big data and cognitive computing

IMPACT FACTOR 3.7

CITESCORE 4.9

Review

Ransomware Detection Using Machine Learning: A Survey

Amjad Alraizza and Abdulmohsen Algarni

Special Issue

Managing Cybersecurity Threats and Increasing Organizational Resilience

Edited by

Dr. Peter R.J. Trim and Dr. Yang-Im Lee

MDPI

https://doi.org/10.3390/bdcc7030143

big data and cognitive computing

MDPI

Review

Ransomware Detection Using Machine Learning: A Survey

Amjad Alraizza [1,*] and Abdulmohsen Algarni [2]

[1] Department of Information Systems, King Khalid University, Alfara, Abha 61421, Saudi Arabia
[2] Department of Computer Science, King Khalid University, Alfara, Abha 61421, Saudi Arabia; a.algarni@kku.edu.sa
* Correspondence: 444800503@kku.edu.sa

Abstract: Ransomware attacks pose significant security threats to personal and corporate data and information. The owners of computer-based resources suffer from verification and privacy violations, monetary losses, and reputational damage due to successful ransomware assaults. As a result, it is critical to accurately and swiftly identify ransomware. Numerous methods have been proposed for identifying ransomware, each with its own advantages and disadvantages. The main objective of this research is to discuss current trends in and potential future debates on automated ransomware detection. This document includes an overview of ransomware, a timeline of assaults, and details on their background. It also provides comprehensive research on existing methods for identifying, avoiding, minimizing, and recovering from ransomware attacks. An analysis of studies between 2017 and 2022 is another advantage of this research. This provides readers with up-to-date knowledge of the most recent developments in ransomware detection and highlights advancements in methods for combating ransomware attacks. In conclusion, this research highlights unanswered concerns and potential research challenges in ransomware detection.

Keywords: machine learning; ransomware techniques; cybersecurity; ransomware detection; ransomware attacks

Citation: Alraizza, A.; Algarni, A. Ransomware Detection Using Machine Learning: A Survey. *Big Data Cogn. Comput.* **2023**, *7*, 143. https://doi.org/10.3390/bdcc7030143

Academic Editors: Peter R.J. Trim, Yang-Im Lee and Min Chen

Received: 18 May 2023
Revised: 7 August 2023
Accepted: 11 August 2023
Published: 16 August 2023

1. Introduction

The rapid proliferation of ransomware attacks has emerged as one of the most significant cybersecurity threats facing organizations today. In recent years, ransomware has become an increasingly popular tool with which cybercriminals extort money from victims by encrypting their data and demanding payment for a decryption key. The impact of ransomware attacks has been felt across all industries, from healthcare and finance to government and education. Given the high stakes involved, it is crucial to understand the nature of ransomware attacks, how they spread, and the potential consequences of falling victim to one [1]. The importance of research in this area cannot be overstated. With the threat of ransomware attacks continuing to grow, there is a pressing need for scholars and practitioners to delve deeper into the problem and identify effective strategies for prevention and mitigation. This paper aims to contribute to this effort by providing a comprehensive overview of the ransomware threat landscape, analyzing the factors that contribute to the spread of ransomware, and exploring potential avenues for future research. By shedding light on this critical issue, we hope to help individuals and organizations better-protect themselves against ransomware attacks and mitigate the potential damage caused by these malicious programs [1].

This paper is organized as follows: Section 2 introduces the concept of ransomware and how it works. It also discusses the different types of ransomware attacks, such as encrypting ransomware, locker ransomware, and scareware. Section 3 describes the methodology used for this paper. Section 4 provides studies of machine-learning-based ransomware-detection systems developed by researchers. It discusses the methodology used, the performance

achieved, and the limitations of each system. It also discusses the challenges of collecting and preprocessing data for ransomware detection using machine learning. Section 5 provides an in-depth analysis of the evolution of ransomware over the last twelve years. Section 6 provides an overview of the existing ransomware detection techniques, including signature-based detection, behavior-based detection, and machine-learning-based detection. Furthermore, it discusses the different evaluation metrics used for measuring the performance of machine learning models for ransomware detection. It also focuses on the use of machine learning techniques for ransomware detection. It discusses the different machine learning algorithms used for this purpose, such as decision trees, random forests, support vector machines, and neural networks. It also addresses the different features used for ransomware detection using machine learning and covers the techniques used for feature selection. Section 7 discusses the challenges of developing effective machine-learning-based ransomware-detection systems. It also highlights future directions in this field, such as developing more robust and accurate models, incorporating real-time detection capabilities, and addressing the issue of adversarial attacks. Section 8 concludes what has been achieved in this research. This research offers a valuable resource for researchers and practitioners interested in developing effective ransomware-detection systems using machine-learning techniques.

2. Background

Ransomware encrypts information or computer systems and prevents unauthorized users from accessing them. Ransomware attacks use tactics, techniques, and procedures that can lock computers or encrypt data and are challenging for a computer professional to undo. They might also steal private information from victims' PCs and network systems. Individual PCs, commercial systems (and the data and software they contain), and industrial control systems are all potential targets for ransomware attacks. Additionally, we emphasize the variety of sensors that Internet of Things (IoT) users employ [1]. A ransomware attack employs private key encryption to prevent authorized users from accessing a system or data unless they pay a ransom (cash), typically in Bitcoin [2]. Ransomware operations may include data exfiltration techniques. Hackers steal private information from vulnerable networks and threaten to release it if the owner does not pay a ransom. The infection is disseminated through malicious advertising, email attachments, and connections to rogue websites. The attacker also sends a file (or files) with instructions for paying the ransom. Once the attacker has verified that the ransom has been paid, the victim can access the decryption key [3]. Files with encryption or ransomware infections frequently include extensions, such as Locky, Cryptolocker, Vault, Micro, Encrypted, TTTT, XYZ, ZZZ, Petya, etc. Each file's extension indicates the type of ransomware that affected it. Examples of ransomware include WannaCry, WannaCry.F, Fusob, TorrentLocker, CryptoWall, CryptoTear, and Reveton [4]. Figure 1 illustrates the classification of ransomware into three categories: scareware, locker ransomware, and crypto-ransomware [2,4].

Crypto is the most prevalent ransomware that targets computer systems and networks. Ransomware encrypts files and data using symmetric and asymmetric encryption algorithms. Even if the malicious software is removed from an infected computer or a compromised storage device is introduced into another system, crypto-ransomware renders the encrypted data unusable. Because the malware frequently does not corrupt imported essential data, the compromised device can still be used to pay the ransom [4]. Figure 2 provides a visual representation of crypto-ransomware, a form of malicious software that is becoming increasingly prevalent in cyberattacks [4].

However, by locking a computer or other device and demanding money, locker ransomware prevents its owner from using it. The workstation is affected by the locker ransomware, but saved data are not rendered inaccessible. Once the malicious program has been eliminated, the data are not altered. The data are often recoverable by connecting the infected storage device, such as a hard drive, to another machine. Individuals wanting to extort money from assault victims will not be drawn to locker ransomware. Figure 3

provides a visual representation of locker ransomware, a form of malicious software that is becoming increasingly prevalent in cyberattacks [4].

Figure 1. Types of ransomware [2,4].

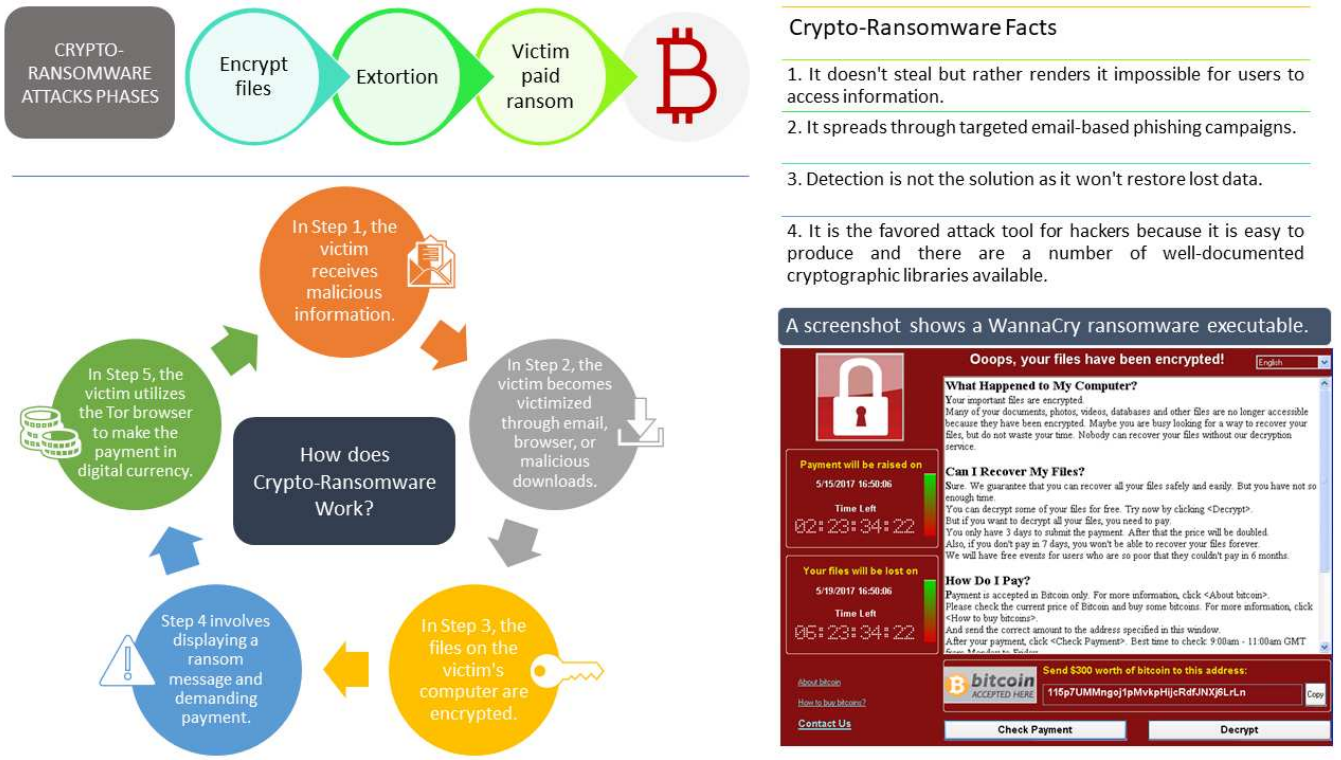


Figure 2. Crypto-ransomware [4].

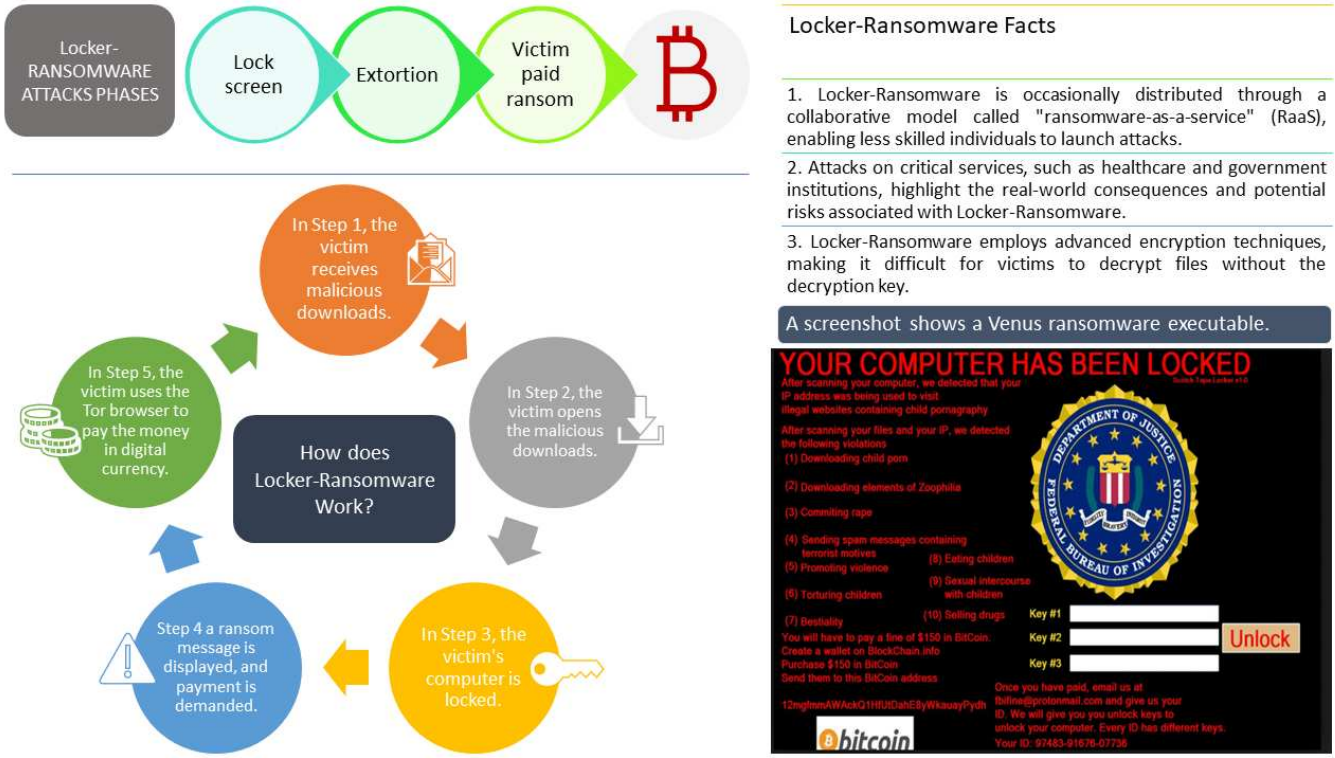


Figure 3. Locker ransomware [4].

Scareware preys on its victims by informing them that their machines have been hijacked and promising to eradicate the ransomware using a false antivirus program backed by the attacker. Numerous innocent consumers buy and install fake antivirus software due to scareware alerts' frequent appearance [5]. Human-operated malware and ransomware without data are different from ransomware. Cybercriminals also employ human-operated ransomware to break into networks or cloud infrastructure, carry out privilege escalation, and launch attacks on sensitive data. Instead of simply one system, the attack actively targets an entire organization. Attackers typically access a whole IT system, move laterally, and exploit flaws via improper security configurations. Ultimately, unauthorized access to privileged user credentials leads to ransomware assaults on IT systems that enable crucial corporate activities [3,4]. Figure 4 provides a visual representation of scareware, a form of malicious software that is becoming increasingly prevalent in cyberattacks [4].

However, ransomware without files uses a native and reliable system to launch attacks. It is difficult to identify the attack because no code needs to be placed on the victim's machine for it to work. As a result, anti-ransomware technologies do not find any suspicious files to trace during an attack. Depending on the attacker's intentions, file-based and human-operated ransomware can encrypt, lock, or leak data from files [2]. Ransomware poses a danger to businesses' technology and files. Until the ransom is paid, typically with Bitcoin, infected files or compromised devices are locked out of reach. The decryption key is frequently withheld even after a victim pays the ransom the hackers want. They periodically try to use the attacker's key to decrypt the data, which damages the system's stored files. Technology advancements such as ransomware development kits, ransomware-as-a-service, and bitcoins are to blame for the ongoing rise in ransomware attacks on desktop PCs, networks, and mobile devices [2]. Attacks using ransomware cost businesses and individuals hundreds of millions yearly [3]. New types of malware are continually being created thanks to the enormous cash benefits that hackers gain from ransomware assaults. Since 2013, numerous ransomware variants have appeared. Therefore, new, effective, and reliable techniques are needed to detect, prevent, and mitigate ransomware attacks. Different ransomware strains cannot be created using conventional

antivirus software or other intrusion-detection systems. People and companies experience significant financial losses as a result of ransomware attacks. The encryption of files or devices until a ransom is paid can result in the permanent loss of important data, which can have severe consequences for individuals and businesses alike. Even after the ransom is paid, the decryption key is often withheld, causing additional damage to the system's stored files when attackers attempt to decrypt the data [1,6].

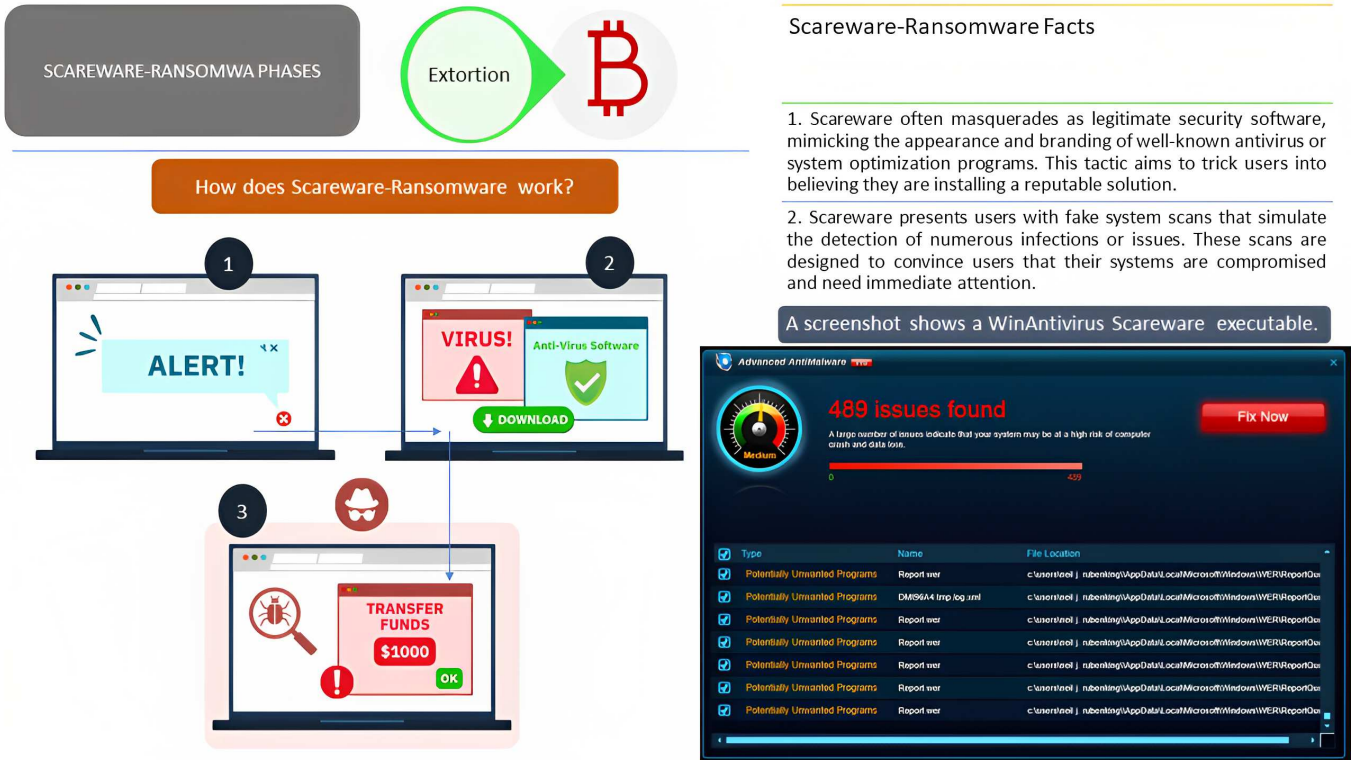


Figure 4. Scareware ransomware [4].

3. Survey Planning

The present research involved several phases to achieve its overall objectives, including data collection and information gathering, data extraction and analysis, information synthesis, and reporting. A visual representation of the research process flow is presented in Figure 5, which depicts the activities involved in each phase and their interrelation.

The data collection process was carried out by selecting relevant and up-to-date journal and conference papers from reputable databases such as IEEE, Springer, MDPI, Elsevier, IET, and Archive.org, as well as other sources including university-based journals, theses/dissertations, and blogs published by reputable organizations such as Microsoft, Crowdstrike, Symantec, and Techspot. The collected materials were then categorized into two main groups: non-technical sources and technical sources. Non-technical sources contained general information on ransomware and were used to provide reliable information while writing the introduction and detailing the history of ransomware/chronology of attacks. Technical papers proposing solutions for ransomware attacks were divided into detection groups based on the nature and purpose of the proposed solution. Papers focusing on detection were further sub-categorized into artificial-intelligence-based methods and non-AI-based approaches. AI-based approaches were classified into machine learning methods, deep learning approaches, and artificial neural network approaches, while non-AI-based papers were grouped into packet and traffic analysis categories. The data extraction phase involved a detailed analysis and summary of each technical paper by identifying the problem it addressed, its objectives, the method/technique used, the achievements of the paper in terms of results obtained, and the research's limitations. Information synthesis

was applied to identify similarities or relationships among papers in each group and to determine if and how the research improved upon or addressed the limitations of another work. The reporting phase placed papers that addressed similar problems or used similar techniques in the same group and presented their reviews in the same paragraph. This approach provided a good flow of communication and enhanced the readability of the paper, while also providing readers with a clear understanding of the concepts discussed in the research.

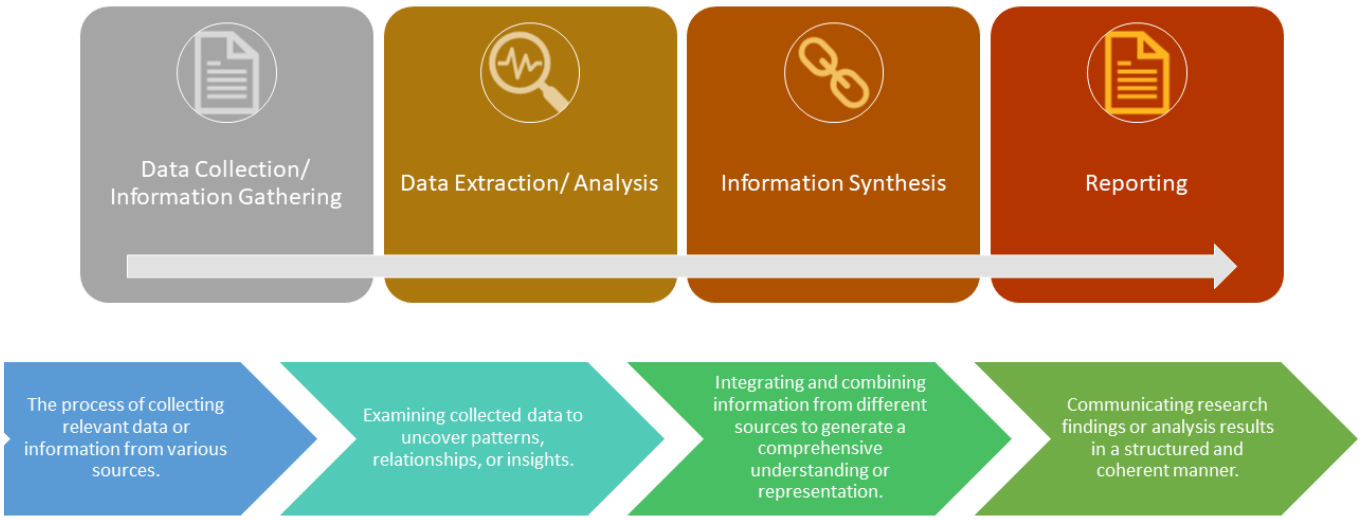


Figure 5. Research process flow.

4. Literature Review

Preventing ransomware is challenging for several reasons. The way ransomware functions is the same as benign software, which acts covertly. Ransomware detection in zero-day assaults is, therefore, crucial at this time. The primary objectives are to avoid ransomware-caused system damage, identify zero-day (previously unidentified) malware, and minimize detection, which means reducing the number of false positives while still detecting all instances of ransomware. False positives are instances where the system flags a harmless program or file as ransomware, leading to unnecessary alerts and actions. Ransomware can be found using a variety of tools and methodologies. Methods based on static analysis decompose source code without running it. They generate many false positives and cannot find ransomware that is disguised. Attackers frequently create new variations and modify their codes using various packaging techniques. To solve these issues, researchers use dynamic behavior analysis methods that monitor interactions between the executed code and a virtual environment. However, these detection methods are cumbersome and memory-intensive. Machine learning is ideal for analyzing any process or application's behavior.

Machine learning is considered ideal for analyzing the behavior of processes or applications because it can effectively learn patterns and anomalies in large datasets, which can be difficult for humans to detect. In the context of ransomware detection, machine learning algorithms can be trained on large datasets of both benign and malicious software to learn the behavioral characteristics that distinguish ransomware from legitimate software. This training can be used to identify new and previously unseen variants of ransomware, including zero-day attacks, based on their behavioral patterns.

Moreover, machine learning can be used to continuously learn and adapt to new threats, making it an effective approach to keep up with the constantly evolving tactics of ransomware attackers. Machine learning can also reduce false positives by accurately distinguishing between benign software and ransomware based on their behavioral patterns.

Compared with traditional signature-based detection and static analysis methods, machine learning is considered ideal because it can provide a more comprehensive and

accurate analysis of the behavior of software, making it a powerful tool for ransomware detection. However, it is important to note that machine learning models need to be properly trained and validated to ensure their effectiveness and avoid biases or errors. The following are some machine-learning-based detection systems that follow highly traditional methodologies.

Table 1 summarizes previous studies on machine learning techniques (behavioral techniques) for ransomware detection from 2017 to 2022.

Table 1. Studies on machine learning techniques (behavioral techniques) for ransomware detection from 2017 to 2022.

Reference	Year	Author	Resolved the Issue	Utilized Technique	Result	Limitation
[7]	2017	Zahra and Sha	Detecting a ransomware attack using Cryptowall.	Blocklisting of command-and-control (C&C) servers.	The web proxy server, which acts as the TCP/IP traffic gateway, extracts the TCP/IP header.	The model's efficacy and precision in identifying ransomware and its attack techniques against various operating system environments were not demonstrated through implementation.
[8]	2018	Shaukat and Ribeiro	Detection of ransomware.	RansomWall, a layered and hybrid mechanism.	Effective at identifying zero-day attacks.	N/A
[9]	2019	Makinde et al.	To determine whether an actual network system is vulnerable to a ransomware assault.	Learning machines.	Correlation greater than 0.8.	It imitated the behavior of a small group of users.
[10]	2019	Ahmad et al.	Differentiating Locky ransomware users.	Utilizing parallel classifiers, a behavioral approach to ransomware detection.	Highly reliable detection with a low proportion of false positives.	N/A
[11]	2022	Singh et al.	Discovery of new ransomware families and classification of newly discovered ransomware assaults.	Checks process memory access privileges to enable rapid and accurate malware detection.	Between 81.38% and 96.28% accuracy.	N/A

An application's normal behavior is assessed from a user and resource perspective. A baseline for normal behavior is established based on what is thought to be the typical or routine operation of a computer system or network. Indicators of usual activity include logins, file access, user and file behaviors, resource utilization, and other significant indicators [1].

The length of the learning process is determined by the amount of data needed to build a baseline to represent typical system behavior. The tool investigates behavioral outliers from the baseline's depiction of the typical behavioral pattern. A ransomware-detection

and -prevention model was created for unstructured datasets derived from Ecuadorian Control and Regulatory Institution (EcuCERT) logs [12].

The methodology uses musing to spot peculiar behavioral patterns connected to Windows malware. Feature selection is applied to the Log data to extract the most beneficial and discriminating information that indicate a ransomware attack. The extracted data represent that autonomous learning algorithms in ransomware are swiftly and precisely identified using the input feature set and algorithms that mimic abnormal behavioral patterns. Code obfuscation tools and new polymorphic variants have been developed as signature additions in identifying ransomware attacks, which are constantly evolving [8].

Since generic malware attack vectors cannot effectively capture the particular behavioral traits of cryptographic ransomware, they are insufficient or inaccurate for ransomware detection. The suggested approach, RansomWall, is a hybrid system that uses static and dynamic analytics to present a research set of properties that mimic ransomware activity. The technique allows for early ransomware detection while utilizing a strong trap layer to detect zero-day attacks. RansomWall with the Gradient Tree Boosting Algorithm demonstrated a detection rate of 98.25% and an incredibly low (almost nil) false-positive rate when tested against 574 samples of 12 cryptographic ransomware running on the Microsoft Windows operating system. It also had a detection rate of less than 10% for 30 zero-day attack samples compared with 60 VirusTotal security engines. One version of behavioral detection methodologies uses a machine learning baseline model for simulating and forecasting the specific network user behavior pattern at the micro level to identify potential scenarios that could indicate a vulnerability or a true ransomware assault [9].

The goal was to find a simple network system's vulnerability to a ransomware attack. Comparing the outcomes from the simulated network and the log data from the server in the existing network system revealed a realistic model with a correlation above 0.8. This method's drawback was that it only adequately captured the activity of a small percentage of users. Future studies should focus on mimicking user behavior over a large user base using big data analytics tools. A more recent method of behavioral ransomware detection used two parallel classifiers [10].

To distinguish between the several Locky ransomware variants, one technique focused on early detection based on the behavioral analysis of ransomware network traffic to prevent ransomware from connecting to command-and-control servers and carrying out damaging payloads. The study employed a dedicated network to collect information and extract important details from network traffic. Using data at the packet and datagram levels, two different (parallel) classifiers were used to analyze the extracted properties of the Locky ransomware family. The results of the studies show that the technology has a high level of success in detecting ransomware activities on the network. Furthermore, it permits an extreme lexicon with a low percentage of false positives. Using command-and-control (C&C), the server blocklists ransomware attacks as the means of communication and conducts behavioral analysis of the ransomware in an IoT environment [7].

A domain-specific strategy for identifying Cryptowall ransomware attacks is provided. The operation obtains the TCP/IP header from the web proxy server, which serves as the TCP/IP traffic gateway. Furthermore, it retrieves source and destination IPs and compares them to the IPs of forbidden command-and-control servers. Ransomware is identified if the source or destination IPs match an attack targeting Internet of Things devices. However, the model was not used to demonstrate how well it could spot ransomware and its attack vectors against different operating system environments. Using a very recent technique of behavioral-based detection that uses access privileges in process memory, ransomware may now be quickly and accurately detected [11,13].

It is possible to categorize new ransomware attacks and find malware families that have not yet been recognized by looking at a file or application's access privileges and the area of memory it intends to access. Examining the behavior and ascertaining the purposes of lawful files and applications before executing them is beneficial. The experimental results

employing these several approaches show good detection accuracy, ranging from 81.38% to 96.28%.

Table 2 summarizes previous studies on machine learning techniques (static and dynamic analysis) for ransomware detection from 2017 to 2022.

Table 2. Studies on machine learning techniques (static and dynamic analysis) for ransomware detection from 2017 to 2022.

Reference	Year	Author	Problem Addressed	Method Used	Result
[14]	2017	Rahman and Hasan	Enhanced ransomware-detection method.	Using support vector machines as an analysis tool.	Better ransomware detection is achieved with an integrated approach than static or dynamic analysis used separately.
[13]	2018	Dehghantanha et al.	Windows ransomware detection that is quick and accurate.	Netconverse (classifier using j48 decision tree).	97.1% actual-positive detection rate.
[15]	2019	Jasmin	Separating ransomware traffic and regular traffic.	Algorithms used in logistic regression include random forest and support vector machine.	The best detection rate is 99.9% for the random forest, with 0% false positives.
[16]	2019	Ameer	Detection of ransomware.	Analyses that are static and dynamic.	100% detection and classification precision.
[17]	2020	Khammas	Detection of ransomware.	Random forest method.	97.74% of samples are detected.
[18]	2020	Hwang et al.	An improved method of detecting ransomware.	Random forest and Markov models.	97.3% overall accuracy, 4.8% for false positives, and 1.5% for false negatives.
[19]	2022	Talabani and Abdulhadi	Tools for detecting ransomware that involve data mining and machine learning approaches have poor accuracy.	Decision Table and PARTially Decided Decision Tree.	Recall (96%), accuracy (96.01%), F-measure (95.6%), and precision (95.9%).

Several improved machine learning approaches have been applied for accurate and efficient ransomware detection. These methods are meant to address the drawbacks of the current ML-based ransomware-detection tools. One of these advancements regards the challenges detection systems (such as sandbox analysis and pipelines) face in isolating a sample and handling the wait time for isolated ransomware samples to be evaluated [20].

The approach predicts ransomware using a dataset containing 30,000 attributes as independent variables. Five qualities that were obtained through feature selection were used in the support vector machine technique. The approach provides a respectable 88.2% accuracy rate in ransomware detection. To reduce the number of false positives, this hybrid technique combines the "guilt by association" hypothesis with content-, metadata-, and behavior-based analysis. Giving the user control over recovery is necessary, and file versioning in cloud storage is used to halt the process. The only duty of the end user is to keep track of the recovery. Users are given classification information so they may make educated decisions and prevent false positives. The method results in more-accurate detection and reliable recovery. An innovative method for detecting network-level ransomware uses machine learning, certificate information, and network connection information [21].

This technique can be used with system-level monitoring to detect ransomware outbreaks early. This method uses connection-, encryption-, and certificate-based network traffic characteristics to extract and model ransomware features. It is a feature model that uses support vector machines, logistic regression, and random forest to distinguish ransomware traffic. According to experimental findings on various datasets, random forest has the best detection rate of 99.9% and the lowest rate of false positives. Another more-effective detection method is a decision tree model based on big data technology that uses Argus for packet preprocessing, combining, and malware file identification [21].

The flow replaced the packet data, resulting in a 1000-fold (1000:1) reduction in data size. Feature selection and concatenation were used to extract and aggregate the attributes of the actual network traffic. In order to improve classification accuracy, the technique made use of six feature selection techniques. Machine learning has recently been creatively applied to monitor Android device power usage as a ransomware-detection technique [13].

The suggested method measures how much energy particular Android processes use to distinguish ransomware from valuable programs. Data on the ransomware's unique local energy fingerprint are gathered and analyzed to accomplish this. According to experimental findings, the approach offers high detection and precision rates of 95.6% and 89%, respectively. Additionally, it outperforms k-nearest neighbor, neural network, support vector machine, and random forest regarding the accuracy, recall rate, precision rate, and F-measure.

Another superior option is the cutting-edge, portable RanDroid approach for automatically detecting polymorphic ransomware [22]. The RanDroid approach uses both static and dynamic analyses to detect polymorphic ransomware. The method compares the structural similarity of pieces obtained from an application with a collection of threat information from well-known ransomware variants to detect new ransomware variants on Android devices. Image similarity measurements (ISMs) and string similarity measurements (SSMs) are the two similarity measures used. Using language analysis, the app's behavioral attributes and picture textural strings are mined for additional information. The strategy reduces ransomware threats without changing the Android OS or its underlying security module while addressing the constraints of static analysis. The methodology can detect ransomware using evasive tactics such as complex codes or dynamic payloads, according to an analysis of the method based on 950 malware samples. According to a related study, a strategy combining static and dynamic analysis can help identify and separate Android ransomware from other malware [16].

We looked at network-based features, text, and permissions using static analysis. Furthermore, dynamic analysis was performed on the system call, CPU, and memory logs. The strategy's effectiveness in reducing evasive ransomware assaults is demonstrated by experiments using traits from malicious and benign samples. Additionally, it is 100 percent accurate at classifying and identifying unknown ransomware.

5. Evolution of Ransomware

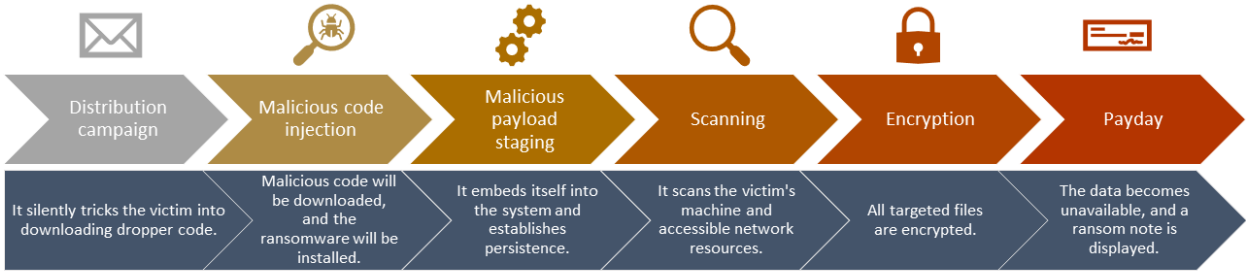
Ransomware attacks have been around since the late 1980s; Joseph Popp showcased the first instance of ransomware. This attack utilized symmetric-key encryption to take control of victims' hard drives and request a ransom. The flaw in this system was that the same key was used for encryption and decryption, making it vulnerable. As a result, it was possible to research the AIDS ransomware (also known as PC Cyborg) to find the decryption key and create a solution for the malware's encryption. Ransomware attacks have continued evolving and have become more sophisticated in recent years, making them a significant threat to individuals and organizations [23]. A brief timeline of various potent ransomware attacks is shown in Table 3. The table, an excerpt from a timeline of the most significant ransomware attacks from 2012 to 2023, contains essential information on the evolution of ransomware based on the year the ransomware first appeared, its name, and its primary description [2,3,23].

Table 3. Brief chronology of major ransomware attacks from 2012 to 2022.

Reference	Year	Name of the Ransomware	Description
[4]	1989	AIDS Trojan	The first known ransomware attack, the AIDS Trojan, was distributed on floppy disks and demanded a payment of USD 189 to unlock infected files.
[5]	2012	Reveton	Ransomware that posed as law enforcement and demanded payment for supposed illegal activities.
[23]	2013	CryptoLocker	One of the first widespread ransomware attacks that used encryption to lock victims' files.
[24]	2014	CryptoWall	A variant of CryptoLocker that caused millions of dollars in damages.
[3]	2015	TeslaCrypt	A ransomware strain that targeted gamers and encrypted game-related files.
[25]	2016	Locky	Ransomware that was spread through malicious email attachments.
[3]	2017	WannaCry	A ransomware attack affecting over 200,000 systems across 150 different countries.
[26]	2018	SamSam	A ransomware attack that targeted hospitals, municipalities, and other organizations.
[3]	2019	Ryuk	A ransomware attack that caused significant damage to several companies and organizations.
[27]	2020	Maze	A ransomware attack that encrypted victims' files and threatened to leak sensitive data if the ransom was not paid.
[3]	2021	REvil/Sodinokibi	A ransomware attack that targeted Kaseya, a software company, and affected over 1500 businesses worldwide.
[28]	2022	Royal Ransomware	A ransomware attack that encrypted victims and demanded a ransom payment in order to decrypt them, targeting businesses, governments, and healthcare organizations, with victims mostly from the United States.
[28]	2023	LockBit Ransomware	A ransomware attack that encrypts the files and demands payment in exchange for the decryption key, often in conjunction with phishing emails or other social engineering techniques.

Ransomware has become a popular tool for cybercriminals to extort money from individuals and organizations. As technology advances, preventing such attacks is more challenging. It is essential to remain vigilant and take appropriate measures to protect against these threats, such as keeping software up-to-date and regularly backing up important data [5]. There are six levels, which can be summarized as follows, as adapted from [29] and shown in Figure 6.

1. Distribution campaign: The attacker silently induces the victim to download the infection-starting dropper code. The attacker uses methods including email phishing, social engineering, and others.
2. Malicious code injection: During this phase, the target's computer is infected with ransomware, and malicious code is downloaded.
3. Malicious payload staging: Ransomware sets up persistence by inserting the system.
4. Scan checks for encryption on the target computer and any network-accessible resources.
5. Encryption: The process of encrypting all of the selected documents begins.
6. Payday: Victims cannot access their data, and a notification seeking payment is visible on the screen of the targeted device.



Kill Chain Stage	Examples of Observed Ransomware Activities	Log Artifacts
Distribution campaign	Evidence, like an email or web activity log, shows a file arriving through a download or email attachment. In our observation, an email with an attachment came from a previously unknown domain to the company.	Proxy Firewall
Malicious code injection	The process interacts with the outside world using a domain that is typically recognized as an artifact of a domain generation algorithm (DGA).	Proxy Process tracking
Malicious payload staging	A process initiates a command prompt and performs actions such as deleting shadow copies or modifying boot options.	File activity Registry tracking
Scanning	A collection of authentication logs indicates scanning activity originating from the compromised host.	Authentication Network activity
Encryption	A process accesses, generates, and removes files from an unusually high number of directories.	File activity Process tracking logs
Payday	A process originating from an atypical location creates instances of a web browser and/or Notepad, accompanied by command line arguments.	File activity Process tracking

Figure 6. Six levels of ransomware attacks [29].

6. Ransomware Detection

6.1. Ransomware-Detection Methods

The two main types of ransomware-detection methods are automated and manual. Employing technologies to identify and report ransomware attacks is a prerequisite for automated methods. These tools are typically software programs that have the potential to be able to stop attacks. Techniques for manual detection focus on routinely scanning data and devices for indicators of attacks. Checking to see if a malware attack has not modified data or stopped authorized users from accessing their devices or files includes looking at any changes to file extensions, the accessibility of devices and files by authorized users, and any changes to file extensions. The flow of the presentation in this section is illustrated in Figure 7.

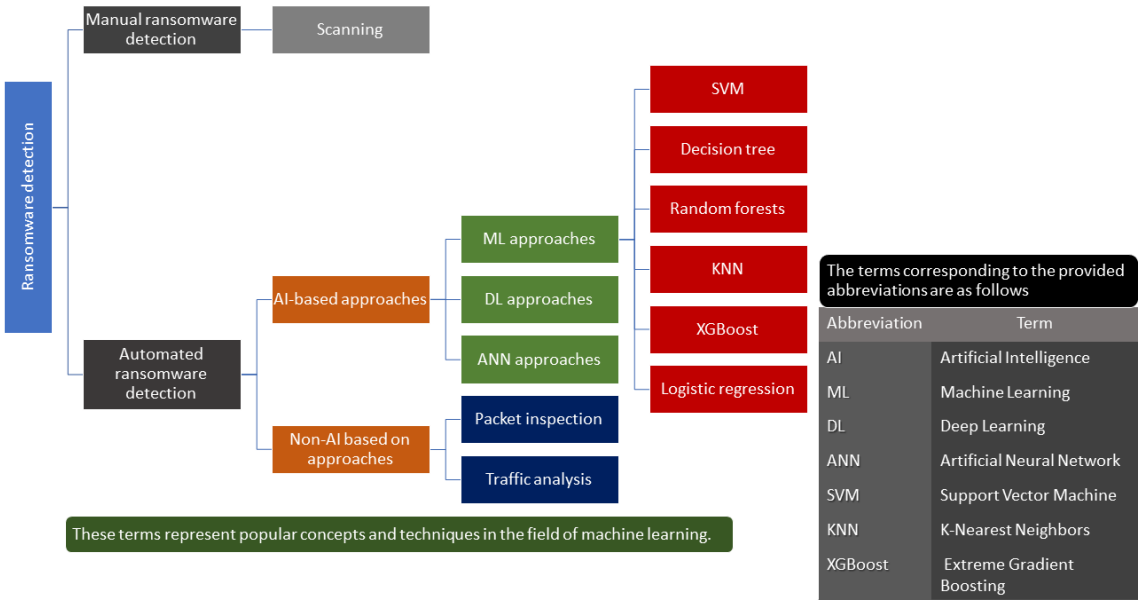


Figure 7. Ransomware detection taxonomy.

6.1.1. Manual Ransomware Detection

Manual ransomware detection refers to the process of detecting ransomware through human analysis and intervention rather than automated systems. This approach involves analyzing system logs, network traffic, and other indicators of compromise to identify patterns and behaviors associated with ransomware attacks. While manual detection can be time-consuming and resource-intensive, it can be an effective complement to automated detection methods, as it can help identify new or unknown types of ransomware that may not be detected by automated systems [30].

Despite its effectiveness, manual ransomware detection has some limitations. It can be labor-intensive and requires highly trained personnel to analyze system logs and network traffic. Additionally, manual detection may not scale well in large organizations or networks, where automated detection methods may be more efficient [30].

Scanning

Manual ransomware-detection scanning is a technique used to detect ransomware through the manual analysis of files and systems. This approach involves scanning individual files or systems for signs of ransomware activity, such as encrypted files or abnormal network traffic. Manual scanning can be a complementary approach to automated scanning methods, as it can help detect new or unknown types of ransomware that may not be detected by automated systems [30].

While manual ransomware-detection scanning can be effective, it has some limitations. It can be time-consuming and labor-intensive, especially when scanning large networks or systems. Additionally, manual scanning may generate false positives, which can be disruptive to normal system operations [30].

6.1.2. Automated Ransomware Detection

The current methods for detecting ransomware primarily involve monitoring the system at the file system level. Automated approaches to detecting ransomware can be categorized into two main groups: those based on artificial intelligence (AI) and those that are not based on AI. AI-based methods typically employ machine learning (ML), deep learning (DL), and artificial neural network (ANN) techniques to detect ransomware. Some tools utilize variations of these techniques or a hybrid approach that combines two or more techniques to combat the threat of ransomware attacks. Non-AI methods rely on packet inspection and traffic analysis to detect ransomware. One of the major advantages of automated approaches is their ability to detect, block, and recover from ransomware attacks without human intervention. Additionally, these tools are highly accurate and reliable in terms of detecting, preventing, and recovering from ransomware attacks [31].

Artificial-Intelligence-Based Approaches

Artificial intelligence (AI) techniques, including machine learning, deep learning, and artificial neural networks, have been utilized for automated ransomware detection. These techniques involve the use of behavioral techniques, as well as static and dynamic analysis, to identify and prevent ransomware attacks. Machine learning algorithms can learn from previous ransomware attacks and detect new variants by analyzing patterns and behaviors. On the other hand, deep learning methods can leverage neural networks to detect ransomware attacks by analyzing large amounts of data. Artificial neural networks can also be used to identify ransomware by processing and analyzing multiple data sources. These AI-based approaches offer a more efficient and reliable way to detect and prevent ransomware attacks, reducing the potential impact on businesses and individuals [31]. AI-based approaches include the following:

1. Machine Learning Approaches

Machine-learning-based detection is a more advanced approach that relies on training a machine learning model to detect ransomware based on its behavior patterns or features. This approach is based on collecting a large dataset of benign and malicious samples,

extracting relevant features from them, and then training a machine learning model to classify new samples as peaceful or hostile based on their characteristics [32,33].

Machine-learning-based detection has several benefits, including its ability to detect new or unknown ransomware variants that do not match existing signatures or patterns and to adapt to changing ransomware behavior patterns over time. Moreover, this approach is less prone to false positives than signature-based and heuristic-based detection, as it relies on detecting actual behavior patterns rather than static code signatures or predefined rules. However, machine-learning-based detection is limited by its reliance on a large and representative dataset of training samples and by its susceptibility to adversarial attacks that can manipulate the features or behavior of the ransomware to evade detection [31].

a. Machine Learning Algorithms for Ransomware Detection

A particular kind of artificial intelligence known as machine learning enables computer systems to improve their performance on a given job without being explicitly taught. Malicious ransomware malware encrypts a victim's files and demands payment for the decryption key. Due to their rising prevalence and severity, machine learning techniques are increasingly needed to identify and stop ransomware attacks. Table 4 lists the machine learning algorithms that are employed. Support vector machines, decision trees, random forests, k-nearest neighbors, XGBoost, and logistic regression are just a few machine learning approaches that can detect ransomware. Each method has advantages and disadvantages, and the best approach depends on the situation and the data [1,6].

Table 4. Machine learning algorithms.

References	Algorithm	Characteristics
[17,34]	Decision tree	Decision trees can be trained on features such as file modifications, network traffic, and system calls to distinguish between ransomware and benign software behavior. The resulting decision tree can then be used to determine whether new data contain ransomware.
[17,34]	Random forest	In order to guarantee that each tree in the forest has the same distribution and is dependent on the values of a randomly selected random vector, this strategy uses an ensemble method that combines tree predictors. Performance may be enhanced in comparison to standalone decision trees. Using a network of decision trees, the random forest approach is used to select and forecast the input data type.
[14,35]	Support vector machine	Support vector machines can be trained on features such as system calls, network traffic, and file behavior to distinguish between ransomware and benign software behavior. After that, it is possible to determine whether new data constitute ransomware using the resultant support vector machines. Support vector machines are handy when the data are high-dimensional and non-linearly separable, as is often the case in ransomware detection.
[36,37]	k-nearest neighbor	k-nearest neighbor is a popular machine learning algorithm used in various research fields. It is a non-parametric approach that can be used for both classification and regression tasks. KNN is known for its simplicity, but is also computationally expensive, with simplified and concise hyperparameters.
[38]	XGBoost	Extreme gradient boosting is a powerful machine learning algorithm that has gained widespread popularity in research. It is an ensemble method that combines multiple decision trees to improve the accuracy of the model. XGBoost is known for its scalability, speed, and ability to handle complex datasets.
[39]	Logistic regression	Logistic regression is a widely used machine learning algorithm in various research fields. It is a linear model that can be used for binary classification tasks. Logistic regression is known for its simplicity, interpretability, and ability to handle small datasets.

Decision trees are a simple and intuitive machine learning algorithm that can be used for classification tasks, including ransomware detection. Decision trees work by recursively partitioning the data into subsets based on the values of the features and creating a tree-like structure representing the decision-making process. Both categorical and continuous

components can be handled by decision trees, which are simple to interpret but susceptible to overfitting and sensitive to minute changes in the data [13,31,34].

Random forests are an extension of decision trees that improve performance and reduce overfitting. By randomly selecting features and data, random forests create multiple decision trees and combine their predictions. They are better-equipped to handle high-dimensional data and are less likely to overfit. However, they can be computationally demanding and difficult to interpret [17].

Support vector machines are reliable machine learning techniques that can be utilized for ransomware detection and classification and regression applications. Support vector machines operate by identifying the hyperplane that divides the data into distinct classes according to the values of the features as thoroughly as possible. Support vector machines can effectively handle high-dimensional data. They can accept both linear and nonlinear borders, but the choice of the kernel function and its parameters may impact them [14].

k-NN is a non-parametric algorithm used for classification and regression tasks. It works by finding the k closest data points in the training set to a given input, and then predicting the label of the input based on the most common label among those k neighbors. It is a simple but effective algorithm that can be used in a wide range of applications [36,37]

XGBoost (short for "Extreme Gradient Boosting") is a powerful machine learning algorithm that is especially popular for gradient boosting tasks. It uses a combination of decision trees and gradient boosting to create a highly accurate model that can handle large datasets and complex feature interactions. XGBoost has become widely used in the industry [38].

Logistic regression is a parametric algorithm used for binary classification tasks (i.e., where the output is one of two possible classes). It works by modeling the probability of the output class as a function of the input features. The algorithm is trained to find the optimal parameters that maximize the likelihood of the training data and can be regularized to prevent overfitting [39].

The choice of a machine learning algorithm for ransomware detection depends on the specific problem and data available. Decision trees, random forests, support vector machines, and neural networks are all effective options, and researchers have successfully used each of these algorithms for ransomware detection in different contexts [5,31].

2. Deep Learning Approaches

Deep learning techniques have been proposed as a solution to address the limitations of traditional supervised ransomware-detection tools to enhance the accuracy and reliability of ransomware detection. These algorithms utilize automatic feature generation and are well-suited to handle unstructured datasets, requiring minimal or no human intervention due to their self-learning capabilities. Their effectiveness in classifying audio, text, and image data makes them particularly useful in detecting textual and image-based ransomware data. However, training deep learning algorithms demand a considerable amount of data, which may render them unsuitable for general-purpose applications, particularly those involving small datasets or sizes. Other challenges associated with deep learning include the need for high processing power and difficulty with adapting to real-world datasets [6,40].

3. Artificial Neural Network Approaches

Artificial neural network approaches are well-suited for detecting various types and variants of ransomware data, including text and image ransomware variants, due to their wide range of applications. Neural networks are an excellent choice for adapting to new ransomware data and identifying zero-day attacks because of their ability to continuously learn. The versatility of neural networks makes them highly effective in detecting different forms of ransomware data and adapting to new threats. However, these techniques are dependent on hardware and can be vulnerable to data dependencies, as well as the black-box nature of the technology, which limits the ability of human analysts to monitor data processing and identify deviations in the process [5,6,41].

Non-Artificial-Intelligence-Based Methods

Non-AI techniques such as packet inspection and traffic analysis can be utilized to detect ransomware. Anomaly detection is one effective algorithm used to detect ransomware. These algorithms analyze network traffic and identify patterns that deviate from normal behavior. Unusual patterns of network traffic, such as a sudden increase in file encryption activity or a large number of outbound network connections to suspicious IP addresses, are indications of ransomware activity. By comparing network traffic to a baseline of normal behavior, anomaly-detection algorithms can quickly identify and alert security teams to potential ransomware attacks [2].

Other non-AI techniques include signature-based detection, which involves comparing network traffic to known ransomware signatures, and behavior-based detection, which looks for patterns of behavior consistent with known ransomware attacks [2].

Another approach involves the use of honeypots to monitor network activity and detect the presence of ransomware. This method entails the establishment of a honeypot folder and observing any changes that may indicate the presence of ransomware. The early detection of ransomware is critical in mitigating its impact and preventing further damage [2].

It is important to note that these detection techniques are not foolproof and should be used in conjunction with other security measures such as user education, regular backups, and security patches [2].

Antivirus software is an example of a non-AI-based approach for detecting and preventing malware, including ransomware. It typically uses a combination of signature-based detection and behavior-based detection to identify and block malicious software. Signature-based detection involves comparing files against a database of known malware signatures, while behavior-based detection looks for patterns of behavior that are indicative of malware activity. While antivirus software has been an effective tool for detecting and preventing malware, it has some limitations. For example, signature-based detection is only effective against known malware signatures, meaning that new or unknown forms of malware can bypass this detection method. Additionally, some types of malware can be designed to evade behavior-based detection methods [42].

In recent years, AI-based approaches, such as machine learning and deep learning, have been introduced to enhance the accuracy and effectiveness of malware detection. However, antivirus software continues to be a critical component of cybersecurity, particularly for organizations with limited resources or expertise in AI-based techniques. By using a combination of signature-based and behavior-based detection, antivirus software can provide an effective defense against known and unknown forms of malware, including ransomware [42].

1. Packet Inspection

Packet inspection refers to examining individual data packets' contents as they move through a network. This technique can be used to detect the presence of malware by identifying packets that contain suspicious data or have characteristics that are inconsistent with normal network traffic. For example, packets containing large amounts of encrypted data or sent from suspicious IP addresses may indicate ransomware activity [43,44].

2. Traffic Analysis

Traffic analysis, on the other hand, involves the examination of patterns of network traffic over a period of time. This technique can be used to detect ransomware by identifying patterns of behavior that are consistent with known ransomware attacks. For example, traffic analysis may reveal a sudden increase in network traffic during off-hours or a large number of outbound network connections to suspicious IP addresses. Packet inspection and traffic analysis are two important techniques used in detecting malicious software, including ransomware. These techniques involve the examination of network traffic to identify potentially harmful data packets and patterns of behavior that may indicate the presence of malware. By examining network traffic and identifying patterns of behavior

indicative of malicious activity, these techniques can help organizations detect ransomware attacks and protect their critical data and systems [45,46].

Packet inspection and traffic analysis are two essential techniques for detecting ransomware and other forms of malware. By examining network traffic and identifying behavior indicative of malicious activity, these techniques can help organizations detect ransomware attacks and protect their critical data and systems. They should be used alongside other security measures, such as regular backups and security patches, as they are not completely infallible. Furthermore, these techniques necessitate specialized tools and expertise, which can pose a challenge for organizations without dedicated cybersecurity resources [43–46].

6.2. Ransomware-Detection Techniques

Ransomware detection is a critical component of cybersecurity, and various techniques have been developed to detect ransomware attacks. This section will discuss different ransomware-detection techniques proposed in the literature and their strengths, weaknesses, and limitations.

6.2.1. Signature-Based Detection

Signature-based detection is a traditional approach that relies on identifying known ransomware signatures or patterns in the code or behavior of the malware. This approach is based on creating a database of known ransomware signatures or marks and scanning the system or network for matching signatures or patterns. If a match is found, the ransomware is flagged as malicious and appropriate actions are taken [32,33].

One benefit of signature-based detection is its simplicity and effectiveness in detecting known ransomware variants. However, this approach is limited by its inability to detect new or unknown ransomware variants that do not match existing signatures or patterns. Moreover, attackers can easily evade signature-based detection by modifying the code or behavior of the ransomware to avoid detection [31].

6.2.2. Heuristic-Based Detection

Heuristic-based detection is a more advanced approach that identifies ransomware behavior patterns or anomalies indicative of malicious activity. This approach is based on creating rules or heuristics that describe typical ransomware behavior and then monitoring the system or network for any deviations or anomalies from these rules. If such variations or abnormalities are detected, the ransomware is flagged as suspicious or malicious, and appropriate actions are taken [32,33].

One of the advantages of heuristic-based detection is its ability to detect new or unknown ransomware variants that do not match any existing signatures or patterns. Moreover, this approach is less prone to false positives than signature-based detection, as it relies on detecting actual behavior patterns rather than static code signatures. However, heuristic-based detection is limited by its reliance on predefined rules or heuristics, which may only capture some possible ransomware behavior patterns or anomalies. Moreover, attackers can easily evade heuristic-based detection by modifying the behavior of the ransomware to avoid detection [31].

6.2.3. Network-Based Detection

Network-based detection is an approach that relies on monitoring the network traffic for suspicious or malicious activity that may be indicative of a ransomware attack. This approach is based on analyzing the network traffic for anomalies or patterns characteristic of ransomware, such as large volumes of outbound traffic, unusual network connections, or network traffic encryption [32,33].

One of the advantages of network-based detection is its ability to detect ransomware activity even if the malware has not yet infected the system or if the ransomware is using non-standard encryption methods. Moreover, this approach is less prone to false positives

than other detection approaches, as it relies on detecting actual network traffic patterns rather than static code signatures or predefined rules. However, network-based detection is limited by its reliance on network traffic analysis tools that may not be available or may not capture all ransomware activity. Moreover, attackers can easily evade network-based detection by encrypting their network traffic or using stealthy communication channels [31].

6.2.4. Hybrid Detection

Hybrid detection is an approach that combines different ransomware-detection techniques to improve the overall detection accuracy and speed. This approach combines the strengths of other detection techniques, such as signature-based, heuristic-based, machine-learning-based, and network-based detection, to create a more robust and effective detection system [32,33].

One of the advantages of hybrid detection is its ability to overcome the limitations of individual detection approaches and to improve the overall detection accuracy and speed. Moreover, this approach is less prone to false positives and negatives than unique detection approaches, as it combines different sources of information and analysis. However, hybrid detection is limited by its complexity and resource requirements, as it requires integrating and coordinating other detection systems and tools [31].

6.3. Feature Extraction and Selection

Machine learning techniques have been increasingly used to detect ransomware due to their ability to learn behavior patterns and detect anomalies. In this section, we will discuss different features used for ransomware detection using machine learning and the techniques used for feature selection, such as principal component analysis and correlation analysis [18,47].

6.3.1. Features Used for Ransomware Detection

There are several features that can be used for ransomware detection, with the most common ones including the following:

1. File access patterns are a common feature used to detect ransomware. Ransomware often accesses and encrypts files in a specific pattern, such as alphabetical order, extension type, or creation date. This behavior can be detected using file access patterns as features. For example, analysis of file access patterns may reveal that a large number of files are being accessed and modified in a short period of time, indicating a potential ransomware attack [48].
2. System calls are another feature commonly used for ransomware detection. Ransomware frequently uses system calls to perform malicious activities, such as reading and writing files, creating processes, and network communication. System-call traces can be extracted and used as features for detection. For example, analysis of system-call traces may reveal that a process is making an unusually high number of system calls, which could indicate ransomware activity [34].
3. Network traffic analysis is a valuable feature for detecting ransomware. Typically, ransomware uses a command-and-control (C&C) server to deliver and receive orders. Analysis of network traffic can provide valuable features for detecting ransomware. For example, analysis of network traffic may reveal that a large amount of data are being sent to an unusual IP address, which could indicate that the system is infected with ransomware [49].
4. Behavioral analysis is another approach to ransomware detection. This involves monitoring the behavior of running processes and identifying anomalies that indicate malicious activity. Features such as process creation, termination, and file access can be used for this type of analysis. For example, the analysis of process creation and termination events may reveal that a process is spawning multiple child processes, which could indicate ransomware activity [1].

5. Static analysis is the examination of the executable file's source code to spot malicious activity. Features such as code size, entropy, and string patterns can be used for this purpose. For example, analysis of code size and entropy may reveal that a file contains obfuscated code, which could indicate ransomware activity [32]. Behavioral analysis and dynamic analysis are similar in that they both involve the monitoring of running processes to identify malicious activity. However, there are some key differences between the two approaches.

Behavioral analysis involves monitoring the behavior of running processes on a system to identify anomalies that indicate malicious activity. This is typically carried out in real-time, allowing the detection of ransomware as it is executed on a system. In contrast, dynamic analysis involves running an executable file in a controlled environment, such as a sandbox, to observe its behavior and identify any malicious activity. This is typically conducted prior to deploying the executable file on a production system.

The confusion between static and dynamic analysis may arise from the fact that both approaches involve the analysis of executable files, but they do so in different ways. Static analysis involves looking at the executable file's source code to spot malicious activity, while dynamic analysis involves running the executable file in a controlled environment to observe its behavior.

Dynamic analysis can be performed in real-time, but it can also be conducted in a sandbox environment before deploying the executable file on a production system. In a sandbox environment, the executable file is executed in a controlled environment, allowing its behavior to be monitored and analyzed without affecting the production system. Once the analysis is complete, the results can be used to determine whether the executable file is malicious or benign.

In the case of ransomware, real-time behavioral analysis is typically the preferred approach for detecting and responding to attacks. However, dynamic analysis can also be useful for identifying new and previously unseen variants of ransomware, which can then be used to improve the effectiveness of real-time behavioral analysis.

By using these features, machine-learning-based ransomware-detection methods can achieve high detection rates and low false-positive rates.

6.3.2. Feature Selection Techniques

- Principal component analysis: This technique is used to reduce the dimensionality of a dataset by identifying the most critical features that explain the majority of the variance in the data. Principal component analysis can help identify redundant or irrelevant features and select the most informative ones for ransomware detection [50].
- Correlation analysis: Correlation analysis is a technique used to identify the correlation between features in a dataset. Highly correlated features may be redundant and can be removed to simplify the model and improve performance [27].

6.4. Performance Evaluation of Machine Learning Models for Ransomware Detection

Evaluating the performance of machine learning models for ransomware detection is crucial to determine their effectiveness in detecting and preventing its spread. In this section, we will discuss different evaluation metrics used for measuring the performance of machine learning models for ransomware detection, including accuracy, precision, recall, F1-score, and ROC curve.

1. Accuracy: Accuracy is the most straightforward evaluation metric, representing the percentage of correct predictions made by the model. It is calculated as the ratio of accurate predictions to the total number of predictions. However, accuracy can be misleading when dealing with imbalanced datasets, where negative samples greatly outweigh the positive models [51,52].
2. Precision: Out of all samples predicted to be positive (recognized as ransomware by the algorithm), precision is the percentage of true positives (samples of successfully identified malware). The ratio of true positives to the total of true and false positives is

known as precision. A model with a high precision score will have a low false-positive rate, making it less likely to mistakenly label innocent files as ransomware [52].

3. Recall: Recall counts the number of positive samples in the collection that are true positives. The ratio of true positives to true and false negatives is computed. A high recall score suggests that the model has a low incidence of false negatives, which makes it less likely to fail to detect actual ransomware samples [13,52].
4. ROC curve: The performance of a binary classifier as the discrimination threshold is changed is graphically represented by a receiver operating characteristic (ROC) curve. At various threshold values, it plots the actual-positive rate (TPR) versus the false-positive rate (FPR). The model's overall performance is assessed using the area under the ROC curve (AUC), with higher AUC values indicating better performance [53].

7. Challenges and Future Directions

Developing effective machine-learning-based ransomware-detection systems is challenging due to several factors. This section will discuss the challenges of developing such systems and highlight the future directions in this field.

7.1. Challenges in Developing Effective Machine-Learning-Based Ransomware-Detection Systems

Developing effective machine-learning-based ransomware-detection systems presents several challenges, with the most common ones being:

1. Data quality and quantity—A vast amount of high-quality data are needed to train machine learning models effectively. However, obtaining high-quality data for ransomware detection is challenging due to the limited availability of labeled ransomware samples [54,55].
2. Rapidly evolving ransomware—Ransomware is a constantly changing threat, with new variants and attack techniques being developed regularly. This makes it challenging to build machine learning models that can detect all ransomware accurately and quickly [56].
3. Adversarial attacks involve modifying the input data to bypass the machine learning model's detection capabilities. Malicious attacks can be used to evade ransomware-detection systems, making the systems less effective [56].
4. Real-time detection requirements—Ransomware can spread rapidly and cause significant damage within a short time-frame. Therefore, ransomware-detection systems must be able to detect ransomware in real-time to prevent further spread and damage [57].
5. One of the main challenges in collecting data for ransomware detection is the need for publicly available datasets that include real-world ransomware samples. This is due to the sensitive nature of the data and the fact that many victims are reluctant to report ransomware attacks. As a result, researchers often rely on synthetic datasets or datasets generated from sandbox environments, which may not accurately reflect the complexity and variability of real-world ransomware attacks [3].
6. Another challenge is the diversity of ransomware families and variants, which require a large and diverse dataset to ensure adequate coverage. Ransomware behavior can also vary depending on the victim's system and network environment, making generalizing detection models across different contexts challenging [2,54].
7. Preprocessing data for ransomware detection also presents several challenges. Ransomware often employs obfuscation techniques to evade detection, such as encrypting the payload or using anti-analysis mechanisms. This can make extracting relevant data features and identifying patterns that distinguish ransomware from benign software difficult. In addition, ransomware may use legitimate system functions that are difficult to distinguish from malicious behavior, requiring advanced feature engineering and modeling techniques [54].
8. Despite these challenges, several datasets have been used to train and evaluate ransomware-detection models.

9. Collecting and preprocessing data for ransomware detection using machine learning presents several challenges, including the lack of real-world datasets, the diversity of ransomware families and variants, and the obfuscation techniques used by ransomware. However, several datasets have been developed to address these challenges, providing valuable resources for training and evaluating ransomware-detection models [54].

7.2. Future Work

Future work in machine-learning-based ransomware detection could include the following:

1. Developing more robust and accurate models—Researchers must build more substantial and precise machine learning models that detect a wide range of ransomware variants and attack techniques. This can be achieved through advanced techniques such as deep learning and ensemble learning [4,54,58].
2. Incorporating real-time detection capabilities—Ransomware-detection systems must incorporate real-time detection capabilities to quickly identify and prevent ransomware attacks. This can be achieved through the use of real-time monitoring and analysis techniques [55].
3. Addressing the issue of adversarial attacks—Researchers need to develop machine learning models that are robust to malicious attacks. This can be achieved through techniques such as negative training and defensive distillation [54,56].
4. Collaboration and sharing of data—Collaboration and sharing of data among researchers and organizations can help develop more effective ransomware-detection systems. This can help build more comprehensive datasets for training and testing machine learning models [56].
5. Developing effective machine-learning-based ransomware-detection systems is challenging for several reasons. However, with advanced techniques and collaboration among researchers and organizations, it is possible to develop more robust and accurate ransomware-detection systems [54].

8. Conclusions

Ransomware attacks have caused significant harm to computer systems and the data they manage, resulting in unauthorized access, disclosure, and the destruction of important and sensitive information. These attacks have led to substantial financial losses and reputational damage for both individuals and businesses. In response, various methods have been suggested to detect ransomware accurately, quickly, and dependably. This research provides readers with a historical background and timeline of ransomware attacks, as well as a discussion of the issue's context. The review of the recent literature offers an up-to-date understanding of automated ransomware-detection approaches. This knowledge will help readers stay current on the latest advances in automated ransomware detection, prevention, mitigation, and recovery. Additionally, this research discusses future research directions, highlighting open issues and potential research problems for those interested in researching ransomware detection, prevention, mitigation, and recovery.

Author Contributions: Author Contributions: collecting the papers, A.A. (Amjad Alraizza); Formal analysis, A.A. (Amjad Alraizza); Resources, A.A. (Abdulmohsen Algarni); Writing—original draft, A.A. (Amjad Alraizza); Writing review and editing, A.A. (Abdulmohsen Algarni); Supervision, A.A. (Abdulmohsen Algarni); Funding acquisition, A.A. (Abdulmohsen Algarni). All authors have read and agreed to the published version of the manuscript.

Funding: This research was financially supported by the Deanship of Scientific Research at King Khalid University under research grant number (R.G.P.2/549/44).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Celdrán, A.H.; Sánchez, P.M.S.; Castillo, M.A.; Bovet, G.; Pérez, G.M.; Stiller, B. Intelligent and behavioral-based detection of malware in IoT spectrum sensors. *Int. J. Inf. Secur.* **2022**, *22*, 541–561. [CrossRef]
2. Chesti, I.A.; Humayun, M.; Sama, N.U.; Jhanjhi, N. Evolution, mitigation, and prevention of ransomware. In Proceedings of the 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 13–15 October 2020; pp. 1–6.
3. Philip, K.; Sakir, S.; Domhnall, C. Evolution of ransomware. *IET Netw.* **2018**, *7*, 321–327.
4. Jegede, A.; Fadele, A.; Onoja, M.; Aimufua, G.; Mazadu, I.J. Trends and Future Directions in Automated Ransomware Detection. *J. Comput. Soc. Inform.* **2022**, *1*, 17–41. [CrossRef]
5. Brewer, R. Ransomware attacks: Detection, prevention and cure. *Netw. Secur.* **2016**, *2016*, 5–9. [CrossRef]
6. Bello, I.; Chiroma, H.; Abdullahi, U.A.; Gital, A.Y.; Jauro, F.; Khan, A.; Okesola, J.O.; Abdulhamid, S.M. Detecting ransomware attacks using intelligent algorithms: Recent development and next direction from deep learning and big data perspectives. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 8699–8717. [CrossRef]
7. Zahra, A.; Shah, M.A. IoT based ransomware growth rate evaluation and detection using command and control blacklisting. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; pp. 1–6.
8. Shaukat, S.K.; Ribeiro, V.J. RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning. In Proceedings of the 2018 10th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 3–7 January 2018; pp. 356–363.
9. Makinde, O.; Sangodoyin, A.; Mohammed, B.; Neagu, D.; Adamu, U. Distributed network behaviour prediction using machine learning and agent-based micro simulation. In Proceedings of the 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), Istanbul, Turkey, 26–28 August 2019; pp. 182–188.
10. Almashhadani, A.O.; Kaiiali, M.; Sezer, S.; O'Kane, P. A multi-classifier network-based crypto ransomware detection system: A case study of locky ransomware. *IEEE Access* **2019**, *7*, 47053–47067. [CrossRef]
11. Singh, A.; Ikuesan, R.A.; Venter, H. Ransomware detection using process memory. *arXiv* **2022**, arXiv:2203.16871.
12. Silva, J.A.H.; Hernández-Alvarez, M. Large scale ransomware detection by cognitive security. In Proceedings of the 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM), Salinas, Ecuador, 16–20 October 2017; pp. 1–4.
13. Azmoodeh, A.; Dehghantanha, A.; Conti, M.; Choo, K.K.R. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *J. Ambient Intell. Humaniz. Comput.* **2018**, *9*, 1141–1152. [CrossRef]
14. Ghouti, L.; Imam, M. Malware classification using compact image features and multiclass support vector machines. *IET Inf. Secur.* **2020**, *14*, 419–429. [CrossRef]
15. Modi, J. Detecting Ransomware in Encrypted Network Traffic Using Machine Learning. Ph.D. Thesis, University of Victoria, Saanich, BC, Canada, 2019.
16. Ameer, M. Android Ransomware Detection Using Machine Learning Techniques to Mitigate Adversarial Evasion Attacks. Master's Thesis, Capital University of Science and Technology, Islamabad, Pakistan, 2019.
17. Khammas, B.M. Ransomware detection using random forest technique. *ICT Express* **2020**, *6*, 325–331. [CrossRef]
18. Hwang, J.; Kim, J.; Lee, S.; Kim, K. Two-stage ransomware detection using dynamic analysis and machine learning techniques. *Wirel. Pers. Commun.* **2020**, *112*, 2597–2609. [CrossRef]
19. Talabani, H.S.; Abdulhadi, H.M.T. Bitcoin ransomware detection employing rule-based algorithms. *Sci. J. Univ. Zakho* **2022**, *10*, 5–10. [CrossRef]
20. Adamu, U.; Awan, I. Ransomware prediction using supervised learning algorithms. In Proceedings of the 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), Istanbul, Turkey, 26–28 August 2019; pp. 57–63.
21. Wan, Y.L.; Chang, J.C.; Chen, R.J.; Wang, S.J. Feature-selection-based ransomware detection with machine learning of data analysis. In Proceedings of the 2018 3rd International Conference on Computer and Communication Systems (ICCCS), Nagoya, Japan, 27–30 April 2018; pp. 85–88.
22. Alzahrani, A.; Alshehri, A.; Alshahrani, H.; Alharthi, R.; Fu, H.; Liu, A.; Zhu, Y. Randroid: Structural similarity approach for detecting ransomware applications in android platform. In Proceedings of the 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 3–5 May 2018; pp. 0892–0897.
23. Scaife, N.; Carter, H.; Traynor, P.; Butler, K.R. Cryptolock (and drop it): Stopping ransomware attacks on user data. In Proceedings of the 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), Nara, Japan, 27–30 June 2016; pp. 303–312.
24. Sgandurra, D.; Muñoz-González, L.; Mohsen, R.; Lupu, E.C. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. *arXiv* **2016**, arXiv:1609.03020.
25. Prakash, K.P.; Nafis, T.; Biswas, S.S. Preventive Measures and Incident Response for Locky Ransomware. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 392–395.
26. Paquet-Clouston, M.; Haslhofer, B.; Dupont, B. Ransomware payments in the bitcoin ecosystem. *J. Cybersecur.* **2019**, *5*, tyz003. [CrossRef]
27. Kok, S.; Abdullah, A.; Jhanjhi, N.; Supramaniam, M. Ransomware, threat and detection techniques: A review. *Int. J. Comput. Sci. Netw. Secur* **2019**, *19*, 136.

28. Thakran, E.; Kumari, A. Impact of "Ransomware" on Critical Infrastructure Due to Pandemic. 2023; p. 5. Available online: https://ssrn.com/abstract=4361110 (accessed on 3 July 2023).
29. Ahmed, Y.A.; Huda, S.; Al-rimy, B.A.S.; Alharbi, N.; Saeed, F.; Ghaleb, F.A.; Ali, I.M. A weighted minimum redundancy maximum relevance technique for ransomware early detection in industrial IoT. *Sustainability* **2022**, *14*, 1231. [CrossRef]
30. Aslan, Ö.A.; Samet, R. A comprehensive review on malware detection approaches. *IEEE Access* **2020**, *8*, 6249–6271. [CrossRef]
31. Akhtar, M.S.; Feng, T. Malware Analysis and Detection Using Machine Learning Algorithms. *Symmetry* **2022**, *14*, 2304. [CrossRef]
32. Yamany, B.; Elsayed, M.S.; Jurcut, A.D.; Abdelbaki, N.; Azer, M.A. A New Scheme for Ransomware Classification and Clustering Using Static Features. *Electronics* **2022**, *11*, 3307. [CrossRef]
33. Yamany, B.; Azer, M.A.; Abdelbaki, N. Ransomware Clustering and Classification using Similarity Matrix. In Proceedings of the 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), Cairo, Egypt, 8–9 May 2022; pp. 41–46.
34. Ullah, F.; Javaid, Q.; Salam, A.; Ahmad, M.; Sarwar, N.; Shah, D.; Abrar, M. Modified decision tree technique for ransomware detection at runtime through API Calls. *Sci. Program.* **2020**, *2020*, 8845833. [CrossRef]
35. Arunkumar, M.; Kumar, K.A. GOSVM: Gannet optimization based support vector machine for malicious attack detection in cloud environment. *Int. J. Inf. Technol.* **2023**, *15*, 1653–1660. [CrossRef]
36. Selamat, N.; Ali, F. Comparison of malware detection techniques using machine learning algorithm. *Indones. J. Electr. Eng. Comput. Sci.* **2019**, *16*, 435. [CrossRef]
37. Mezquita, Y.; Alonso, R.S.; Casado-Vara, R.; Prieto, J.; Corchado, J.M. A review of k-nn algorithm based on classical and quantum machine learning. In *Distributed Computing and Artificial Intelligence, Special Sessions, 17th International Conference*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 189–198.
38. Saadat, S.; Joseph Raymond, V. Malware classification using CNN-XGBoost model. In *Artificial Intelligence Techniques for Advanced Computing Applications: Proceedings of ICACT 2020*; Springer, Berlin/Heidelberg, Germany, 2021; pp. 191–202.
39. Noorbehbahani, F.; Rasouli, F.; Saberi, M. Analysis of machine learning techniques for ransomware detection. In Proceedings of the 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Mashhad, Iran, 28–29 August 2019; pp. 128–133.
40. Sharmeen, S.; Ahmed, Y.A.; Huda, S.; Koçer, B.Ş.; Hassan, M.M. Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. *IEEE Access* **2020**, *8*, 24522–24534. [CrossRef]
41. Swami, S.; Swami, M.; Nidhi, N. Ransomware Detection System and Analysis Using Latest Tool. *Int. J. Adv. Res. Sci. Commun. Technol.* **2021**, *7*, 2581–9429. [CrossRef]
42. Wang, X.b.; Yang, G.y.; Li, Y.c.; Liu, D. Review on the application of artificial intelligence in antivirus detection system i. In Proceedings of the 2008 IEEE Conference on Cybernetics and Intelligent Systems, Chengdu, China, 21–24 September 2008; pp. 506–509.
43. Yang, B.; Liu, D. Research on Network Traffic Identification based on Machine Learning and Deep Packet Inspection. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15–17 March 2019; pp. 1887–1891. [CrossRef]
44. Pimenta Rodrigues, G.A.; de Oliveira Albuquerque, R.; Gomes de Deus, F.E.; de Sousa Jr, R.T.; de Oliveira Júnior, G.A.; Garcia Villalba, L.J.; Kim, T.H. Cybersecurity and network forensics: Analysis of malicious traffic towards a honeynet with deep packet inspection. *Appl. Sci.* **2017**, *7*, 1082. [CrossRef]
45. Song, W.; Beshley, M.; Przystupa, K.; Beshley, H.; Kochan, O.; Pryslupskyi, A.; Pieniak, D.; Su, J. A software deep packet inspection system for network traffic analysis and anomaly detection. *Sensors* **2020**, *20*, 1637. [CrossRef]
46. Cascarano, N.; Ciminiera, L.; Risso, F. Optimizing deep packet inspection for high-speed traffic analysis. *J. Netw. Syst. Manag.* **2011**, *19*, 7–31. [CrossRef]
47. Dargahi, T.; Dehghantanha, A.; Bahrami, P.N.; Conti, M.; Bianchi, G.; Benedetto, L. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *J. Comput. Virol. Hacking Tech.* **2019**, *15*, 277–305. [CrossRef]
48. Sheen, S.; Asmitha, K.; Venkatesan, S. R-Sentry: Deception based ransomware detection using file access patterns. *Comput. Electr. Eng.* **2022**, *103*, 108346. [CrossRef]
49. Madani, H.; Ouerdi, N.; Boumesaoud, A.; Azizi, A. Classification of ransomware using different types of neural networks. *Sci. Rep.* **2022**, *12*, 4770. [CrossRef] [PubMed]
50. Arivudainambi, D.; Varun Kumar, K.A.; Visu, P.; Sibi Chakkaravarthy, S. Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance. *Comput. Commun.* **2019**, *147*, 50–57.
51. Kok, S.; Azween, A.; Jhanjhi, N. Evaluation metric for crypto-ransomware detection using machine learning. *J. Inf. Secur. Appl.* **2020**, *55*, 102646. [CrossRef]
52. Masum, M.; Faruk, M.J.H.; Shahriar, H.; Qian, K.; Lo, D.; Adnan, M.I. Ransomware classification and detection with machine learning algorithms. In Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 26–29 January 2022; pp. 0316–0322.
53. Edis, D.; Hayman, T.; Vatsa, A. Understanding Complex Malware. In Proceedings of the 2021 IEEE Integrated STEM Education Conference (ISEC), Princeton, NJ, USA, 13 March 2021; pp. 1–2.
54. Beaman, C.; Barkworth, A.; Akande, T.D.; Hakak, S.; Khan, M.K. Ransomware: Recent advances, analysis, challenges and future research directions. *Comput. Secur.* **2021**, *111*, 102490. [CrossRef] [PubMed]

55. McIntosh, T.; Kayes, A.; Chen, Y.P.P.; Ng, A.; Watters, P. Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–36. [CrossRef]
56. Aboaoja, F.A.; Zainal, A.; Ghaleb, F.A.; Al-rimy, B.A.S.; Eisa, T.A.E.; Elnour, A.A.H. Malware detection issues, challenges, and future directions: A survey. *Appl. Sci.* **2022**, *12*, 8482. [CrossRef]
57. Gorment, N.Z.; Selamat, A.; Cheng, L.K.; Krejcar, O. Machine Learning Algorithm for Malware Detection: Taxonomy, Current Challenges and Future Directions. *IEEE Access* **2023**, 1. [CrossRef]
58. Kapoor, A.; Gupta, A.; Gupta, R.; Tanwar, S.; Sharma, G.; Davidson, I.E. Ransomware detection, avoidance, and mitigation scheme: A review and future directions. *Sustainability* **2021**, *14*, 8. [CrossRef]