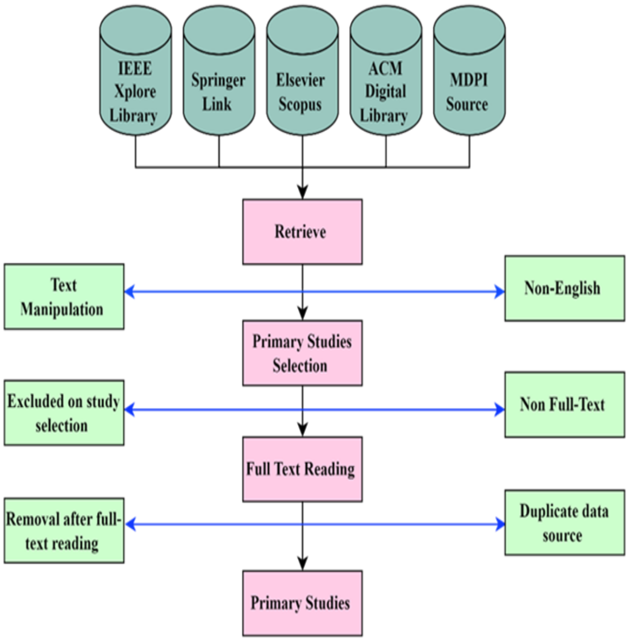

Fig. 7. Study selection criteria.

TABLE VIII. QUALITY ASSESSMENT CRITERIA

No	Quality Assessment Criteria
1	Is the study's direction clear?
2	Is the approach for static and dynamic well stated?
3	Do the experimental datasets provide clear descriptions?
4	Exactly what features are being used?
5	Is the model mentioned clearly?
6	Do the empirical experiments provide a clear description?
7	Are performance metrics given in a transparent manner?
8	Does the research study contribute to this SLR?

TABLE IX. QUALITY ASSESSMENT SCORE

No	Category	Result
1	Systematically Adopted	3
2	Reviewed effectively	2
3	Minor declared	1
4	Does not mention	0

E. Data Extraction

To support the study questions, the required data was acquired, and a detailed analysis was conducted. The following details were extracted from the selected primary studies and entered an extraction form that had been pre-made. Fig. 8 shows extraction of complete information.

- Class, Info, and reference ID
- Publication name
- Country of organization
- Authority of research

- The type of machine learning methods used to mitigate ransomware.
- Algorithms, models, and ideas are essential.
- Categorization of machine learning algorithm with a certain approach and analysis type.
- For ransomware detection process tools were used.

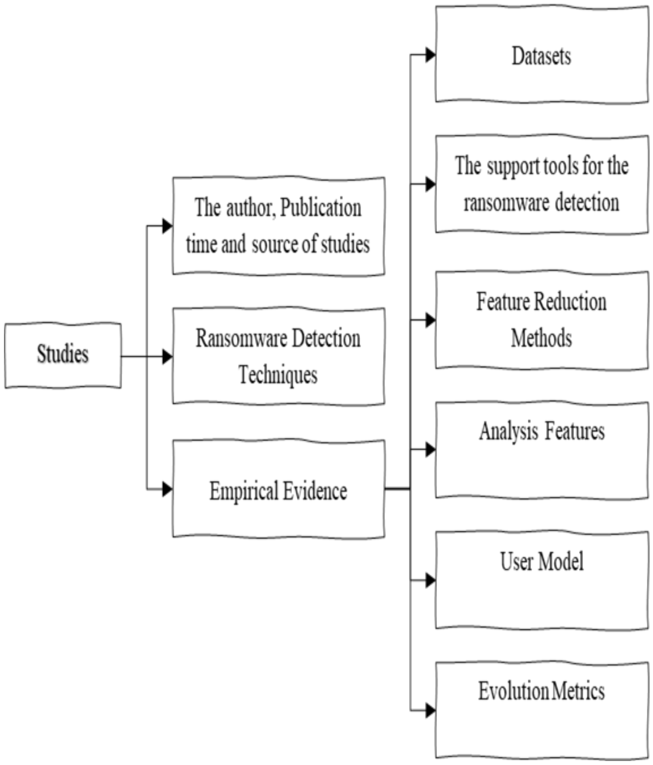
Studies
The author, Publication time and source of studies
Ransomware Detection Techniques
Empirical Evidence
Datasets
The support tools for the ransomware detection
Feature Reduction Methods
Analysis Features
User Model
Evolution Metrics

Fig. 8. Information extraction.

F. *Data Analysis*

Each main study's data was extracted, and then each research question was addressed with thorough data analysis. Machine learning algorithms that had been implemented were identified to respond to RQ1, and their effectiveness was assessed to respond to RQ2. Related theories or models were found for each category and key features of successful pre-encryption detection as RQ2.1. The outputs of the algorithm were evaluated in terms of their ability to respond to RQ3.

1) Difficulty of problem in practice: It is highly recommended to study the idea of ransomware camouflage to learn more about and develop the field of malware analysis and new ransomware detection. Malware camouflage involves using techniques to hide harmful code, extending its undetected presence by eluding conventional malware detection tools. Malware authors use a variety of strategies, from straightforward ones like encryption to more complex ones like metamorphism. For academics and security experts to create efficient defenses against developing malware threats and improve overall detection methods, they must be aware of various disguise strategies [20].

2) Sophisticated techniques: In the context of ransomware, sophisticated tactics relate to sophisticated and complicated ways employed by attackers to conduct effective and evasive ransomware operations. These strategies aim to circumvent established cybersecurity defenses and increase the difficulty of discovery, prevention, and recovery.

3) Encryption and data exfiltration: Data security and privacy are seriously threatened by ransomware attacks, which are crucially based on encryption and data exfiltration. Effective cybersecurity measures need a thorough understanding of data exfiltration risks, ransomware use of encryption, and related issues.

4) Impact on critical systems: New ransomware attacks can have severe consequences, especially when targeting critical infrastructure systems, healthcare institutions, or government agencies. Disruptions caused by new ransomware can lead to financial losses, endanger lives, or compromise sensitive national security information.

V. Ransomware Detection Taxonomy

The methodologies utilized to identify ransomware, the operation of the machine learning algorithm, the performance outcome, the classification strategy, and the chosen analysis type used to respond to RQ1 through RQ3 are all covered in this part.

The motivating methodology, findings, restrictions, and future directions of the investigated approaches were all covered in the authors' assessment of the ransomware detection methods put out in the literature. They also examined several ransomware detection methods about factors including the operating system for mobile devices and PCs, the cloud, data sources, various machine learning algorithms in use, and result and assessment standards. Fig. 10 demonstrates the ransomware detection environments, along with the many standards and related metrics. The comparison charts of the detection environment, data analysis, machine learning, results, and assessment criteria charts are shown in Fig. 9 to 13.

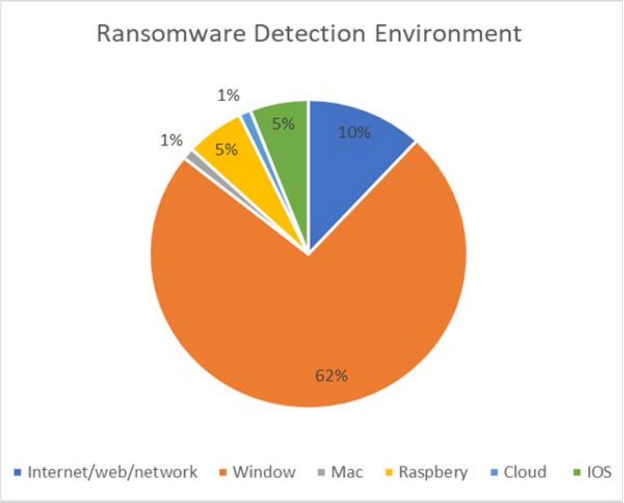

Fig. 9. Ransomware detection environments.

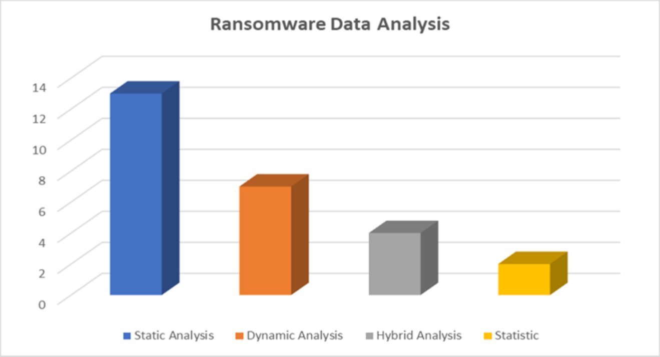

Fig. 10. Ransomware data analysis understanding.

A. *Early Detection*

Early detection of ransomware is crucial for preventing data encryption and minimizing attacks. The Pre-Encryption Detection Algorithm (PEDA) is a machine learning-based algorithm that detects ransomware behavior patterns before the encryption process begins. This helps identify patterns and characteristics indicative of ransomware before it can cause severe damage. Runtime data analysis captures runtime data during the initial phases of ransomware attacks, allowing for the identification of patterns and indicators of ransomware. However, challenges like accurately defining pre-encryption phases and limited data availability require further research to develop more robust techniques. Combining machine learning algorithms like PEDA with runtime data analysis can contribute to the early detection of ransomware and improve the effectiveness of preventive measures [16].

Ransomware detection environments play a crucial role in safeguarding organizations and individuals from the ever-increasing threat of ransomware attacks. These detection environments are designed to identify and mitigate ransomware activities during the initial stages, before encryption occurs, and severe damage is inflicted.

“Ransomware data analysis understanding" refers to the process of examining, interpreting, and making sense of data related to ransomware attacks. This involves delving into various aspects of ransomware incidents, and analysis techniques as shown in Fig. 10.

A thorough taxonomy of ransomware detection is comparable to an orderly road map of the various kinds, techniques, and strategies applied to the identification and mitigation of ransomware threats in Fig. 11 and classifies the various methods, tools, and approaches used in cybersecurity.

Comparison of the effectiveness of different machine learning classifiers used especially for ransomware detection. It suggests assessing various models or algorithms for ransomware classification, stressing their relative performance and efficacy as shown in Fig. 12.Machine learning classifiers.

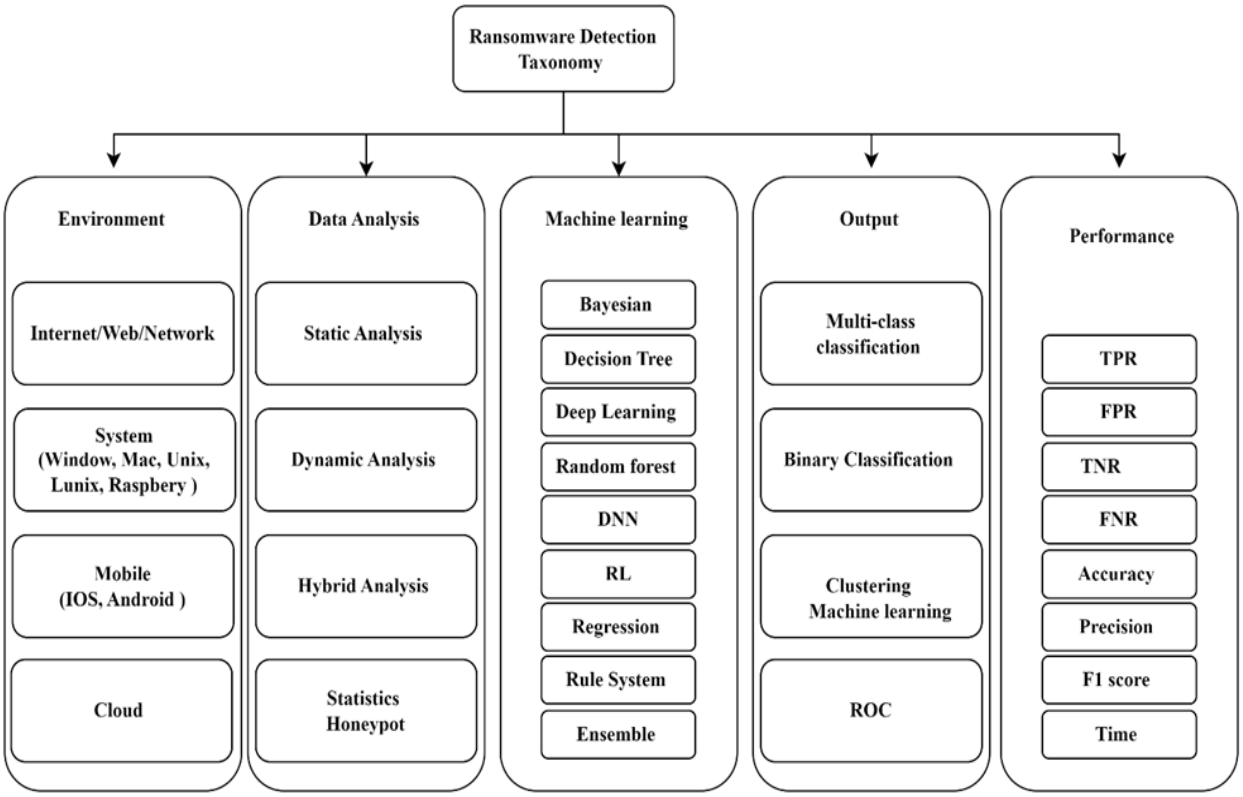

Fig. 11. A comprehensive ransomware detection taxonomy assists cybersecurity.

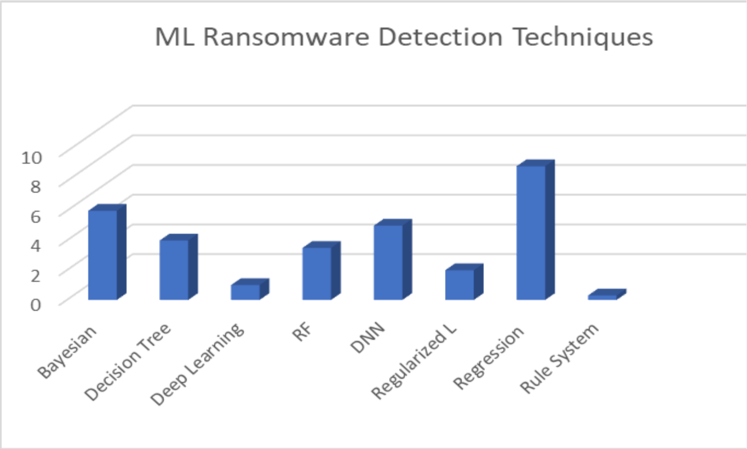

Fig. 12. Machine learning classifiers.

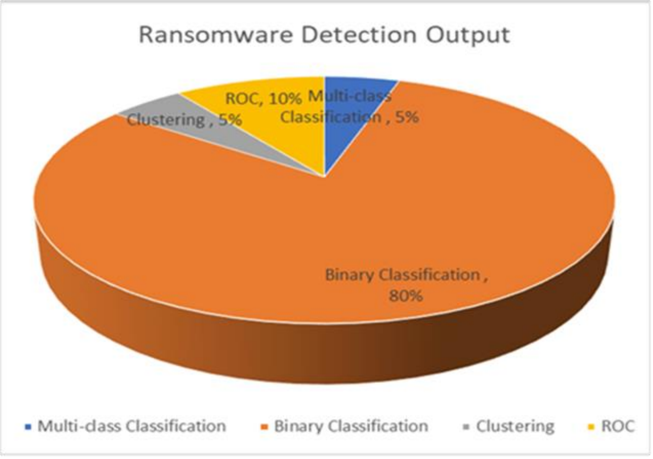

Fig. 13. Ransomware output responding to threats promptly.

Outcomes produced by a system for detecting ransomware. It highlights how quickly the system can detect any ransomware threats. The picture illustrates the steps involved in detecting these threats and taking appropriate action in response, emphasizing how crucial prompt and efficient action is in lessening the impact of ransomware attacks.

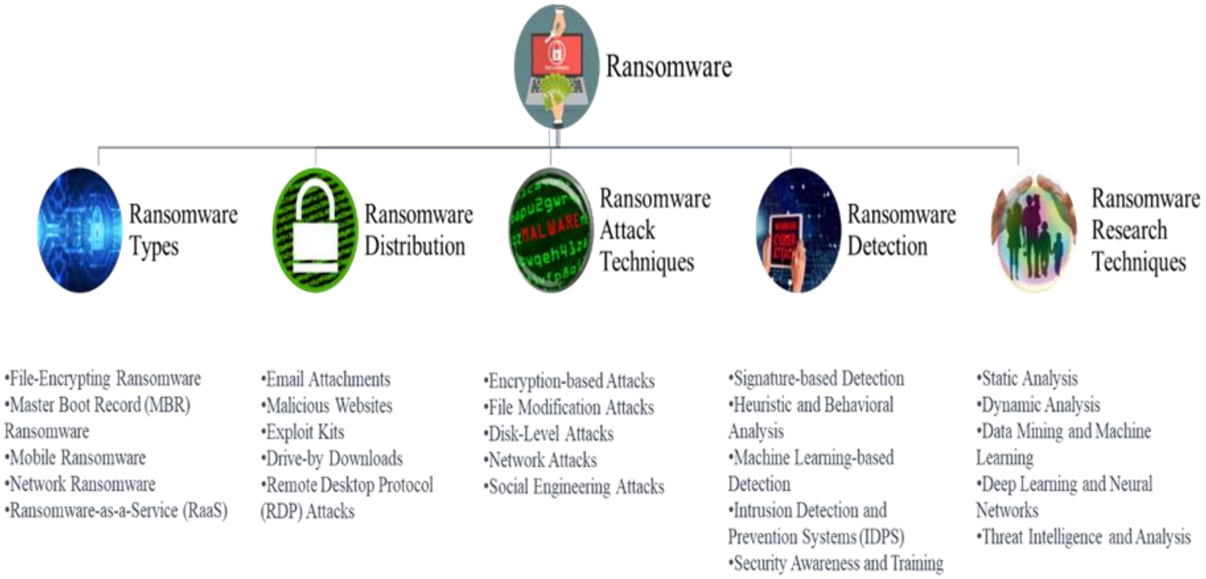
Ransomware
Ransomware Types
Ransomware Distribution
Ransomware Attack Techniques
Ransomware Detection
Ransomware Research Techniques
•File-Encrypting Ransomware
•Master Boot Record (MBR) Ransomware
•Mobile Ransomware
•Network Ransomware
•Ransomware-as-a-Service (RaaS)
•Email Attachments
•Malicious Websites
•Exploit Kits
•Drive-by Downloads
•Remote Desktop Protocol (RDP) Attacks
•Encryption-based Attacks
•File Modification Attacks
•Disk-Level Attacks
•Network Attacks
•Social Engineering Attacks
•Signature-based Detection
•Heuristic and Behavioral Analysis
•Machine Learning-based Detection
•Intrusion Detection and Prevention Systems (IDPS)
•Security Awareness and Training
•Static Analysis
•Dynamic Analysis
•Data Mining and Machine Learning
•Deep Learning and Neural Networks
•Threat Intelligence and Analysis

Fig. 14. Ransomware techniques overview.

Fig. 14 presents a summary of the ransomware approaches discussed in this section, categorized by approach type, analysis features, and availability. However, upon thorough examination of the literature, it became evident that previous studies had certain limitations. Specifically, there was a lack of research focusing on ransomware, with most works primarily utilizing static analysis for detection. Moreover, since ransomware can evade static analysis through code obfuscation techniques, it is crucial to incorporate dynamic analysis. Unfortunately, existing dynamic analysis tools target malicious programs rather than ransomware, and some tools are either immature, outdated or only accessible commercially. Consequently, a need to propose a hybrid system that investigates the effectiveness of integrating techniques, and static and dynamic analysis to detect ransomware more efficiently and accurately, thereby safeguarding system users from falling victim to such attacks. This hybrid system should incorporate various established static analysis approaches and evaluate their ability to differentiate between ransomware apps and benign apps. Based on the results of the static analysis, a decision can be made regarding the need for additional dynamic analysis on these apps. Furthermore, careful consideration should be given to selecting appropriate tools for conducting dynamic analysis. The primary objective is to achieve accurate pre-encryption ransomware detection while minimizing costs. Table X contains the different ransomware detection approaches**.**

TABLE X. PRE-ENCRYPTION RANSOMWARE DETECTION METHODS

Detection Method	**Description**
File Signature	Finds ransomware based on known file signatures
Behavior Analysis	Monitors unusual file access or encryption behavior
Heuristic Analysis	Finds potential ransomware based on patterns
Machine Learning	Uses algorithms to detect ransomware-like behavior
Sandbox Analysis	Executes files in a controlled environment for detection

Metrics used to evaluate the efficacy of ransomware detection and mitigation techniques are included, such as detection accuracy, false positive rates, mitigation speed, and recovery efficiency. An examination of these metrics across time or several approaches may be shown in Fig. 15 along with trends.

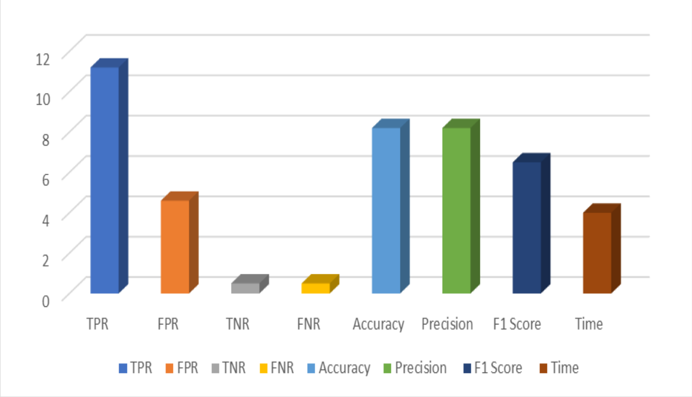

Fig. 15. Performance evaluation metrics of ransomware detection and mitigation.

B. *Ransomware Detection Based on Machine Learning*

Preventing ransomware is difficult for several reasons. Ransomware often mimics the behavior of legitimate software, operating in a covert manner. As a result, detecting ransomware in zero-day attacks has become a critical priority. The main goals are to prevent system damage caused by ransomware, identify previously unknown malware (zero-day attacks), and reduce detection time. Various tools and techniques are available for detecting ransomware. Static analysis methods, for example, examine source code without executing it. However, these methods tend to produce many false positives and struggle to detect ransomware that has been obfuscated. As Table XI represent existing detection techniques. Attackers frequently develop new variants and modify their code using different packing techniques. To address these challenges, researchers have turned to dynamic behavior analysis, which observes how executed code interacts with a virtual environment. While effective, these methods can be resource-heavy and slow. Machine learning, by contrast, excels at analyzing the behavior of applications or processes. Several machine learning-based detection systems follow well-established methodologies: Table XII summarizes previous studies on Machine learning techniques (behavioral techniques) for ransomware detection.

TABLE XI. EXISTING RANSOMWARE DETECTION TECHNIQUES

Study	**Year**	**Features used**	**Static**	**Dynamic**	**Available**
[38]	2018	Employs Droid Bot, test response creator, and API Packages	×	✓	×
[39]	2018	UI widgets, users' finger activities	×	✓	×
[40]	2019	Text, sysadmin, win pro, sys Opp, Priority, Consent	×	✓	×
[15]	2020	27 API-level, permissions	✓	×	✓
[41]	2020	General features in Static	✓	×	✓
[42]	2020	API call level 27	✓	×	✓
[43]	2021	API call level 30s	✓	×	✓
[48]	2022	ML-based API Calls	×	✓	✓
[44]	2021	API call level 30	✓	×	✓

TABLE XII. COLLECTED STUDIES ON ML-BASED RANSOMWARE DETECTION

Study	Features	AI Techniques												Accuracy
		ML Classifier								DL Techniques				
		DT	RF	GB	NB	SVM	LR	KNN	XGB	LSTM	ANN	RNN	MLP	
[45]	Network traffic	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	99.8%
[46]	API calls	✓	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	98.63%
[47]	Access privileges, read/write/implement/copy	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	96.28%
[48]	API calls	✗	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✗	94.9%
[15]	API calls	✓	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗	✓	97.08%
[19]	API	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	--
[49]	IRPs	✓	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	96.6%
[50]	Opcode sequence	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	99.3%
[39]	API calls packages	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	97%
[11]	APIs, IRPs	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	--
[51]	C&C, no of bytes read/written	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	99.9%
[52]	Power/energy consumption patterns	✗	✓	✗	✗	✓	✗	✓	✗	✗	✓	✗	✗	83.7%
[53]	API calls	-	-	-	-	-	-	-	-	✓	✗	✓	✗	93%
[56]	System logs, network logs	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	98.5%
[54]	DLL, function calls assembly levels	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	99.7%
[55]	Raw byte	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	97.7%

1) *File behavior analysis:* Machine learning algorithms can analyze the behavior of files on a system to detect ransomware. By creating baselines of legitimate code executions, the algorithms can detect any behavior that deviates from those baselines.

2) *Network traffic analysis:* Algorithms based on machine learning can analyze network traffic to detect ransomware. By monitoring the traffic patterns and identifying anomalies, the algorithms can detect ransomware attacks.

3) *Dynamic feature dataset:* A dynamic feature dataset can be used to detect ransomware using machine learning algorithms. The dataset contains features that are extracted from the binary file of the ransomware. By analyzing these features, the algorithms can detect ransomware attacks.

4) *Multi-classifier network-based system:* A multi-classifier network-based system can be used to detect ransomware. The system uses machine learning algorithms to analyze the behavior of files and network traffic. By combining the results of multiple classifiers, the system can improve the accuracy of ransomware detection.

C. Limitations of Machine Learning Based Ransomware Detection

The limitations of machine learning-based ransomware detection can be summarized as follows:

1) *False negatives:* Machine learning algorithms can sometimes fail to detect ransomware attacks, resulting in false negatives. This can be due to the lack of training data or the inability of the algorithm to detect new variants of ransomware.

2) *Limited dataset:* The accuracy of machine learning algorithms depends on the quality and quantity of the dataset used for training. A limited dataset may not capture all the variations of ransomware, leading to inaccurate results.

3) *Overfitting:* Machine learning algorithms can sometimes overfit the training data, resulting in deficient performance on new data. This can be due to the algorithm's complexity or the lack of regularization.

4) *Encryption:* Ransomware attacks often involve the encryption of files, which can make it difficult for machine learning algorithms to detect them. This is because the encrypted files may not contain the same features as the original files.

5) *Adversarial attacks:* Adversarial attacks can be used to evade ransomware detection based on machine learning. Attackers can modify the ransomware code to bypass the detection algorithm.

Study has explored the use of machine learning algorithms such as the J48 decision tree and random forest to detect and classify different ransomware families based on TCP malware network traffic [45]. Another study introduced a new approach called WmRmR to detect early ransomware, effectively evaluating the fundamental characteristics of large-scale datasets at low complexity and false positive rates [46]. A related study proposes a detection method focused on analyzing access privileges in process memory and enabling accurate and efficient identification of key functions of ransomware [47]. In the field of ransomware classification, researchers developed an advanced technique to exploit the suspicious behaviors displayed by ransomware, in particular several API requests to find an optimal execution environment. By generating fingerprints of these behaviors from more than 3,000 recently known ransomware samples, the authors achieved an impressive classification accuracy of 94.92% [48]. The redundancy coefficient gradual upweighting (RCGU) approach improves the selection of crypto-ransomware detection features by dynamically adjusting the weight of redundancy terms. The combination of RCGU and other mutual information methods further improved accuracy compared to previous studies [15]. Several studies focused on the detection of Android ransomware. Researchers have been using decoy techniques to detect ransomware in real-time, monitor file systems and running processes, and identify and prevent benign file changes from triggering alerts based on learned encryption behavior [49]. Developed a classification model. Using N-gram sequences from ransomware sample opcode sequences, it is possible to classify families more accurately [50]. The API-based ransomware detection system (API-RDS) was used to study the static and dynamic analytical approach of ransomware detection in mobile devices. Although this approach has not been put into practice or proven through simulation, the author presented it as a framework for the early detection of ransomware, considering the temporal correlations between IRPs and APIs. In the context of network traffic analysis [11]. This study presented a detection approach based on the analysis of file-sharing traffic, effective detection, and prevention of crypto-ransomware activity [51]. The author introduced a unique method for detecting Android ransomware with energy consumption levels [52]. The study incorporated an attention mechanism in learning malware sequences to detect ransomware based on repetitive patterns associated with repeated encryption [53]. The author proposed artificial intelligence-powered hybrid models that would overcome the challenges of detecting ransomware using functions such as assembly, dynamic link libraries, and function calls [54]. Based on the ease of static malware analysis, an approach based on data mining techniques in particular, frequent pattern mining was developed to identify ransomware. Similarly, a pre-distributed model was created using convolutional neural networks to classify binary items and improve performance using transfer learning [55].

D. Non-Machine Learning Based Ransomware Detection

The term "non-machine learning-based ransomware detection" refers to techniques that do not rely on machine learning algorithms but rather are conventional and rule-based. This method is useful in some circumstances since it makes use of predetermined rules, patterns, and heuristics to find ransomware activity. Known signatures or patterns of previously recognized ransomware variants are used to identify and stop ransomware in one popular technique called signature-based detection. Another method is behavior-based detection, which keeps an eye on system activity for ransomware-specific suspicious behaviors such as quick file encryption. Furthermore, even if the precise ransomware strain is unknown, heuristics may be used to spot ransomware-like behavior. Non-machine learning-based techniques may be able to provide quick detection and reaction capabilities shown in Table XIII, but they could have trouble spotting new or polymorphic ransomware versions. The authors also discussed the integration of this contextual detection technique into digital forensics for ransomware mitigation and prevention [57].

A software-defined network (SDN)-based detection technique for Windows computers was also demonstrated in [58]. The technique extracts pertinent HTTP message sequences as key features from network traffic between the crypto-ransomware variants Crypto Wall and Locky. The reading and writing activities of backup files and ransomware samples with significant read/write operations are tracked. The context-aware detection model uses entropy data to spot unusual file activity [24]. The basis for the detection is manipulation files (such as desktop files and/or user files). The system creates a fake user environment and can identify file modifications caused by ransomware. The system keeps track of system modifications as well as their behavior. The detection can spot previously unreported, unknown (zero-day), and evasive ransomware. Passively observes traffic produced by 19 ransomware families using a network prober. Less than 10 files are lost prior to the ransomware activity being detected by the model, which focuses on early detection [59] and examines the characteristics of cryptographic ransomware. To stop ransomware, they suggested deceptive file protection methods. Incorporated a dynamic analysis-based automated malware detection technology. The latter extracts a call to the Application Programming Interface (API) from logs to find ransomware [62]. The researchers demonstrated how their techniques could enhance the automatic analysis of numerous malware samples [63], [64]. To categorize tweets to fulfill the requirement for file protection on rootless devices, they developed and deployed KRProtector, which can recognize ransomware and protect files using deception [65], [66]. The author used static and dynamic analysis of the executable malware to extract both static and running-time behavior. Reverse engineering is used to extract binary signatures using the CRSTATIC model. No matter what kind of malware is being assessed, the authors show that using YARA rules with fuzzy hashing can enhance the evaluation's outcomes [67], [68], [69], [70].

TABLE XIII. COLLECTED STUDIES ON NON ML-BASED RANSOMWARE DETECTION

Study	Methods	Features	Evaluation metrics	Correctness	Platform	Environment
[57]	Rule-based	API calls DLL libraries windows registry	Trigger threshold CAT	-	OS	Cuckoo sandbox
[58]	Software-defined network	HTTP	ROC curve	-	OS-7	Cuckoo Sandbox, VMware
[24]	Hardware-based	I/O requests	Accuracy	96.3%	OS	Cuckoo sandbox
[59]	Rule-based	IP traffic	Overhead detection rate, file lost	100%	OS-7	Virtual
[60]	Decoy-based	File access read/write/remove	Precision Accuracy	96.2%	IoT Android	Real in Android 7.1
[61], [64]	Forensic based	Network sign Function calls	-	-	OS	Real in testbed

VI. Results

The results of primary research are intended to be presented in this section. We begin by outlining the main studies. In terms of fact, we next provide the SLR's findings considering the study's questions.

A. *Study Description*

103 Studies are addressed in this section in terms of publication time.

B. *Publication Time*

Fig. 16 demonstrates that there were 26, 25, 25, 23, 10, and 26, respectively, studies from 2018 to 2023-H1. This data shows that the number of studies in 2018 accounts for the biggest share. The number of research connected to ransomware detection using static analysis and dynamic is increasing from 2018 to 2023, except for certain papers in 2023 (some publications in 2023 are not released, thus the time of these papers in 2023 is from January to May) [71], [72], [73]. This data indicates that pre-encryption ransomware detection has consistently been a popular issue in recent years.

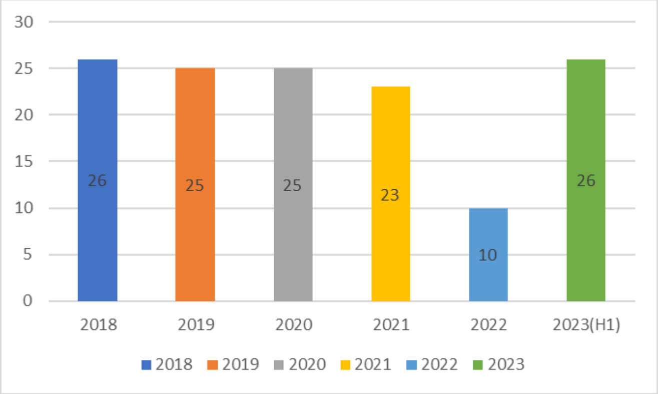

Fig. 16. Year-wise distribution of studies.

RQ1: What are the current limitations/challenges in existing ransomware detection techniques that affect during the early phases?

There are several limitations and challenges in existing ransomware detection techniques that affect early detection. These include:

- Signature-based detection is easily bypassed by malware authors. Signature-based detection relies on identifying known malicious files or patterns. However, malware authors can easily obfuscate their code to evade detection by signature-based tools [74], [75], [76], [77].
- Behavior-based detection can be triggered by legitimate applications. Behavior-based detection looks for suspicious or malicious behavior, such as file encryption or network traffic patterns. However, legitimate applications can also exhibit these same behaviors, which can lead to false positives [78], [79], [80], [81].
- Ransomware attacks are often targeted and stealthy. Ransomware authors often target specific organizations or individuals, and they may take steps to conceal their attack. This can make it difficult for detection tools to identify the attack in its initial stages [82], [83], [84], [85].
- Ransomware is constantly evolving. Ransomware authors are constantly developing new techniques to evade detection. This makes it difficult for detection tools to keep up with the latest threats.

As a result of these limitations and challenges, it can be difficult to detect ransomware in its initial stages. This is why it is important to have a layered security approach that includes a variety of detection techniques. By combining signature-based, behavior-based, and other detection techniques, organizations can improve their chances of detecting ransomware early and preventing a successful attack [86], [87], [88], [89].

- Insufficient data and attack patterns
- Evolving tactics and techniques
- Lack of awareness
- Visibility into systems

The current limitations/challenges in existing ransomware detection techniques during the early phases include insufficient data and attack patterns, evolving tactics and techniques, limited detection capabilities, lack of awareness, and limited visibility into systems. These challenges require innovative solutions and collaborative efforts to combat the rise of ransomware attacks.

RQ2: What factors contribute to the improvement of pre-encryption ransomware detection?

Improving pre-encryption ransomware detection requires the development of advanced detection techniques, such as behavior matching, machine learning, detection of symmetrical and asymmetrical encryption, early detection, high detection rate, and continuous updates. These factors can help improve the detection and prevention of ransomware attacks.

1) *Pre-encryption detection algorithms:* Pre-encryption detection algorithms, such as the Pre-Encryption Detection Algorithm (PEDA), can detect ransomware before it starts its encryption function. These algorithms use machine learning or behavior matching to identify patterns in the ransomware code and create a signature repository to detect future attacks [19].

2) *Adaptive models:* Adaptive models that combine machine learning and non-machine learning techniques can improve pre-encryption ransomware detection. For example, an adaptive pre-encryption crypto-ransomware early detection model uses both machine learning and non-machine learning techniques to detect ransomware before it can be executed [90], [91].

3) *Behavior matching:* Behavior matching can be used to detect small variants of unknown crypto-ransomware. This approach involves comparing the behavior of a file to a known set of behaviors associated with ransomware [92], [93], [94].

4) *Improved visibility:* Improved visibility into network activities can help detect ransomware during its early phases. This involves monitoring, aggregation, correlation, and analysis

of network activities to identify suspicious behavior [95], [96], [97].

Continuous research and collaboration: Continuous research and collaboration are needed to stay ahead of evolving ransomware tactics and techniques. This includes sharing threat intelligence and developing new detection techniques to address emerging threats and evaluation metrics for crypto-ransomware.

Q3 How can the pre-encryption of ransomware be improved using machine learning and non-machine learning?

Improving the pre-encryption detection of ransomware can be achieved through the integration of both machine learning and non-machine learning techniques. Machine learning approaches enhance pre-encryption ransomware detection by leveraging advanced algorithms to analyze data and identify patterns indicative of ransomware behavior. Through feature engineering, anomaly detection, and deep learning models, machine learning can detect ransomware with higher accuracy and adapt to new variants. Ensemble methods and continuous learning mechanisms further enhance the detection capabilities. On the other hand, non-machine learning approaches such as signature-based detection, heuristics, behavioral analysis, and network traffic analysis provide additional layers of defense. By combining these approaches, organizations can leverage the strengths of both methods. As shown in Fig. 17, detection system analyzes ransomware behaviors, utilizing classifiers.

Non-machine learning techniques offer rule-based detection and proactive measures such as authorization, block-listing, and user education. Integrating machine learning with non-machine learning techniques creates a comprehensive defense strategy that improves pre-encryption ransomware detection, providing more effective protection against emerging threats and reducing the risk of successful attacks [98], [99], [101]. Machine learning techniques have progressively been widely used for ransomware detection in recent years due to the rapid growth of these techniques in natural language processing, image recognition, and other areas. Support Vector Machine (SVM), Naive Bayes (NB), Logistic Regression (LR), Ensemble Learning (EL), and neural networks are some of the machine learning models that are frequently utilized in primary investigations [100], [102], [103]. Table XIV shows ML and Non-ML based methods.

By utilizing a combination of machine learning and non-machine learning approaches, organizations can improve pre-encryption ransomware detection, providing more robust and proactive defenses against ransomware threats. The integration of these methods complements each other, resulting in a comprehensive approach that enhances detection accuracy and responsiveness, thus minimizing the potential impact of ransomware attacks (Fig. 18) [93].

To extract configuration, "MalConfScan with Cuckoo" launches malware on the host computer. MalConfScan can extract the configuration of recognized malware from a memory image that is dumped when malware is registered on Cuckoo and executed on the host computer. A report will then display the extracted configuration that can be seen in Fig. 18 [93].

JPCERTCC/MalConfScan-GitHub
https://github.com/JPCERTCC/MalConfScan-with-Cuckoo

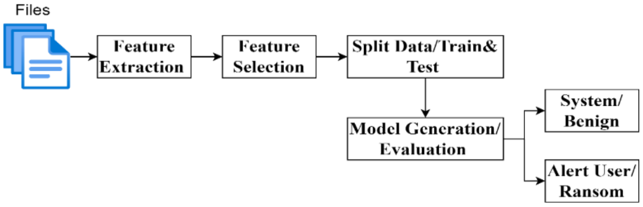

Fig. 17. Machine learning detection for ransomware.

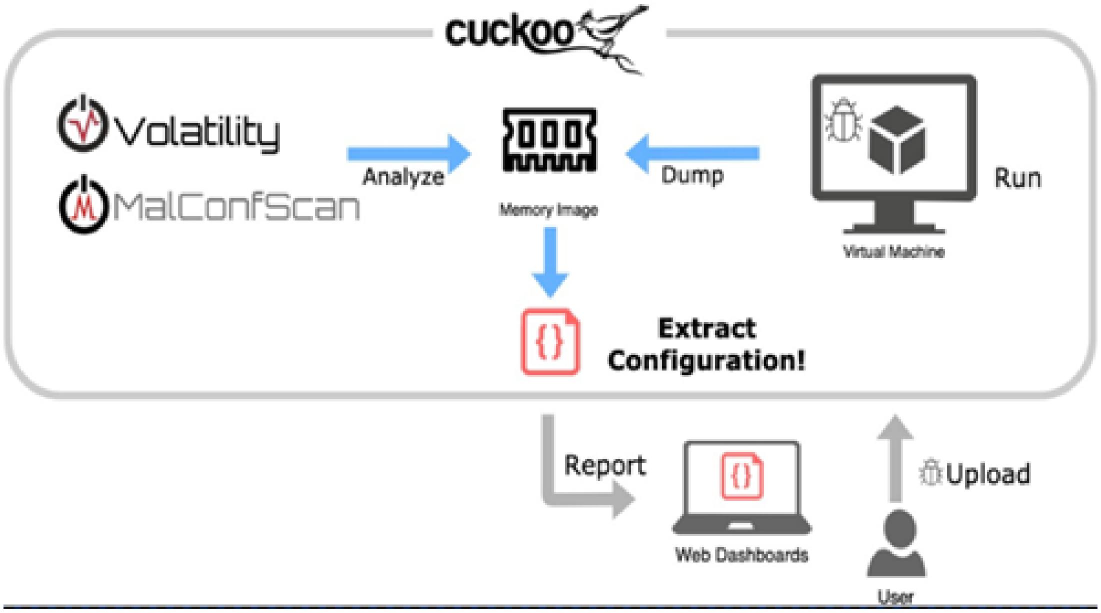

Fig. 18. Non-machine learning detection for ransomware [93].

TABLE XIV. ML AND NON-ML-BASED METHODS

Method	Machine Learning Approach	Non-Machine Learning Approach
Feature Engineering	- Extract relevant and discriminative features from data	- Define heuristics based on known ransomware characteristics
	- Find patterns using deep learning models	- Create rules to detect ransomware behaviors
Anomaly Detection	- Detect deviations from normal system behavior	- Monitor network traffic for unusual patterns
	- Find abnormal file access patterns	- See unusual file encryption behavior
Ensemble Methods	- Combine multiple models to enhance detection performance	- Integrate various detection techniques for comprehensive analysis
	- Reduce false positives through ensemble approaches	- Combine signature-based and heuristic-based detection
Continuous Learning	- Adapt models in real-time with new ransomware samples	- Update signature databases regularly
	- Stay up to date with evolving ransomware variants	- Check for new ransomware families
Dynamic Analysis	- Analyze ransomware behavior in sandboxed environments	- See ransomware actions in isolated systems
	- Find malicious code execution within the sandbox	

VII. RESEARCH DIRECTION

This paper provides a brief overview of machine learning, and deep learning techniques applied to the detection of ransomware. To increase the effectiveness of ransomware detection systems, additional research is required on several open issues.

1) High computational complexity and time: Develop efficient detection systems for new ransomware attacks, considering computational overhead for low-resource devices like embedded systems and IoT.

2) Hardware complexity: Modern systems rely on RAM-intensive hard drives, requiring careful consideration of hardware limitations for sophisticated detection systems and solutions.

3) Evasion and obfuscation: Ransomware detection is dynamic, requiring evasive and secretive methods for accuracy, less false alarms, and dependable handling of escape and confusion.

4) Rich Dataset: Dataset for ransomware attack patterns training machine learning and deep learning models; regular updates needed for effective ransomware detection systems.

VIII. CONCLUSION

This article presents an overview of ransomware detection using heuristic-based machine learning, and non-machine learning technologies. It investigates various ransomware platform detection tools and uses datasets containing different methods. The study provides taxonomy and related concepts for research on new ransomware detection methods, categorizing studies into classical, conventional, and early detection before encryption. It examines the frequency of attack patterns across different platforms and analyzes attacks targeting these platforms. Using heuristic-based machine learning approaches can produce a reliable and precise solution for new ransomware attack patterns. The study aims to encourage academics to use contemporary technologies in ransomware attack detection, evaluating potential solutions and creating more effective models. The main findings and contributions of the reviews shed light on new ransomware detection and pre-encryption strategies. Heuristic-based machine learning should be the focus of future research to identify new ransomware patterns, adjust to changing strategies, and combat evasion methods. In future noise data can be reduced during feature extraction process. Sustained innovation is essential to keep up with the evolution of ransomware.

ACKNOWLEDGMENT

This research is funded by the Fundamental Research Grant Scheme (FRGS) under cost Centre (015MA0-151) from the Ministry of Higher Education (MOHE) Malaysia.

REFERENCES

[1] T. B. Slayton, “Ransomware: The virus attacking the healthcare industry,” J. Leg. Med., vol. 38, no. 2, pp. 287–311, 2018, doi: 10.1080/01947648.2018.1473186.

[2] P. Kuper, “The state of security,” IEEE Secur. Priv., vol. 3, no. 5, pp. 51–53, 2005, doi: 10.1109/MSP.2005.134.

[3] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, “Ransomware detection and mitigation using software-defined networking: The case of WannaCry,” Comput. Electr. Eng., vol. 76, no. March 2019, pp. 111–121, 2019, doi: 10.1016/j.compeleceng.2019.03.012.

[4] S. Razaulla et al., “The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions,” IEEE Access, vol. 11, no. April, pp. 40698–40723, 2023, doi: 10.1109/ACCESS.2023.3268535.

[5] ENISA, Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends, no. January. 2018. doi: 10.2824/622757.

[6] N. Scaife, H. Carter, P. Traynor and K. R. B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), Nara, Japan, 2016, pp. 303-312, doi: 10.1109/ICDCS.2016.46.

[7] M. Hamad and D. Eleyan, “Survey On Ransomware Evolution, Prevention, And Mitigation,” Lume, vol. 10, no. October, p. 2, 2021, [Online]. Available: www.ijstr.org

[8] Bo Li, Kevin Roundy, Chris Gates, and Yevgeniy Vorobeychik. 2017. Large-Scale Identification of Malicious Singleton Files. In Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy (CODASPY '17). Association for Computing Machinery, New York, NY, USA, 227–238. https://doi.org/10.1145/3029806.3029815

[9] Heena, “Advances In Malware Detection- An Overview,” 2021, [Online]. Available: http://arxiv.org/abs/2104.01835

[10] S. I. Popoola, U. B. Iyekekpolo, S. O. Ojewande, F. O. Sweetwilliams, S. N. John, and A. A. Atayero, “Ransomware: Current trend, challenges, and research directions,” Lect. Notes Eng. Comput. Sci., vol. 1, pp. 169–174, 2017.

[11] U. Urooj, M. A. B. Maarof and B. A. S. Al-rimy, "A proposed Adaptive Pre-Encryption Crypto-Ransomware Early Detection Model," 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 2021, pp. 1-6, doi: 10.1109/CRC50527.2021.9392548.

[12] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, “Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions,” Comput. Secur., vol. 74, pp. 144–166, May 2018, doi: 10.1016/j.cose.2018.01.001.

[13] Hassan, M. F., Akbar, R., Savita, K. S., Ullah, R., & Mandala, S. (2024). Ransomware Classification with Deep Neural Network and Bi-LSTM. Journal of Advanced Research in Applied Sciences and Engineering Technology, 47(2), 266-280.

[14] A. Moser et al., “Cyber security threats and mitigation techniques for multifunctional devices,” Comput. Secur., vol. 10, no. 1, pp. 1–6, Dec. 2022, doi: 10.1109/ICTAS.2018.8368745.

[15] B. A. S. Al-rimy et al., “Redundancy Coefficient Gradual Up-weighting-based Mutual Information Feature Selection technique for Crypto-ransomware early detection,” Futur. Gener. Comput. Syst., vol. 115, pp. 641–658, 2021, doi: 10.1016/j.future.2020.10.002.

[16] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, “Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection,” Futur. Gener. Comput. Syst., vol. 101, pp. 476–491, Dec. 2019, doi: 10.1016/j.future.2019.06.005.

[17] C. Moore, "Detecting Ransomware with Honeypot Techniques," 2016 Cybersecurity and Cyberforensics Conference (CCC), Amman, Jordan, 2016, pp. 77-81, doi: 10.1109/CCC.2016.14.

[18] S. R. Davies, R. Macfarlane, and W. J. Buchanan, “Differential area analysis for ransomware attack detection within mixed file datasets,” Comput. Secur., vol. 108, p. 102377, 2021, doi: 10.1016/j.cose.2021.102377.

[19] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, “Prevention of crypto-ransomware using a pre-encryption detection algorithm,” Computers, vol. 8, no. 4, pp. 1–15, 2019, doi: 10.3390/computers8040079.

[20] O. Aslan and R. Samet, “A Comprehensive Review on Malware Detection Approaches,” IEEE Access, vol. 8, no. March 2021, pp. 6249–6271, 2020, doi: 10.1109/ACCESS.2019.2963724.

[21] M. E. Ahmed, H. Kim, S. Camtepe, and S. Nepal, “Peeler: Profiling Kernel-Level Events to Detect Ransomware,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 12972 LNCS, pp. 240–260, 2021, doi: 10.1007/978-3-030-88418-5_12.

[22] V. Madhushalini and L. Raja, “A Novel Ransomware Virus Detection Technique using Machine and Deep Learning Methods,” pp. 8–14, 2023, doi: 10.1109/ICICCS56967.2023.10142938.

[23] K. Begovic, A. Al-ali, and Q. Malluhi, “Cryptographic Ransomware Encryption Detection : Survey,” Comput. Secur., vol. 132, no. February 2022, p. 103349, 2023, doi: 10.1016/j.cose.2023.103349.

[24] V. A. Popescu, G. N. Popescu, and C. R. Popescu, “The relation productivity – Environment in the context of sustainable development–Case study on the Romanian industry,” Metalurgija, vol. 54, no. 1, pp. 286–288, 2015.

[25] G. Cusack, O. Michel, and E. Keller, “Machine learning-based detection of ransomware using SDN,” SDN-NFVSec 2018 - Proc. 2018 ACM Int. Work. Secur. Softw. Defin. Networks Netw. Funct. Virtualization, Co-located with CODASPY 2018, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1145/3180465.3180467.

[26] B. A. S. Al-Rimy et al., “A Pseudo Feedback-Based Annotated TF-IDF Technique for Dynamic Crypto-Ransomware Pre-Encryption Boundary Delineation and Features Extraction,” IEEE Access, vol. 8, pp. 140586–140598, 2020, doi: 10.1109/ACCESS.2020.3012674.

[27] L. J. García Villalba, A. L. Sandoval Orozco, A. López Vivar, E. A. Armas Vega, and T. H. Kim, “Ransomware Automatic Data Acquisition Tool,” IEEE Access, vol. 6, pp. 55043–55051, 2018, doi: 10.1109/ACCESS.2018.2868885.

[28] R. Moussaileb, N. Cuppens, J. L. Lanet, and H. Le Bouder, “A Survey on Windows-based Ransomware Taxonomy and Detection Mechanisms: Case Closed?,” ACM Comput. Surv., vol. 54, no. 6, 2021, doi: 10.1145/3453153.

[29] E. Berrueta, D. Morato, E. Magana, and M. Izal, “A Survey on Detection Techniques for Cryptographic Ransomware,” IEEE Access, vol. 7, pp. 144925–144944, 2019, doi: 10.1109/ACCESS.2019.2945839.

[30] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, “A 0-day aware crypto-ransomware early behavioral detection framework,” Lect. Notes Data Eng. Commun. Technol., vol. 5, pp. 758–766, 2018, doi: 10.1007/978-3-319-59427-9_78.

[31] Monika, P. Zavarsky, and D. Lindskog, “Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization,” Procedia Comput. Sci., vol. 94, pp. 465–472, 2016, doi: 10.1016/j.procs.2016.08.072.

[32] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, “Cybersecurity data science: an overview from machine learning perspective,” J. Big Data, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00318-5.

[33] B. A. S. Al-Rimy, M. A. Maarof, Y. A. Prasetyo, S. Z. M. Shaid, and A. F. M. Ariffin, “Zero-day aware decision fusion-based model for crypto-ransomware early detection,” Int. J. Integr. Eng., vol. 10, no. 6, pp. 82–88, 2018, doi: 10.30880/ijie.2018.10.06.011.

[34] A. I. M. Detection et al., “A proposed Adaptive Pre-Encryption Crypto-Ransomware Early Detection Model,” IEEE Access, vol. 10, no. 1, pp. 3–8, Jan. 2023, doi: 10.1109/CRC50527.2021.9392548.

[35] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, “Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement.,” Ann. Intern. Med., vol. 151, no. 4, pp. 264–9, W64, Aug. 2009, doi: 10.7326/0003-4819-151-4-200908180-00135.

[36] K. Adnan, R. Akbar, and K. S. Wang, “Development of Usability Enhancement Model for Unstructured Big Data Using SLR,” IEEE Access, vol. 9, pp. 87391–87409, 2021, doi: 10.1109/ACCESS.2021.3089100.

[37] N. Ariffin, A. Zainal, M. A. Maarof and M. Nizam Kassim, "A Conceptual Scheme for Ransomware Background Knowledge Construction," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-4, doi: 10.1109/CR.2018.8626868.

[38] B. Celiktas and E. Karacuha, “Ransomware , Detection and Prevention Techniques , Cyber Security , Malware Analysis Istanbul Technical University Informatics Institute Using Signature and Anomaly Based Detection Methods Barış Çeliktaş Department of Applied Informatics Applied Informa,” no. July, 2018.

[39] S. Alsoghyer and I. Almomani, “Ransomware detection system for android applications,” Electron., vol. 8, no. 8, pp. 1–36, 2019, doi: 10.3390/electronics8080868.

[40] E. G. Dada, J. Stephen Bassi, Y. J. Hurcha, and A. H. Alkali, “Performance Evaluation of Machine Learning Algorithms for Detection and Prevention of Malware Attacks Related papers Performance Evaluation of Machine Learning Algorithms for Detection and Prevention of Malware Attacks,” vol. 21, no. 3, pp. 18–27, 2019, doi: 10.9790/0661-2103011827.

[41] H. Aghakhani et al., “When Malware is Packin’ Heat; Limits of Machine Learning Classifiers Based on Static Analysis Features,” no. February, 2020, doi: 10.14722/ndss.2020.24310.

[42] D. W. Fernando, N. Komninos, and T. Chen, “A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques,” IoT, vol. 1, no. 2, pp. 551–604, Dec. 2020, doi: 10.3390/iot1020030.

[43] M. Almousa, S. Basavaraju, and M. Anwar, “API-Based Ransomware Detection Using Machine Learning-Based Threat Detection Models,” in 2021 18th International Conference on Privacy, Security and Trust, PST 2021, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/PST52912.2021.9647816. 13-15 December 2021 at Auckland, New Zealand

[44] M. Rhode, P. Burnap, and A. Wedgbury, “Real-Time Malware Process Detection and Automated Process Killing,” Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/8933681.

[45] M. Almousa, J. Osawere and M. Anwar, "Identification of Ransomware families by Analyzing Network Traffic Using Machine Learning Techniques," 2021 Third International Conference on Transdisciplinary AI (TransAI), Laguna Hills, CA, USA, 2021, pp. 19-24, doi: 10.1109/TransAI51903.2021.00012.

[46] Y. A. Ahmed et al., “A Weighted Minimum Redundancy Maximum Relevance Technique for Ransomware Early Detection in Industrial IoT,” Sustain., vol. 14, no. 3, pp. 1–16, 2022, doi: 10.3390/su14031231.

[47] A. Singh, R. Ikuesan, and H. Venter, “Ransomware Detection using Process Memory,”. 17th International Conference on Cyber Warfare and Security (ICCWS 2022), hosted State University of New York at Albany, USA on 17-18 March 2022. doi: 10.34190/iccws.17.1.53

[48] R. M. A. Molina, S. Torabi, K. Sarieddine, E. Bou-Harb, N. Bouguila, and C. Assi, “On Ransomware Family Attribution Using Pre-Attack Paranoia Activities,” IEEE Trans. Netw. Serv. Manag., vol. 19, no. 1, pp. 19–36, 2022, doi: 10.1109/TNSM.2021.3112056.

[49] S. Mehnaz, A. Mudgerikar, and E. Bertino, RWGuard: A real-time detection system against cryptographic ransomware, vol. 11050 LNCS,

no. March 2019. Springer International Publishing, 2018. doi: 10.1007/978-3-030-00470-5_6.

[50] H. Zhang, X. Xiao, F. Mercaldo, S. Ni, F. Martinelli, and A. K. Sangaiah, “Classification of ransomware families with machine learning based on N-gram of opcodes,” Futur. Gener. Comput. Syst., vol. 90, pp. 211–221, 2019, doi: 10.1016/j.future.2018.07.052.

[51] 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 Syst. Appl., vol. 209, Dec. 2022, doi: 10.1016/j.eswa.2022.118299.

[52] A. Azmoodeh, A. Dehghantanha, M. Conti, and K.-K. K. R. Choo, “Detecting crypto-ransomware in IoT networks based on energy consumption footprint,” J. Ambient Intell. Humaniz. Comput., vol. 9, no. 4, pp. 1141–1152, 2018, doi: 10.1007/s12652-017-0558-5.

[53] R. Agrawal, J. W. Stokes, K. Selvaraj, and M. Marinescu, “University of California , Santa Cruz , Santa Cruz , CA 95064 USA Microsoft Corp ., One Microsoft Way , Redmond , WA 98052 USA,” pp. 3222–3226, 2019.

[54] S. Poudyal and Di. Dasgupta, “Analysis of Crypto-Ransomware Using ML-Based Multi-Level Profiling,” IEEE Access, vol. 9, pp. 122532–122547, 2021, doi: 10.1109/ACCESS.2021.3109260.

[55] B. M. Khammas, “Ransomware Detection using Random Forest Technique,” ICT Express, vol. 6, no. 4, pp. 325–331, Dec. 2020, doi: 10.1016/j.icte.2020.11.001.

[56] R. Moussaileb, N. Cuppens, J. L. Lanet, and H. Le Bouder, “Ransomware Network Traffic Analysis for Pre-encryption Alert,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 12056 LNCS, pp. 20–38, 2020, doi: 10.1007/978-3-030-45371-8_2.

[57] A. Singh, A. Ikuesan, and H. Venter, “A context-aware trigger mechanism for ransomware forensics,” 14th Int. Conf. Cyber Warf. Secur. ICCWS 2019, Feb 28- Mar 1, 2019 at Stellenbosch, South Africa pp. 629–638, 2019.

[58] K. Cabaj, M. Gregorczyk, and W. Mazurczyk, “Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics,” Comput. Electr. Eng., vol. 66, no. November 2016, pp. 353–368, 2018, doi: 10.1016/j.compeleceng.2017.10.012.

[59] D. Morato, E. Berrueta, E. Magaña, and M. Izal, “Ransomware early detection by the analysis of file sharing traffic,” J. Netw. Comput. Appl., vol. 124, no. September, pp. 14–32, 2018, doi: 10.1016/j.jnca.2018.09.013.

[60] S. Wang et al., “KRProtector: Detection and Files Protection for IoT Devices on Android Without ROOT Against Ransomware Based on Decoys,” IEEE Internet Things J., vol. 9, no. 19, pp. 18251–18266, 2022, doi: 10.1109/JIOT.2022.3156571.

[61] K. P. Subedi, D. R. Budhathoki, and D. Dasgupta, “Forensic analysis of ransomware families using static and dynamic analysis,” Proc. - 2018 IEEE Symp. Secur. Priv. Work. SPW 2018, pp. 180–185, 2018, doi: 10.1109/SPW.2018.00033.

[62] S. Sharmeen, Y. A. Ahmed, S. Huda, B. S. Kocer, and M. M. Hassan, “Avoiding Future Digital Extortion through Robust Protection against Ransomware Threats Using Deep Learning Based Adaptive Approaches,” IEEE Access, vol. 8, pp. 24522–24534, 2020, doi: 10.1109/ACCESS.2020.2970466.

[63] S. Maniath, A. Ashok, P. Poornachandran, V. G. Sujadevi, A. U. P. Sankar, and S. Jan, “Deep learning LSTM based ransomware detection,” 2017 Recent Dev. Control. Autom. Power Eng. RDCAPE 2017, vol. 3, pp. 442–446, 2018, doi: 10.1109/RDCAPE.2017.8358312.

[64] V. R., M. Alazab, A. Jolfaei, S. K.P. and P. Poornachandran, "Ransomware Triage Using Deep Learning: Twitter as a Case Study," 2019 Cybersecurity and Cyberforensics Conference (CCC), Melbourne, VIC, Australia, 2019, pp. 67-73, doi: 10.1109/CCC.2019.000-7.,

[65] S. Homayoun et al., “DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer,” Futur. Gener. Comput. Syst., vol. 90, pp. 94–104, 2019, doi: 10.1016/j.future.2018.07.045.

[66] S. Usharani, P. M. Bala, and M. M. J. Mary, “Dynamic analysis on crypto-ransomware by using machine learning: Gandcrab ransomware,” J. Phys. Conf. Ser., vol. 1717, no. 1, 2021, doi: 10.1088/1742-6596/1717/1/012024.

[67] S. Song, B. Kim, and S. Lee, “The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform,” Mob. Inf. Syst., vol. 2016, 2016, doi: 10.1155/2016/2946735.

[68] J. K. Lee, S. Y. Moon, and J. H. Park, “CloudRPS: a cloud analysis based enhanced ransomware prevention system,” J. Supercomput., vol. 73, no. 7, pp. 3065–3084, 2017, doi: 10.1007/s11227-016-1825-5.

[69] A. Wani and S. Revathi, “Ransomware protection in loT using software defined networking,” Int. J. Electr. Comput. Eng., vol. 10, no. 3, pp. 3166–3174, 2020, doi: 10.11591/ijece.v10i3.pp3166-3175.

[70] S. K. Shaukat and V. J. Ribeiro, "RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning," 2018 10th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 2018, pp. 356-363, doi: 10.1109/COMSNETS.2018.8328219.

[71] A. Kharraz and E. Kirda, “Redemption: Real-Time Protection Against Ransomware at End-Hosts BT - Recent Advances in Intrusion Detection,” Recent Adv. Intrusion Detect., vol. 10453, no. Chapter 5, pp. 98–119, 2017, [Online]. Available: http://link.springer.com/10.1007/978-3-319-66332-6_5%0Apapers3://publication/doi/10.1007/978-3-319-66332-6_5

[72] J. Zhang et al., "Scarecrow: Deactivating Evasive Malware via Its Own Evasive Logic," 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Valencia, Spain, 2020, pp. 76-87, doi: 10.1109/DSN48063.2020.00027.

[73] S. Lee, H. K. Kim, and K. Kim, “Ransomware protection using the moving target defense perspective,” Comput. Electr. Eng., vol. 78, pp. 288–299, 2019, doi: 10.1016/j.compeleceng.2019.07.014.

[74] K. Cabaj and W. Mazurczyk, “Using software-defined networking for ransomware mitigation: The case of cryptowall,” IEEE Netw., vol. 30, no. 6, pp. 14–20, 2016, doi: 10.1109/MNET.2016.1600110NM.

[75] Eugene Kolodenker, William Koch, Gianluca Stringhini, and Manuel Egele. 2017. PayBreak: Defense Against Cryptographic Ransomware. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17). Association for Computing Machinery, New York, NY, USA, 599–611. https://doi.org/10.1145/3052973.3053035

[76] J. S. Aidan, Zeenia and U. Garg, "Advanced Petya Ransomware and Mitigation Strategies," 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 2018, pp. 23-28, doi: 10.1109/ICSCCC.2018.8703323.

[77] E. Rouka, C. Birkinshaw and V. G. Vassilakis, "SDN-based Malware Detection and Mitigation: The Case of ExPetr Ransomware," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2020, pp. 150-155, doi: 10.1109/ICIoT48696.2020.9089514.

[78] Marco Antonio Sotelo Monge, Jorge Maestre Vidal, and Luis Javier García Villalba. 2018. A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation. In Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES '18). Association for Computing Machinery, New York, NY, USA, Article 48, 1–10. https://doi.org/10.1145/3230833.3233249

[79] S. R. Davies, R. Macfarlane, and W. J. Buchanan, “Evaluation of live forensic techniques in ransomware attack mitigation,” Forensic Sci. Int. Digit. Investig., vol. 33, 2020, doi: 10.1016/j.fsidi.2020.300979.

[80] R. Umar, I. Riadi, and R. S. Kusuma, “Mitigating sodinokibi ransomware attack on cloud network using software-defined networking (SDN),” Int. J. Saf. Secur. Eng., vol. 11, no. 3, pp. 239–246, 2021, doi: 10.18280/ijsse.110304.

[81] V. Mathane and P. V. Lakshmi, “Predictive Analysis of Ransomware Attacks using Context-aware AI in IoT Systems,” Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 4, pp. 240–244, 2021, doi: 10.14569/IJACSA.2021.0120432.

[82] C. G. Akcora, Y. Li, Y. R. Gel, and M. Kantarcioglu, “Bitcoin heist: Topological data analysis for ransomware prediction on the bitcoin blockchain,” 17th Pacific Rim International Conference on Artificial Intelligence!IJCAI-PRICAI2020 7-15-2021 Yokohama, Japan,

[83] M. Rhode, P. Burnap, and K. Jones, “Early-stage malware prediction using recurrent neural networks,” Comput. Secur., vol. 77, no. December 2017, pp. 578–594, 2018, doi: 10.1016/j.cose.2018.05.010.

[84] Shengyun Xu. 2021. The Application of Machine Learning in Bitcoin Ransomware Family Prediction. In Proceedings of the 2021 5th International Conference on Information System and Data Mining (ICISDM '21). Association for Computing Machinery, New York, NY, USA, 21–27. https://doi.org/10.1145/3471287.3471300

[85] H. Y. Chang, T. L. Lin, T. F. Hsu, Y. S. Shen, and G. R. Li, “Implementation of ransomware prediction system based on weighted-KNN and real-time isolation architecture on SDN Networks,” 2019 IEEE Int. Conf. Consum. Electron. - Taiwan, ICCE-TW 2019, pp. 4–5, 2019, doi: 10.1109/ICCE-TW46550.2019.8991771.

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

[87] W. Song et al., “Crypto-ransomware Detection through Quantitative API-based Behavioral Profiling,” 2023, [Online]. Available: http://arxiv.org/abs/2306.02270

[88] J. Modi and B. Eng, “Detecting Ransomware in Encrypted Network Traffic Using Machine Learning,” 2019, [Online]. Available: https://dspace.library.uvic.ca/handle/1828/11076

[89] R. Brewer, “Ransomware attacks: detection, prevention and cure,” Netw. Secur., vol. 2016, no. 9, pp. 5–9, 2016, doi: 10.1016/S1353-4858(16)30086-1.

[90] A. Djenna, A. Bouridane, S. Rubab, and I. M. Marou, “Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation,” Symmetry (Basel)., vol. 15, no. 3, pp. 1–24, 2023, doi: 10.3390/sym15030677.

[91] H. S. Talabani and H. M. T. Abdulhadi, “Bitcoin Ransomware Detection Employing Rule-Based Algorithms,” Sci. J. Univ. Zakho, vol. 10, no. 1, pp. 5–10, 2022, doi: 10.25271/sjuoz.2022.10.1.865.

[92] S. H. Kok, A. Azween, and N. Z. Jhanjhi, “Evaluation metric for crypto-ransomware detection using machine learning,” J. Inf. Secur. Appl., vol. 55, p. 102646, 2020, doi: 10.1016/j.jisa.2020.102646.

[93] R. S. Rahul, “Malware analysis detection,” Iconic Res. Eng. Journals, vol. 1, no. 10, pp. 132–135, 2018, [Online]. Available: http://irejournals.com/formatedpaper/1700619.pd

[94] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, “Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection,” no. September, 2016, [Online]. Available: http://arxiv.org/abs/1609.03020

[95] Rehman, M. U., Akbar, R., Omar, M., & Gilal, A. R. (2023, September). A Systematic Literature Review of Ransomware Detection Methods and Tools for Mitigating Potential Attacks. In International Conference on Computing and Informatics (pp. 80-95). Singapore: Springer Nature Singapore.

[96] Shaikh, M. R., Ullah, R., Akbar, R., Savita, K. S., & Mandala, S. (2024). Fortifying Against Ransomware: Navigating Cybersecurity Risk Management with a Focus on Ransomware Insurance Strategies. Int. J. Acad. Res. Bus. Soc. Sci, 14(1), 1415-1430.

[97] Sathio, A. A., Dootio, M. A., Lakhan, A., ur Rehman, M., Pnhwar, A. O., & Sahito, M. A. (2021, August). Pervasive futuristic healthcare and blockchain enabled digital identities-challenges and future intensions. In 2021 International Conference on Computing, Electronics & Communications Engineering (iCCECE) (pp. 30-35). IEEE.

[98] Yalli, J. S., Hasan, M. H., Haron, N. S., Rehman Shaikh, M. U., Murad, N. Y., & Bako, A. L. (2023). Quality of Data (QoD) in Internet of Things (IOT): An Overview, State-of-the-Art, Taxonomy and Future Directions. International Journal of Advanced Computer Science & Applications, 14(12).

[99] Mujeeb-ur-Rehman, A. L., Hussain, Z., Khoso, F. H., & Arain, A. A. (2021). Cyber security intelligence and ethereum blockchain technology for e-commerce. International Journal, 9(7).

[100] Ur Rehman, M., Akbar, R., Mujeeb, S., & Janisar, A. A. Deep-learning enabled early detection of COVID-19 infection in IoMT fog-cloud healthcare in LPWAN. In Low-Power Wide Area Network for Large Scale Internet of Things (pp. 235-258). CRC Press

[101] Panhwar, A. O., Sathio, A. A., Lakhan, A., Umer, M., Mithiani, R. M., & Khan, S. (2022). Plant health detection enabled CNN scheme in IoT network. International Journal of Computing and Digital Systems, 11(1), 344-335.

[102] Sahito, M. A., & Kehar, A. (2021). Dynamic content enabled microservice for business applications in distributed cloudlet cloud network. International Journal, 9(7), 1035-1039

[103] Chandio, S. A., & Mahar, J. A. (2017, April). Gadget improved security alert monitoring, management and mitigation system to control the crowded occasions. In 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT) (pp. 1-3). IEEE.