




Review

Earlier Decision on Detection of Ransomware Identification: A Comprehensive Systematic Literature Review

Latifa Albshaier , Seetah Almarri  and M. M. Hafizur Rahman 

Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia; 224108483@student.kfu.edu.sa (S.A.); mhr Rahman@kfu.edu.sa (M.M.H.R.)

* Correspondence: 223000803@student.kfu.edu.sa

Abstract: Cybersecurity is normally defined as protecting systems against all kinds of cyberattacks; however, due to the rapid and permanent expansion of technology and digital transformation, the threats are also increasing. One of those new threats is ransomware, which is a form of malware that aims to steal user's money. Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon a large payment. Ransomware is a way of stealing money in which a user's files are encrypted and the decrypted key is held by the attacker until a ransom amount is paid by the victim. This systematic literature review (SLR) highlights recent papers published between 2020 and 2024. This paper examines existing research on early ransomware detection methods, focusing on the signs, frameworks, and techniques used to identify and detect ransomware before it causes harm. By analyzing a wide range of academic papers, industry reports, and case studies, this review categorizes and assesses the effectiveness of different detection methods, including those based on signatures, behavior patterns, and machine learning (ML). It also looks at new trends and innovative strategies in ransomware detection, offering a classification of detection techniques and pointing out the gaps in current research. The findings provide useful insights for cybersecurity professionals and researchers, helping guide future efforts to develop strong and proactive ransomware detection systems. This review emphasizes the need for ongoing improvements in detection technologies to keep up with the constantly changing ransomware threat landscape.

Keywords: cybersecurity; cyberattacks; ransomware; malware



Citation: Albshaier, L.; Almarri, S.; Rahman, M.M.H. Earlier Decision on Detection of Ransomware Identification: A Comprehensive Systematic Literature Review. *Information* **2024**, *15*, 484. <https://doi.org/10.3390/info15080484>

Academic Editor: Rui Zhang

Received: 30 June 2024

Revised: 2 August 2024

Accepted: 11 August 2024

Published: 14 August 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Cybercriminals from all over the world are making money by using ransomware. Ransomware attacks have been increasing since the Internet was created in 1989. The first attack was executed through floppy disks and asked for USD 189 to be sent to a post office in Panama. The attacker was from Ohio and was quickly caught by the FBI because the attack method was simple and there were fewer people using the Internet at that time [1].

Even if victims pay the ransom, they are sometimes still unable to retrieve their data. This could be because the attacker did not keep their promise or because the victim accidentally deleted the decryption key file [2]. In recent years, many ransomware attacks have caused big losses worldwide because they are easy to carry out and cybercriminals can make a lot of money if they succeed [3].

Cybercriminals like ransomware for a few reasons. First, the Internet is widely used around the world, which makes it easier for cybercriminals to attack across borders. For example, someone in Asia can easily target a company in America [2]. Because of the distance and different laws in each country, it is harder for police to detect them. Second, the use of cryptocurrencies like Bitcoin makes it harder for regulators to track down the owner of the money [2]. This means hacking groups have a reliable way to obtain their ransom money.

In the digital age, ransomware attacks have become a serious concern. Numerous people, companies, and governments suffer from them. These attacks occur when malicious software locks up computers or files and demands payment to be unlocked. There are millions of cases reported globally each year, and they occur frequently. For example, in 2021, there was a huge increase in ransomware attacks, almost over 150 percent, affecting many different sectors like healthcare, finance, and government [4]. Recently, there has been a big increase in ransomware attacks. These attacks are happening more often and are becoming more clever, impacting a wide range of organizations worldwide including governments, corporations, and common people. It is really important to catch these attacks early. Much of the harm they inflict can be stopped if we find them in time. This means organizations might not lose as much data or money and they can keep their operations running smoothly. Catching the attacks early also helps to stop them from spreading through the whole network. This is very important for keeping important information safe, especially in areas like healthcare and finance where trust is a priority.

Detecting ransomware attacks early is crucial to prevent them from causing too much damage. If we detect them early, we can prevent them from locking up more files and spreading to other computers [2–4]. This helps to reduce the money and time lost by people and businesses. It is also crucial for protecting important systems like energy, transportation, and communication networks. However, detecting ransomware attacks is difficult as cybercriminals keep changing their methods to avoid detection. They use tricky techniques like changing their malware to look different or taking advantage of new weaknesses and vulnerabilities in systems [3]. Additionally, it can be difficult to distinguish between ransomware activities and legitimate software behaviors, especially in big networks where a lot of abnormal activities happen most of the time. Table 1 [5] defines major ransomware attacks from 2020 to 2023 and involves listing several significant incidents along with key details such as the targeted organization, the date of the attack, the ransomware used, and the impact of the attack.

Table 1. Major ransomware attacks from 2020 to 2023.

Year	Targeted Organization	Ransomware Used	Impact of Attack
2020	University of California	NetWalker	1.14 million paid and academic data encrypted
2020	Garmin	WastedLocker	Major service outage and 10 million reportedly paid
2020	Software AG	Clop	Data stolen and leaked, and 20 million demanded
2021	Colonial Pipeline	DarkSide	Fuel supply disruption and 4.4 million paid
2021	JBS Foods (one of the world's largest meat processors)	REvil/Sodinokibi	Global meat supply affected and 11 million paid
2021	Kaseya	REvil/Sodinokibi	Managed Service Provider and their clients affected globally
2022	Costa Rica Government	Conti	National healthcare and finance systems disrupted
2022	Kronos	Unknown	Payroll and HR services for numerous companies disrupted
2023	Horizon	Healthcare	Encrypting patient data and disrupting medical services, highlighting the vulnerability of the healthcare sector

Early detection of ransomware is crucial in minimizing the damage caused by these attacks. By identifying ransomware threats early, organizations can reduce the potential data loss and operational disruptions. Early detection allows for swift and effective response measures, such as isolating affected systems and initiating recovery protocols

before the ransomware can spread further. This proactive approach is essential in limiting the financial and operational impact, preserving data integrity, and maintaining business continuity. Additionally, early detection enhances the organization's ability to respond effectively, mitigating the overall risk associated with ransomware attacks.

Ransomware attacks pose significant recovery challenges for affected organizations. The primary difficulty lies in data recovery post-attack, which is often complex and time-consuming. Organizations must restore encrypted or corrupted data, which can be particularly challenging if backups are insufficient or compromised. The financial burden associated with recovery efforts is substantial, encompassing costs related to downtime, lost productivity, and potential ransom payments. Furthermore, the impact on business continuity can be severe, as operations may be disrupted for extended periods, leading to potential loss of revenue and damage to the organization's reputation.

Table 2 [6] below provides a comprehensive overview of ransomware statistics and insights as of 2024. It highlights the global impact of ransomware attacks and the financial and operational challenges associated. The data include trends over recent years, common entry points for ransomware, and the geographic distribution of attacks, offering a detailed snapshot of the ransomware threat landscape.

Table 2. Comprehensive ransomware statistics and insights (2024).

Statistic	Value
Global ransomware attacks (2021)	623.3 million
Global ransomware attacks (H1 2022)	236.1 million
Drop in ransomware attacks (2022 vs. 2021)	23%
Percentage of cyber crimes attributed to ransomware (2022)	20%
Ransomware attributed to Windows-based executables	93%
Common entry point for ransomware	Phishing
US share of global ransomware attacks	47%
Manufacturing industry attacks attributed to ransomware (2021)	Most common
Ransomware attacks that fail or result in zero losses	90%
Average ransomware payment (2021)	USD 570,000
Increase in average ransomware payment (2020 to 2021)	82%
REvil ransomware group's share of attacks (2021)	37%
Top affected countries (ransomware attacks)	Israel, South Korea, Vietnam, China, Singapore, India, Kazakhstan, Philippines, Iran, UK
Top affected organizations' countries (ransomware attacks)	USA, Italy, Australia, Brazil, Germany
Number of ransomware families identified	130
Percentage of ransomware attacks due to phishing	41%
Estimated global successful ransomware attacks (May 2021–June 2022)	3640
Organizations expecting ransomware attack (Canada)	65%
Largest ransom paid (JBS, 2021)	USD 11 million
Ransomware incidents reported to FBI (Jan–July 2021)	2084 incidents, USD 16.8 million losses
Predicted frequency of ransomware attacks by 2031	Every 2 s
Healthcare sector losses due to ransomware (US, 2021)	USD 7.8 billion

The contributions of this paper can be summarized in four key points, as follows:

1. Provides a detailed overview of how ransomware has developed over time, focusing on its mechanisms, types, and the vectors used for attacks.
2. Conducts a comprehensive review of the current approaches in ransomware detection. In addition, emphasizes the techniques and methods used at various stages of detection.
3. Highlights how ML is being employed to improve ransomware detection.
4. Identifies the gaps in current research and suggests potential areas for future investigations to enhance the cybersecurity field's defense against ransomware attacks.

The current literature and practices in ransomware detection are not always efficient. Traditional signature-based detection methods often fail to detect new types of ransomware. Additionally, heuristic and behavior-based approaches have high false-positive rates. These approaches can miss the activities that may indicate ransomware leaving systems vulnerable to attacks. Therefore, we really need new and good detection strategies that can effectively distinguish between ransomware behaviors and legitimate networks activities. This will help keep individuals, businesses, and important systems safe from ransomware attacks. Our paper is all about understanding these challenges and looking for solutions that can help us stay a step ahead of these tricky ransomware attacks.

In our study, we have a few main goals. We are doing a deep dive into lots of research and articles about ransomware. We want to focus on two big things: how to quickly detect ransomware and how to figure out what kind of ransomware it is. Our main goal is to emphasize the need for ongoing improvements in detection technologies to keep up with the constantly changing ransomware threat landscape. We will check if there are any new ideas or tools that seem promising. Also, we are going to look for any gaps or limitations in the research that has been carried out so far. Maybe there are some areas that have not been explored much or ways of detecting ransomware that could be improved. By the end of our review, we hope to have a clearer picture of what works best for detecting ransomware fast and effectively.

This paper delves into the topic of ransomware and aims to provide a thorough understanding and analysis of this significant cybersecurity threat. The paper begins with Section 2, where we explain how we chose the studies and articles that we reviewed with the details of the methods we used to search for relevant literature. Section 3 delves into the background of ransomware, reviewing its types, attack vectors, encryption methods, and detection challenges, and exploring the role of AI in combating such threats. It also addresses preventive measures, legal considerations, and future trends. The discussion in Section 4 focuses on indicators of ransomware incidents, attack frameworks, behavior patterns, and the efficacy of current detection techniques, emerging trends and avoidance strategies. Real-world ransomware incidents are discussed in Section 5, which gives practical insights into the impact of these attacks. Section 6 reviews related studies, providing a critical analysis of the existing literature and identifying research gaps. Open challenges and limitations in ransomware detection and prevention are explored in Section 7. Future directions for research and development are proposed in Section 8. The paper concludes in Section 9, which underscores the importance of enhanced detection capabilities and summarizes the findings of this paper.

2. Papers Selection for Literature Review

2.1. Methodology

The methodology used in this research is a systematic literature review (SLR). SLR is used to present the information in a clear and organized way. It will help in identifying the limitations and research gaps that exist in current studies. It will also help in the determination of the research future direction. Furthermore, the PRISMA flow diagram was used to summarize steps that were followed by researchers during the paper selection process. Identification, screening, and included are the main phases followed in the PRISMA flow diagram. In addition, the research targeted studies that were published between 2020 and 2024. In the identification phase, duplicated and ineligible records were

removed, as well as records after filtering the year and source type—whether journal, book, or conference. In the screening phase, additional records were excluded for other reasons like relevance to the research topic or the length of the paper. Finally, the included phase contains only the papers that will be included in the research.

2.2. Search String

The following search string was used to optimize the quality of the search results: (“Detection”) AND (“Ransomware” OR “ransomware identification” OR “identify Ransomware”). It consists of Boolean operators like “AND” and “OR” between the key words. These operators will greatly help in broadening, narrowing, and adjusting the search string.

2.3. Data Sources

The search string was applied in two databases, which are Google Scholar and Saudi Digital Library.

2.4. Screening Process

In the first stage, we filtered the papers based on their titles by searching the database using the search string, looking at whether the title related to our topic or not. If there were difficulties in evaluating the paper’s topic, we added an extra screening stage, which involved reading the abstract of that paper. Figure 1 shows the PRISMA flow diagram, which presents the selection process of the papers.

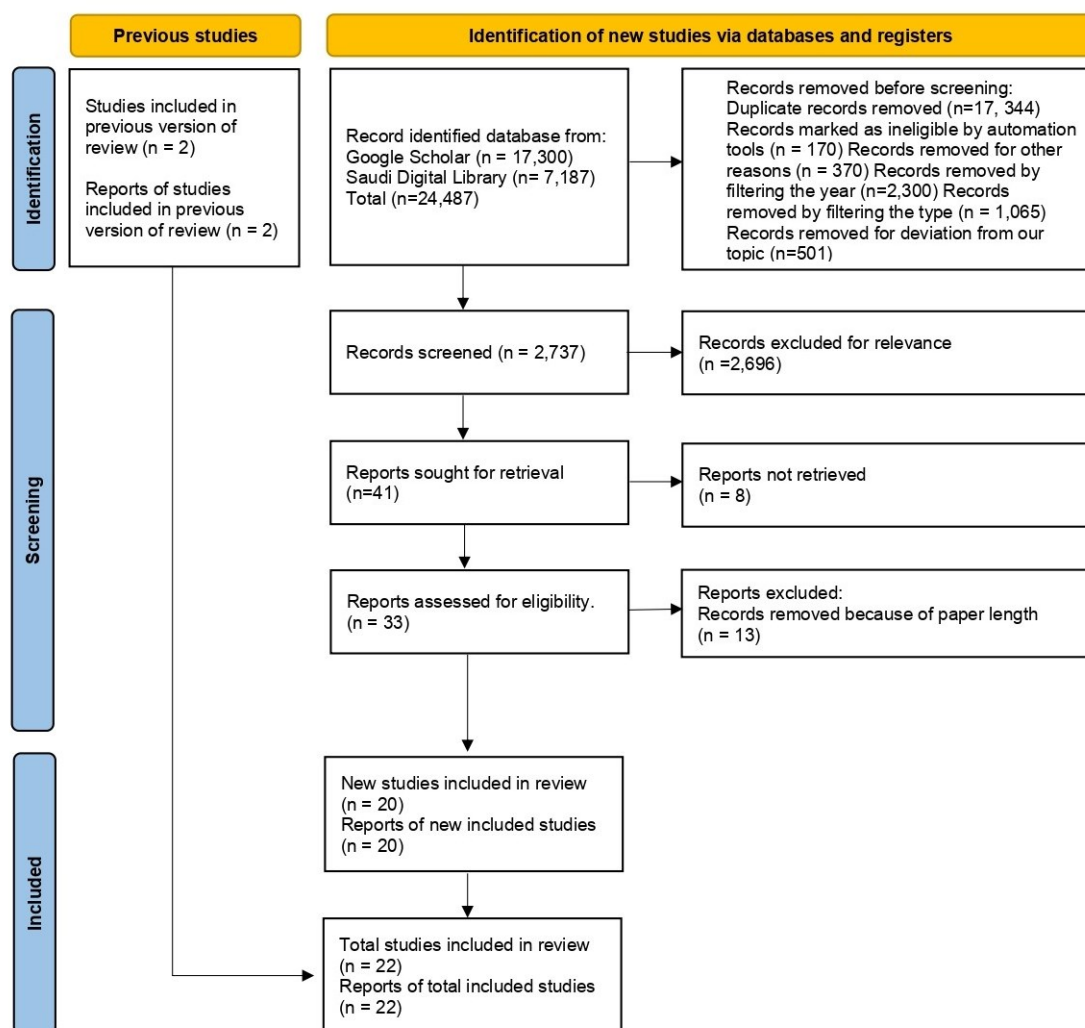


Figure 1. Paper selection for literature review using PRISMA [7,8].

3. Background

3.1. Overview of Ransomware Attacks

In recent years, ransomware has spread quickly, affecting individuals, organizations, and governments. Ransomware is malicious software that aims to prevent access to victims' data or computer devices by encrypting their files and then asking them to pay a ransom to access or decrypt them, which is paid using cryptocurrency to avoid tracking them [9]. Figure 2 presents the total values received by ransomware attackers in the last 5 years.

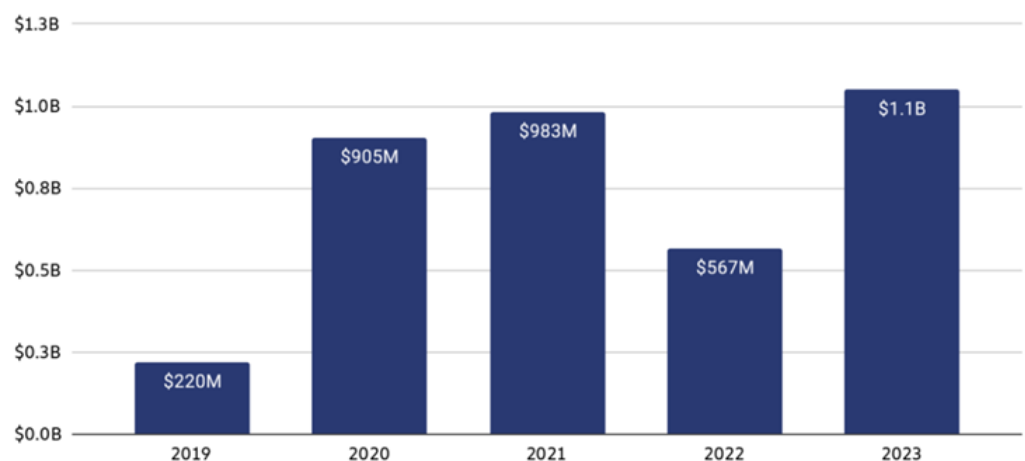


Figure 2. Total values received by ransomware attackers in the last 5 years [10].

The ransomware process consists of five stages, which are infection, downloading malicious files, encryption, demanding payment, and decryption. The infection happens through phishing emails, attachments with malicious code, or malicious websites. Once it gains access to the victim's device, it quickly searches for valuable files to encrypt. The attackers use robust encryption algorithms to make the victim's files inaccessible and unreadable. Thus, the victims are forced to pay the ransom to gain access to their files by using the decryption key from the attacker after payment [9]. Figure 3 shows how the ransomware works.



Figure 3. How the ransomware attacks work [11].

Ransomware can significantly impact individuals, organizations, and governments around the world. On the individual side, there are risks related to the theft of personal data, such as usernames, passwords, ID numbers, or financial data such as banking information. On the organization side, there are risks related to severe disruptions in operations, resulting in stopping work, huge financial losses, or even damage to the organization's reputation. On the government side, there are critical risks that some vital services will stop working, such as healthcare systems, transportation services, and some financial systems, which

may affect the general interest of citizens. Also, efforts to recover and repair the loss of these data may be expensive. In many cases, paying the ransom is chosen by the victims to reduce the risk of losing such data [9]. Early detection plays a significant role in combating ransomware attacks and reducing their impacts. Attackers may target organizations of different types and sizes, including government agencies, educational institutions, and health institutions. Recent statistics show that the expected global cost of ransomware may reach USD 265 billion by 2031 [12].

3.2. Types of Ransomware

Ransomware attacks come in different forms, each with their own way of disrupting the victim's access to their data, as shown in Figure 4. Below, we explain the main types based on their methods [3,13–16]:

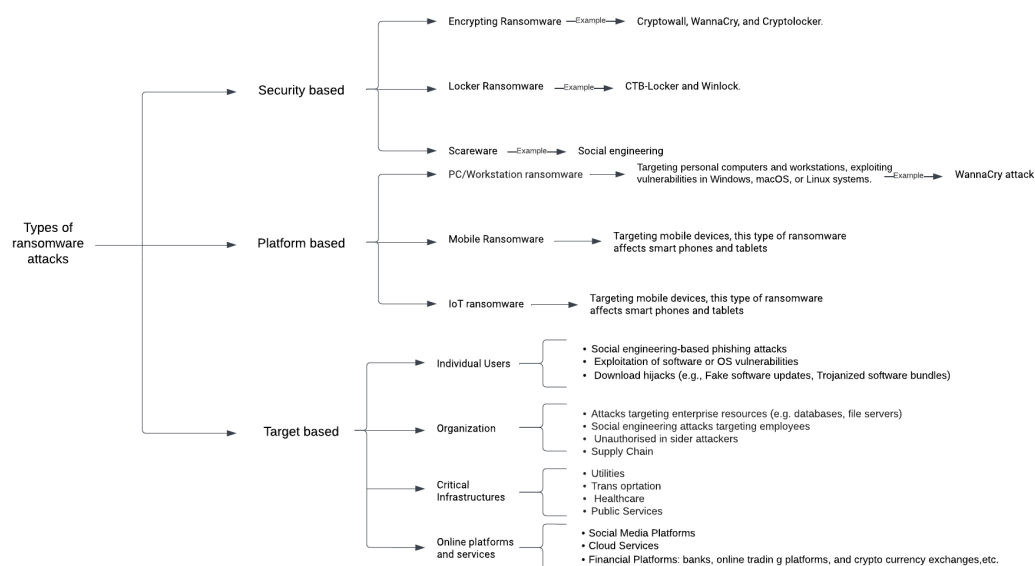


Figure 4. Types of ransomware attacks.

Ransomware classification on malware characteristics:

- **Encrypting Ransomware:** This type is the most common and involves encrypting the victim's files with a strong encryption algorithm, making them inaccessible without a decryption key. Notable examples include Cryptowall, WannaCry, and Cryptolocker. The victim can see the files but cannot open them unless they pay the ransom to obtain the decryption key.
- **Non-Encrypting Ransomware:** Also known as locker ransomware, this type locks you out of your entire device, not just specific files. The data remain unharmed but inaccessible. To regain access, the victim must pay a ransom. Examples include CTB-Locker and Winlock.
- **Scareware:** also known as fake antivirus, scareware tries to convince the victim that their device is infected by showing a false warning and then asking for payment to access the full version of the software to remove or mitigate the risk. Scareware typically uses social engineering methods rather than encrypting the files or devices to scare the victims and then force them to pay.

Ransomware classification based on platforms:

- **PC/Workstation ransomware:** This type targets personal computers and workstations, exploiting vulnerabilities in Windows, macOS, or Linux systems. Examples include the infamous WannaCry attack, which specifically targeted Windows systems using a network exploit.

- **Mobile ransomware:** Targeting mobile devices, this type of ransomware affects smartphones and tablets, primarily through malicious apps or compromised websites. Android devices are more frequently targeted due to the ease of installing apps from third-party sources.
- **IoT ransomware:** IoT devices, such as smart home gadgets and industrial sensors, are increasingly being targeted due to their poor security measures. Attacks on these devices can lead to significant disruptions, especially when they affect critical infrastructure.

Ransomware classification based on targets:

- **Individual users:** This group is often the easiest target due to less stringent security practices. Attackers exploit this by using deceptive emails or malicious websites to initiate ransomware infections.
- **Enterprises:** Businesses are targeted for their valuable data and deeper financial resources. Attacks may involve sophisticated strategies to infiltrate network defenses and encrypt critical business data.
- **Government and critical infrastructure:** Attacks on government systems and critical infrastructure aim to cause significant disruption, often impacting national security, healthcare, and essential services.
- **Online Services:** Cloud services and online platforms, such as social media and banking services, are also targeted, with attackers aiming to encrypt or steal large amounts of data to demand higher ransoms.

3.3. Ransomware Attack Vectors

Ransomware methods and types have varied, as attackers use different techniques to infect the victim's device. Sufficient knowledge of the various attack vectors used by attackers may help individuals, organizations, and governments predict and take suitable preventive measures on time. Below are some attack vectors used by attackers:

Phishing emails: Phishing emails are the most common vector used by attackers. Fraudulent emails are sent to the victim that appear to be from a reliable and well-known source, such as some well-known organization or individual. These messages contain PDF attachments, images, voice mail, or malicious links. Once clicked, some malware is installed, which aims to search for valuable files and encrypt them. Therefore, users should be careful and verify the sender before opening the content of the message, and not open suspicious links that may appear to be from an unknown source [17].

Malicious advertisements: The attackers use fake advertisements to attract the victims by injecting malicious code into legitimate advertisements that will contribute to spreading ransomware very quickly. When the victims click on those ads, the ransomware will be activated and installed. Having up-to-date antivirus software will protect against different ransomware and mitigate its potential risk [16].

Social engineering: Attackers use various social engineering techniques, such as luring the victim into clicking on suspicious links, downloading malicious files, or updating fake software that appears to be legitimate. Victims may also receive emails or text messages stating the urgent need to do something by clicking on electronic links or attached files. Therefore, individuals, companies, and governments must have sufficient awareness of the different methods used by attackers [18].

Exploiting vulnerabilities: Attackers aim to spread ransomware by exploiting operating system, program, or network device vulnerabilities. They mostly target un-updated systems by exploiting vulnerabilities, installing ransomware, and then asking for a ransom to be paid. Regularly updating the operating system and software will prevent different types of attacks from occurring. Also, implementing robust countermeasures and applying best-practice scenarios for managing the vulnerabilities will mitigate the risk of ransomware [19].

3.4. Evolution of Ransomware

The evolution of ransomware attacks can be traced back to the late 1980s when the first known attack, the AIDS Trojan, was distributed via floppy disks and demanded a payment for a software lease [5]. Over the years, ransomware has become more sophisticated. In the early 2000s, attackers began using more advanced encryption techniques to lock files, making it nearly impossible for victims to regain access without the decryption key [20]. A significant shift occurred in the 2010s with the rise of cryptocurrency, which provided a secure and anonymous payment method, making ransomware attacks more appealing to criminals. High-profile attacks like WannaCry in 2017 highlighted the global threat of ransomware, prompting improvements in cybersecurity defenses. Today, ransomware attacks are increasingly targeted, aiming at businesses and governments for higher ransom demands and more significant disruption.

Below, Table 3 [5,14,20] summarizes the evolution of ransomware attacks over the years.

Table 3. Evolution of ransomware.

Year	Key Developments	Impact
1980s	Introduction of AIDS Trojan via floppy disks	First known ransomware; limited in scope.
2000s	Use of advanced encryption to lock files	Increased difficulty in decrypting files without payment.
2010s	Rise of cryptocurrency; notable attacks like WannaCry	Global spread; significant financial and operational impacts.
2020s	Targeted attacks on businesses and governments	Larger ransoms and higher stakes in disruptions.

Ransomware attacks have transformed dramatically since their first appearance in 1989. Table 4 traces the progression of these malicious software attacks, highlighting key versions and their distinctive tactics. Each row illustrates the evolution from basic encryption demands to complex strategies involving data theft and high-profile targeting. This summary captures the ongoing challenge that ransomware poses to individuals and organizations, emphasizing the need for evolving security measures [5,13,14,16,20–23].

Table 4. Timeline of ransomware evolution.

Year	Notable Ransomware	Main Features	Impact
1989	AIDS Trojan	First ransomware	Asked for payment through the mail; locked file names, not the files themselves.
2005	Gpcode	Uses weak RSA encryption	Early use of asymmetric encryption but with weak key sizes, allowing decryption without paying.
2013	CryptoLocker	Strong RSA-2048 encryption	Started using very strong encryption, causing big losses and marking the start of modern ransomware.
2015	Locky, TeslaCrypt	Widespread use, targeted various file types	Advanced on previous attacks by improving encryption strength and targeting a wider array of file types; became highly profitable.
2016	Petya, NotPetya	Disk encryption and wiping capabilities	Innovated by encrypting entire disks and spreading within networks; NotPetya masqueraded as ransomware but primarily caused disruption.

Table 4. Cont.

Year	Notable Ransomware	Main Features	Impact
2017	WannaCry, Bad Rabbit	Exploited EternalBlue vulnerability	Caused global panic due to rapid spread through networks by exploiting unpatched Windows Server Message Block (SMB) protocol vulnerabilities—SMB is a network protocol used for file sharing; prompted urgent global security updates.
2019	Maze	Double extortion technique	Started the trend of stealing data before encrypting devices, threatening to release the data if the ransom was not paid.
2020	Sodinokibi	Targeted big companies, used a partner model	Aimed at large, important targets and expanded the idea of ransomware-as-a-service, allowing more attackers to participate.
2021	DarkSide, REvil	Hit supply chains and crucial services	Major incidents like the Colonial Pipeline attack highlighted the threat to critical infrastructure and supply chains.
2022	LockBit	Automated and sophisticated operations	Introduced automated attack systems to maximize impact and efficiency, further refining the ransomware-as-a-service model.

3.5. Ransomware Encryption Techniques

Ransomware uses several ways to encrypt the victim's files and make them inaccessible. Understanding these ways is important to detecting and responding to ransomware effectively. This section presents encryption techniques used by ransomware, such as symmetric and asymmetric encryption algorithms.

1. Symmetric encryption: an encryption method that uses only a single key in the encrypting and decryption processes [24]. Ransomware typically follows these phases in symmetric encryption:
 - Generate the key: A unique key is generated to be used in symmetric encryption.
 - Encrypt the files: The victim's files are encrypted by ransomware using a single secret key. Ransomware targets the victim's sensitive information and files, such as documents, photos, and videos.
 - Protect the key: To prevent key recovery by the victim, ransomware encrypts it until payment is made. Then, the encrypted key is saved on the attacker's servers.
 - Advanced Encryption Standard (AES): AES is one example of a symmetric encryption algorithm. It is secure and cannot be cracked easily. The key length used in the AES algorithm to encrypt victims' files is 128-, 192-, or 256-bit [25].
2. Asymmetric encryption: an encryption method that uses two different keys, known as the public key and the private key, in the encrypting and decryption processes [24]. Ransomware typically follows these phases in asymmetric encryption:
 - Generate the keys: a pair of keys is generated to be used in asymmetric encryption.
 - Encrypt the file using the public key: the victim's files are encrypted using the public key.
 - Protect the private key: the private key is stored on the attacker's servers until payment is made by the victim.
 - Examples of asymmetric encryption algorithms:
 - RSA encryption: RSA is one example of an asymmetric encryption algorithm. It contains two keys, which are the public key and the private key. The public key is used for the encryption algorithm, which is used to encrypt the victim's files,

and the private key is used for the decryption algorithm, which is used for the decryption and stored remotely on the attacker's servers [26].

Elliptic Curve Cryptography (ECC): ECC is another example of an asymmetric encryption algorithm. ECC key length is shorter than RSA and more secure. As with RSA, ECC consists of two keys, which are public and private—one for encrypting the files and another for decrypting [27].

Understanding ransomware encryption methods contributes to early detection, mitigation, analysis, and response to ransomware. Thus, knowing the attacker's methods will help to develop effective countermeasures, including different detection algorithms and systems such as signature-based detection systems. In addition, backup, user education, and antivirus programs are important to protect the victim and mitigate the impact of ransomware.

3.6. Signs of a Ransomware Attack

Predetection of ransomware attacks is very important to reduce the impact of ransomware and prevent revealing or losing data. This section explains different signs that may indicate that the device has been hacked by ransomware.

Unusual activity: Changes in file names that were not made by the victim or strange file extensions that cannot be recognized [28].

Prevent access to files: If the victim is prevented from accessing certain files, this may be a sign of a ransomware attack [29].

Ransom notes: If a specific device is compromised by ransomware, some notes may be left for the victim. It may consist of pop-up messages or text files in which a ransom is demanded or the victim is threatened. These notes are called "README.txt" [30].

Slow system performance: A severe slowdown in the device's performance that did not previously exist. This may also be an indication that a device has been hacked by malicious ransomware as a lot of malicious code is downloaded by the ransomware, which consumes a lot of system resources [31].

Sudden system restart: If the device is suddenly turned off or restarted without the user's request, this may indicate a malfunction, or it may be an indication that the system has been infected by a ransomware attack [31].

Turning off anti-virus software: Ransomware disables anti-virus or other security systems so they cannot be detected [31].

Suspicious connection patterns on the network: Ransomware may create suspicious or unknown connection patterns on the network, such as connecting to unknown IP addresses. Therefore, network traffic must be monitored to detect any unknown or suspicious connections [31].

If unusual or suspicious movement is observed on your device, this may be an indicator or evidence of the presence of malicious ransomware. To protect your information, you must isolate the infected device and then contact cybersecurity specialists to solve this problem.

3.7. Challenges in Early Detection of Ransomware

The evolving nature of ransomware attacks and the modern techniques used by attackers create many challenges that hinder early detection. This section reviews the most important challenges that may be faced in the early detection of various ransomware.

Polymorphic malware: Ransomware tends to change its forms, techniques, and signatures with each iteration or attack, making it difficult to detect using traditional methods or using anti-virus programs and other security systems. As a result, it has become extremely difficult to detect them using traditional methods [14].

Evasion techniques: Recently, attackers have been using new techniques, such as evasion techniques, to bypass security controls and evade dynamic analysis systems. These technologies use encryption algorithms to hide malicious payloads, obfuscate to bypass early detection, and make analysis more difficult [32].

Increasing complexity: Attackers increase the complexity of their attacks by constantly developing their skills, techniques, methods, and strategies to bypass detection programs and various security systems. Therefore, users must have the latest versions of anti-virus software to detect zero-day attacks, and experts must develop their skills and techniques to keep pace with this development [33].

Encrypted traffic: The use of encrypted communication channels by attackers to secure their communications is one of the most important challenges hindering early detection. Monitoring encrypted traffic by security experts to distinguish between legitimate and malicious traffic is an extremely difficult task because it requires a lot of time, effort, and computational resources. Moreover, it requires advanced technologies such as analyzing traffic patterns, using ML algorithms to identify legitimate and suspicious activities according to specific criteria, and monitoring the behavior of the network [34].

3.8. The Role of Artificial Intelligence to Improve Ransomware Detection

Artificial intelligence (AI) technologies have revolutionized and helped develop many fields—most notably, cybersecurity—as they have been able to improve and develop methods for early detection and prediction of ransomware attacks. AI has three ways to detect ransomware: ML, deep learning, and artificial neural networks. Some models use one of them and others use a hybrid of them to detect ransomware effectively. AI techniques use static and dynamic analysis, along with ransomware behavioral analysis, to better detect ransomware and prevent its attacks, where large databases are used and appropriate decisions are made based on the analysis of this huge amount of data. Algorithms in ML learn from past attacks and perform some analysis to detect new attacks with the same patterns or behaviors. On the other hand, DL analyzes a huge amount of data with the help of neural networks to identify ransomware attacks. All these methods are efficient and reliable in detecting and preventing ransomware attacks [20]. Figure 5 represents how AI can improve ransomware detection and illustrates the relationships and roles of AI, ML, neural networks, and DL in the context of ransomware detection. AI, being the broadest field, encompasses various techniques, including static and dynamic analysis, and behavioral analysis, to enhance ransomware detection and prevention. Within AI, ML focuses on creating intelligent machines capable of learning from data, utilizing both supervised and unsupervised learning methods; these algorithms analyze past attack patterns to identify new threats. Neural networks, forming a subset of ML, further specialize in pattern recognition tasks. DL, a subset of ML methods, leverages artificial neural networks, such as CNNs and RNNs, to process vast amounts of data. DL is particularly effective in identifying ransomware attacks by analyzing large datasets with the aid of neural networks. Each layer in the diagram highlights the role these technologies play in the detection and mitigation of ransomware, emphasizing their interconnected nature and hierarchical structure within the broader field of AI.

1. Machine learning: ML models help improve ransomware detection by depending on features or behavior patterns. This technique focuses on collecting a huge amount of data that contain both malicious and benign samples, and then training the ML model to classify the new sample as benign or malicious based on different features that were extracted from the dataset, as shown in Figure 6. The advantage of ML is being able to detect new or unknown ransomware that does not match existing patterns or signatures. However, this technique has fewer false positives compared with heuristic-based and signature-based detection because it depends on detecting actual behavior patterns rather than predefined rules [9].

Machine learning detection algorithms: Different ML algorithms are employed to detect ransomware attacks, such as support vector machines, k-nearest neighbors, random forests, decision trees, logistic regression, and XGBoost. Table 5 below summarizes all these algorithms.

Advanced algorithms are utilized to monitor behavior and identify patterns, which help identify suspicious cases of different forms of ransomware [20].

Table 5. Machine learning detection algorithms.

Algorithm	Description
Support vector machines	Reliable ML method that can be used to detect and classify ransomware. It can be trained by different features to differentiate between goodware and ransomware, like network traffic, the behavior of the file, and system calls. It can be more beneficial when the data are non-linearly separable and high-dimensional [36].
Decision trees	It is simple and can be utilized in classification to detect ransomware. The data are divided into subsets based on feature values to create a tree structure for decision-making. It can be trained based on different features like system calls, network traffic, and file modification [37].
Random forests	An extension of decision trees that reduce overfitting and enhance performance. Data and features are selected randomly to create multi-decision trees. It can handle high-dimensional data, but these could be difficult to interpret and computationally demanding [38].
k-nearest neighbors	It is simple and operated by selecting the nearest points of data using the training set. Then, predicting the input label based on the common one among those k-neighbors. It is effective and can be used in different applications. Also, the primary use of this algorithm is in the tasks of regression and classification [39].
Extreme Gradient Boosting “XGBoost”	It is a powerful and popular algorithm for the tasks of gradient-boosting. It combines two algorithms, which are decision trees and gradient boosting, to come up with a more accurate model and enhances the scalability by handling large and complex datasets and extracting relevant features [40].
Logistic regression	It is used in the binary tasks of classification where the result could be one of the two possible outputs. It can be trained to discover the optimal parameters that maximize the possibility of the training data. It can be organized to prevent overfitting. It is simple, interpretable, and can be used with small datasets [41].

Behavioral analysis: Using ML models to analyze all patterns and behaviors of operations, files, and network activities to identify suspicious behaviors that may indicate a ransomware intrusion. Such models can detect a deviation from usual activity when any suspicious activity is detected [42].

Anomaly detection: Develop models based on ML algorithms that can distinguish between patterns or legitimate and malicious activities in the behavior of a network or system. Furthermore, malicious behavior is flagged as an indication of a ransomware attack [43].

Signature-based detection: Ransomware signatures can be identified by training ML models to examine a user’s network connections, files, and system logs. Therefore, alarms are sent when the results match the characteristics marked as ransomware [44].
Data mining and threat intelligence: ML techniques are applied to large datasets to analyze and extract useful insights from these data. Also, the characteristics of legitimate patterns and suspicious or harmful patterns are analyzed. Thus, countermeasures and preventive measures are developed against this type of attack [45].

2. Deep learning: Deep learning (DL) techniques are proposed to solve the restrictions of traditional ransomware detection methods, which help to improve reliability, accuracy, and performance. It is suitable for dealing with an unorganized dataset that requires minimal or no human intervention because of its self-learning capabilities. They operate particularly well at identifying text- and image-based ransomware because of how well they can categorize voice, text, and image data. DL methods can be problematic for general-purpose applications, especially those with tiny datasets or sizes, as they require a large quantity of data to train them. High processing power requirements and trouble adjusting to real-world datasets are two further issues with DL [46].
3. Artificial neural networks: Artificial neural network techniques are used in a broad range, which makes them suitable for detecting many kinds and variations of ran-

software data, including variants that target images and text. Because of their capacity for ongoing learning, neural networks make an ideal choice for recognizing zero-day attacks and adjusting to new ransomware data. Neural networks can detect many types of ransomware data and adjust to new threats due to their versatility. However, because of the black-box nature of the technology and their reliance on hardware, these techniques can be susceptible to data dependencies, making it more difficult for human analysts to keep an eye on data processing and spot anomalies [47].

Successful case studies:

- **Ransomware behavioral analysis:** One successful study used ML as a defense mechanism against ransomware attacks. The analysis considered seven ransomware and seven benign software samples to distinguish between benign and malicious software with low false negative and false positive rates. Values from different ransomware, such as Dynamic Link Libraries (DLLs), were extracted in this study. DLLs are a type of file used in Windows operating systems to hold multiple codes and procedures that are shared among various applications. Essentially, DLLs allow programs to use functionalities that are stored in separate files rather than having to include them within the program itself. This not only helps in saving space but also promotes code reuse and modular programming. When a program runs, it can call upon a DLL file to perform certain functions, which helps in efficient memory usage and reduces the application's load time because it only loads the necessary parts. DLLs are crucial for the operating system to manage shared resources effectively, enabling smoother and more performance-efficient operation of software on your computer. Early detection of ransomware attacks and alerting the user about the existing threat are considered a main feature of this proposed system [48].
- **Anomaly detection in network traffic:** In [49], AI algorithms and ML techniques were used to detect anomalies by analyzing network traffic. This process is performed by labeling normal and abnormal features and utilizing ML to detect the unusual status of the network. The system succeeded in isolating harmful activities, allowing early detection, and taking the necessary preventive measures.
- **Signature-based ransomware detection:** ML models were used in some systems that aim to detect ransomware signatures. Ransomware tends to constantly change its signatures to prevent detection by traditional detection techniques. ML models are constantly updated to identify new forms of ransomware, which allows for early detection and appropriate decision-making [19].

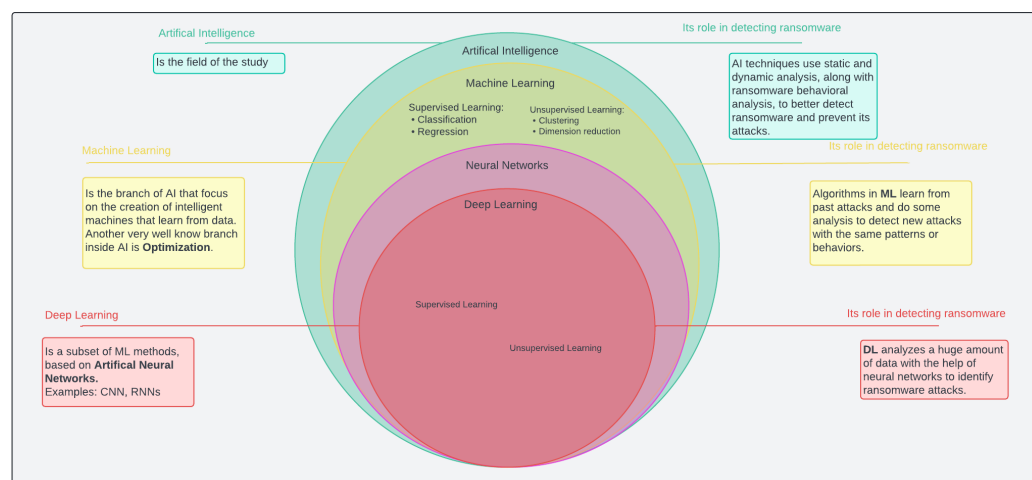


Figure 5. Artificial intelligence techniques [35].

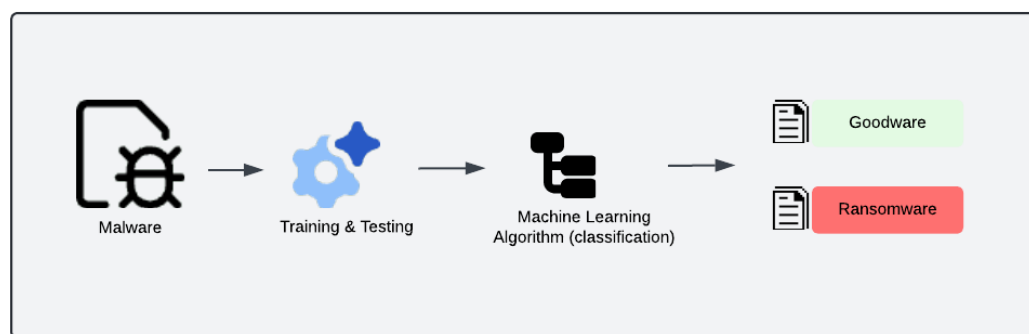


Figure 6. Machine learning: detection algorithm.

3.9. Preventive Measures and Best Practices

Individuals, organizations, and governments can reduce the risk of ransomware by taking some important preventive measures, such as following cyber-hygiene practices, performing regular backups, and keeping antivirus software up to date. Several preventive measures against ransomware are reviewed in this section.

1. **Cybersecurity hygiene:** Cybersecurity hygiene is applied in several steps, the most important of which are as follows:
 - **Employee education and awareness:** Increasing individuals' awareness of the dangers of ransomware and educating them on cybersecurity best practices, such as detecting suspicious messages and avoiding downloading files or programs from suspicious or unreliable links [13].
 - **Strong password policies:** Forcing the user to use strong and complex passwords. In addition, it is necessary to change the passwords regularly and use password management programs for better management and security [50].
 - **Multi-factor authentication (MFA):** Using multi-layer protection to safeguard sensitive data or files such as passwords, voice recognition, and facial recognition [51].
2. **Regular backups:** Regular backups of sensitive data are made to mitigate the damage in case hackers gain access to the original data [52].
3. **Timely updates:** Ensure that all programs and operating systems are updated to the latest version and allow automatic updating of these preventive programs once connected to the Internet [22].
4. **Network segmentation and access Control:** Applying the principle of network segmentation to isolate important data from other data. In addition, implementing the least privilege principle by granting privileges to users as needed to perform tasks [53].

3.10. Regulatory and Legal Considerations

Given the negative impact of ransomware on many individuals, organizations, and governments, many regulatory and legal frameworks have been developed to limit or mitigate its impact. These laws and frameworks vary from country to country, but there are common aspects regarding ransomware detection and response that will be discussed in this section.

Ransomware criminalization: Ransomware attacks or spreading are considered a crime punishable by law in many countries. This is because it results in unauthorized access to sensitive or private data and blackmailing the victim by paying money to recover these data [54].

Data privacy protection laws: Many countries impose strict laws and regulations on organizations to protect the data privacy of their employees and personal information. It asks them to take specific measures to ensure the protection and safety of these data from unauthorized access by ransomware attackers. Once the damage or violation occurs,

the organization is legally responsible for compensating the individual affected by this violation [55].

International cooperation against ransomware: Ransomware targets many victims and is implemented in different countries worldwide. Therefore, efforts are unified through international cooperation and agreements that target various types of attacks, especially ransomware attacks. Also, these agreements aim to facilitate exchanging information, searching for criminals, deporting them, and helping victims, thus accelerating the detection and response process [56].

These regulatory and legal regulations have greatly assisted in detecting and responding directly to ransomware. Also, international cooperation between organizations has helped to enhance the role of cybersecurity and develop effective preventive techniques to detect, mitigate, and respond to ransomware attacks.

3.11. Future Trends in Ransomware

In this section, the future trends in ransomware development will be discussed.

Increased complexity: The complexity of ransomware increases as technology continues to evolve, as attackers use these advanced technologies to carry out ransomware attacks, such as using AI techniques and various encryption algorithms to avoid detection and observation until the victim's data are seized [12].

Targeted attacks: Attackers often conduct reconnaissance to identify their targets, design their attacks, and then carry out the attacks. Usually, governments are targeted to leak sensitive data, large organizations, or specific individuals to obtain greater advantages or benefits [57].

Exploitation of emerging technologies: With technological advancements, attackers aim to exploit the vulnerabilities in new techniques like IoT devices or cloud services [58].

4. Comprehensive Analysis of Ransomware: Detection, Prevention, and Trends

4.1. Indicators of Potential Ransomware Incidence

Certain behavioral patterns may serve as indicators that a system is under a ransomware attack. Recognizing these signs early can be crucial in identifying and mitigating ransomware incidents. The following list outlines several key indicators [59]:

- Excessive File Operations: A noticeable rise in file access activities. For example, opening or attempting to open a large number of files in a short time frame. This may indicate an ongoing ransomware attack.
- Altered Input/Output Behavior: The input and output patterns where the structure and volume of data being processed significantly change.
- High Volume of Write Operations: A large increase in write or overwrite operations on the system could suggest that files are being encrypted by ransomware.
- Use of Encryption Functions: The call of Application Programming Interfaces (APIs) by a process not typically associated with.
- Rapid File Modification Requests: Frequent requests to read, modify, or delete files within a short period of time. These could be signs of ransomware attempting to encrypt or erase data.
- Unusual Network Communications: Initiating communications with a command-and-control (C2) server. This is a common step for ransomware to receive instructions or transmit encryption keys.
- Registry Key Modifications: Unexpected changes in the keys associated with system startup or file associations.

Recognizing these indicators can help in the early detection of ransomware and, additionally, potentially preventing the encryption process and mitigating the damage caused by such attacks.

4.2. Ransomware Attack Framework

Ransomware operations are executed following a structured framework, typically progressing through identifiable stages [59]. This framework outlines the sequence of actions a ransomware undertakes from its initial deployment to the eventual demand for ransom. The phases are as follows:

- Target Identification: the initial phase involves selecting and identifying vulnerable systems or networks as potential targets for the attack.
- Infection Vector Distribution: this step encompasses executing the ransomware through chosen delivery mechanisms—this could be by phishing emails, compromised websites, or malicious downloads.
- Ransomware Installation: after successful entry into the system, the ransomware installs itself.
- Encryption Key Generation and Retrieval: the ransomware then generates an encryption key to lock the victim's files.
- File Access: targeting the data that are valuable to the user.
- Data Encryption: this phase encrypts the victim's files, making them inaccessible without the decryption key.
- Post-Encryption Operations: After encryption, the ransomware may perform additional actions, such as deleting system backups.
- Ransom Demand: Finally, the attacker demands a ransom from the victim, often in a cryptocurrency.

Understanding this attack framework is crucial for developing effective countermeasures and enhancing system defenses against ransomware threats.

4.3. Behavior Patterns of Ransomware Attacks

Ransomware demonstrates distinct behaviors based on how it interacts with victim files during an attack [59]. These behaviors can be classified into three primary categories:

- Type A Behavior: Ransomware directly encrypts the original files without creating copies. The steps include opening, reading, encrypting, and then closing the files. Sometimes, it may also rename the encrypted files to indicate they have been compromised.
- Type B Behavior: Ransomware removes the original files from their location, creates encrypted copies, and then returns these encrypted versions to the original directory. The encrypted files might have different names from the originals, satisfying their encryption status.
- Type C Behavior: Reading the original files and creating separate encrypted versions. The original files are deleted to eliminate any trace of the unencrypted data. The deletion is typically achieved through file movement operations that overwrite the originals.

Identifying these behavior patterns can help in the fast detection of ransomware activities; additionally, it can facilitate quicker response and mitigation efforts to protect data integrity.

4.4. Comparison of Ransomware Detection Methods

Ransomware detection has evolved significantly over the years, utilizing various methodologies, each with their strengths and weaknesses. Traditional signature-based detection methods rely on known patterns of ransomware, identifying threats by matching them against a database of known ransomware signatures [13]. While this method is highly effective against known ransomware strains, it struggles with zero-day attacks and new variants, as it cannot detect threats without pre-existing signatures [60].

In contrast, heuristic-based detection methods analyze the behavior of programs to identify potentially malicious activities [61]. This approach can detect previously unknown ransomware by examining suspicious patterns such as unusual file encryption activities,

unauthorized access to critical files, or attempts to disable security features. However, heuristic methods can generate false positives, where legitimate activities are flagged as malicious, necessitating further analysis to confirm the threat.

Anomaly-based detection leverages ML and statistical analysis to establish a baseline of normal system behavior. It then monitors for deviations from this baseline, flagging unusual activities that may indicate a ransomware attack. This method is particularly effective at identifying novel ransomware variants and zero-day attacks [61]. However, it requires significant computational resources to establish and maintain the baseline, and its accuracy can be impacted by the variability of normal user behavior [62].

ML-based detection methods have gained prominence, using algorithms to learn from vast datasets of both benign and malicious activities [9]. These models can predict and identify ransomware attacks by recognizing complex patterns and correlations that are not easily detectable by traditional methods. ML approaches offer high detection rates and adaptability to new threats [59]. However, they require large amounts of data for training and can be complex to implement and maintain. Additionally, they are not immune to adversarial attacks where attackers subtly alter ransomware characteristics to evade detection [29,63].

Finally, hybrid detection methods combine multiple approaches, such as integrating signature-based, heuristic, and ML techniques, to enhance detection accuracy and reduce false positives [60]. This comprehensive approach aims to leverage the strengths of each method while mitigating their individual weaknesses. Although hybrid methods offer robust protection, they can be resource-intensive and complex to manage, requiring sophisticated infrastructure and continuous updates to maintain efficacy against evolving threats [62].

Each ransomware detection method has its advantages and limitations. Traditional signature-based methods are reliable against known threats but fall short against new variants. Heuristic and anomaly-based methods offer broader detection capabilities but can suffer from false positives and high resource demands. ML approaches provide high adaptability and accuracy but require extensive data and complex implementation. Hybrid methods strive to offer the best of all worlds but come with increased complexity and resource requirements. Choosing the right detection strategy often depends on balancing these factors against the specific needs and resources of the organization. Table 6 below provides a comprehensive comparison of different ransomware detection methods, highlighting their advantages and disadvantages. This comparison aims to offer a clear understanding of the capabilities and limitations of each method, aiding in the selection of the most appropriate strategy for robust ransomware defense.

Table 6. Comparison of ransomware detection methods: advantages and disadvantages.

Detection Method	Advantages	Disadvantages
Signature-based	<ul style="list-style-type: none"> Highly effective against known ransomware Low false-positive rate 	<ul style="list-style-type: none"> Ineffective against zero-day attacks and new variants Requires constant updates to the signature database
Heuristic-based	<ul style="list-style-type: none"> Analyzes suspicious behaviors Can detect previously unknown ransomware Effective in identifying unusual activities 	<ul style="list-style-type: none"> Generates false positives Requires further analysis to confirm threats May struggle with distinguishing between malicious and legitimate activities
Anomaly-based	<ul style="list-style-type: none"> Effective at identifying novel ransomware variants and zero-day attacks Monitors deviations from established baselines 	<ul style="list-style-type: none"> Requires significant computational resources Accuracy impacted by variability in normal user behavior Establishing a baseline can be complex and time-consuming

Table 6. Cont.

Detection Method	Advantages	Disadvantages
Machine Learning-based	<ul style="list-style-type: none"> • High detection rates and adaptability to new threats • Recognizes complex patterns and correlations • Continuously improves with more data 	<ul style="list-style-type: none"> • Requires large amounts of data for training • Complex to implement and maintain • Vulnerable to adversarial attacks
Hybrid	<ul style="list-style-type: none"> • Combines strengths of multiple methods • Enhances detection accuracy • Reduces false positives • Offers robust protection against a wide range of threats 	<ul style="list-style-type: none"> • Resource-intensive • Complex to manage • Requires sophisticated infrastructure • Needs continuous updates and maintenance

4.5. Effectiveness of Current Ransomware Detection Approaches

Ransomware detection methods have become crucial in cybersecurity. These methods aim to identify and detect ransomware attacks before they cause harm. Their effectiveness varies based on the approach used [59]. There are several key points to consider regarding their effectiveness, limitations, and areas for improvement [5].

Current ransomware detection methods include signature-based detection, behavior-based detection, and anomaly detection [59]. Signature-based detection works by comparing known ransomware signatures with files and activities on a system [59]. This method is effective for known threats but struggles with new or modified ransomware. As a result, its success rate is high for existing threats but low for zero-day attacks [5,59].

Behavior-based detection observes the behavior of programs and processes to identify suspicious activities typical of ransomware, like rapid file encryption [59]. This method is more adaptable than signature-based detection and can identify new threats [59]. However, its effectiveness can be limited by the sophistication of evasion techniques used by ransomware developers. False positives, where legitimate software is mistakenly flagged as ransomware, also pose a challenge [5].

Anomaly detection methods use ML to understand the normal operations of a network or system [59]. If something unusual happens, it could be a sign of ransomware [59]. However, putting this idea into practice is tough because it is hard to exactly define between what is normal and to keep up with regular changes in network activity [5].

Moreover, these detection methods can sometimes fail to distinguish between malicious and benign software, which leads to false positives or negatives [59]. Therefore, it is crucial to ensure legitimate software is not incorrectly flagged or blocked. However, it also means some ransomware can bypass these defenses [5].

To enhance ransomware detection, integrating multiple detection methods into a comprehensive defense strategy is crucial. This includes combining signature-based scanning with behavior analysis and ML algorithms to maximize detection capabilities [59]. Additionally, improving threat intelligence sharing among cybersecurity professionals can help in identifying and mitigating ransomware attacks more effectively [59]. While current ransomware detection methods are largely successful, they have limitations, especially against new threats [59]. Future improvements should focus on advanced detection technologies, better information sharing, and user education to enhance overall effectiveness [5].

4.6. Taxonomy of Ransomware Detection Technique

Malware analysis is the process of studying malware to figure out how it works, where it comes from, its purpose, and the damage it can cause. This helps security experts quickly detect, stop, and deal with threats [5]. Usually, analyzing malware is the first step in defending against it. Researchers and security experts have developed different ways to detect ransomware [5]. There are three main types of malware analysis: static analysis, dynamic analysis, and a mix of both (hybrid analysis) [13].

- **Static Analysis:** This involves checking the code of a suspicious file without running it [5]. The process includes examining the file structure, identifying any embedded strings (like text), and looking for known malicious patterns. To detect ransomware, some tools and studies focus on analyzing the parts of a file that do not change. However, as ransomware evolves, these static methods might not always work, especially with ransomware that hides its true nature [13].
- **Dynamic Analysis:** The suspicious file is actually run in a controlled environment to observe what it does [5]. This might include looking at the file's behavior, which files it tries to change [5], and how it interacts with the computer's system. Various studies have used dynamic analysis to understand how ransomware behaves during an attack. This approach has been effective in detecting new types of ransomware but requires careful setup to avoid actual damage [13].
- **Hybrid Analysis:** Combines static and dynamic methods for a more comprehensive examination by looking at both the file's code and its behavior when executed. This approach aims to detect ransomware that might pass through with just one type of analysis. Hybrid analysis has shown promise in identifying ransomware early in the infection process. It benefits from the strengths of both static and dynamic analysis. Therefore, it offers a stronger detection method.

4.7. Emerging Trends in Ransomware

Ransomware continues to evolve and present new challenges for cybersecurity. Among the most concerning trends are RaaS and the targeting of IoT devices [64]. These developments significantly impact the landscape of digital security and complicate the task of early detection.

RaaS is a model where ransomware creators offer their malicious software as a service to other cybercriminals. This method has made it easier for individuals, regardless of their technical expertise, to initiate complex ransomware. Cybercriminals can now rent or buy ransomware, complete with customer support and updates, which is similar to legitimate software services. This trend not only increases the volume of ransomware attacks but also increases the threats. Moreover, it makes detection and prevention more challenging. Early detection systems must now adapt to a wider range of ransomware behaviors and signatures. As a result, the creation of effective defense mechanisms will be complicated [64].

The targeting of IoT devices represents another significant challenge [22]. As more devices connect to the internet such as smart thermostats and security cameras, the attack surface for cybercriminals expands. IoT devices often lack important security measures, making them easy targets for ransomware. An attack on these devices can lead to severe disruptions [52]. Such an attack will not just affect personal convenience but also have serious effects in critical services such as healthcare and public safety systems. The implication for early detection is very important. Security systems must now monitor a large number of devices and communication protocols. They must be able to identify and respond to threats in a highly decentralized and varied ecosystem.

The evolution of ransomware confirmed the need for advanced detection strategies. These include deploying ML algorithms capable of identifying anomalies in device behavior [44], enhancing the security of IoT devices through regular updates and patches, and educating users about the risks of RaaS platforms [50]. As attacks become more complex, the need for early detection has become more urgent than ever. Addressing this challenge requires a comprehensive strategy that includes technological solutions, regulatory measures, and increased public awareness to stay ahead with cybercriminals.

4.8. Ransomware Avoidance Strategies

There are effective measures that can be taken to minimize the risk of falling victim to these attacks [13–15]:

- **Keep software up to date:** Regularly updating the operating system and all applications is crucial. These updates often include patches for security vulnerabilities that ransomware attackers exploit.
- **Unknown emails and downloads:** Avoid opening emails or downloading attachments from unknown or suspicious sources. Cybercriminals often use phishing emails to spread ransomware.
- **Use browser security features:** Enable security features in web browsers that can block malicious websites and downloads. Disabling JavaScript and Java on untrusted sites can also help prevent ransomware from being downloaded on your device.
- **Limit access to important files:** Use features like “Controlled Folder Access” on Windows to prevent unauthorized applications from modifying protected folders. This step is particularly effective in stopping ransomware from encrypting your files.
- **Backup your data:** Regularly back up your data and ensure that backups are stored in a secure location and disconnected from your main network. As a result, if you do fall victim to a ransomware attack, you can restore your data from the backup without paying the ransom.
- **Use security software:** Employ antivirus and anti-ransomware software to detect and prevent ransomware threats. Keep this software up to date to protect against the latest ransomware variants.

By performing these strategies, individuals and organizations can significantly reduce their risk of being impacted by ransomware. In addition, staying updated about the latest ransomware threats and prevention techniques is also crucial in dealing with this kind of attack.

5. Real-World Ransomware Incidents

Ransomware attacks have become a significant threat to individuals, businesses, and government entities worldwide.

- **WannaCry Global Ransomware Attack (2017):** In May 2017, the WannaCry ransomware attack spread across over 150 countries and infected more than 250,000 computers [64]. The attack exploited a vulnerability in Microsoft Windows in which a patch had been released but not widely applied [64]. One of the victims of this attack was the UK’s National Health Service (NHS). The ransomware encrypted files and demanded Bitcoin payments to release the encrypted data [64]. The attack highlighted the importance of regular software updates and the strong impact of ransomware on critical infrastructure and services. It also marked a turning point in encouraging global awareness and efforts to combat cyber threats.
- **Colonial Pipeline Attack (2021)** The Colonial Pipeline ransomware attack in May 2021 underscored the vulnerability of critical infrastructure to cyberattacks [65]. The Colonial Pipeline, which carries gasoline and jet fuel over 5500 miles (about 8850 km) between Texas and New York [65], was forced to shut down operations due to a ransomware attack by a group known as DarkSide [65]. This disruption led to a significant increase in gas prices, panic buying, and fuel shortages across the Eastern United States [65]. The company paid a ransom of nearly USD 5 million in cryptocurrency to regain access to their systems [65]. This incident encouraged the U.S. government to issue new cybersecurity directives for pipeline operators [65]; moreover, it emphasized the national security implications of ransomware attacks.
- **Atlanta City Government Attack (2018)** In March 2018, the city government of Atlanta, Georgia, was hit by a ransomware attack [66]. This attack hit a big part of its digital infrastructure [66]. The SamSam ransomware attack affected multiple city services, which included court proceedings, bill payments, and law enforcement activities [66]. These affected services demonstrated how ransomware could damage the day-to-day operations of a city. They demanded a ransom of USD 51,000 in Bitcoin but the city chose not to pay [66]. The recovery and mitigation efforts cost the city an

estimated USD 17 million [66]. This incident provided motivation to other cities across the United States to strengthen their cybersecurity defenses.

- University of California, San Francisco (UCSF) Attack (2020): The University of California, San Francisco (UCSF), fell victim to a ransomware attack in June 2020. This attack targeted the School of Medicine's IT infrastructure [67]. They faced the potential loss of critical academic research data, including work related to COVID-19 [67]. UCSF chose to pay a ransom of over USD 1.14 million [67]. The NetWalker ransomware group was responsible for the attack [67]. They exploited vulnerabilities in unsecured networks [67]. This incident satisfied the complex ethical and financial decisions ransomware victims must take when critical scientific research is in danger.

6. Comparison with Other Review Papers

The main goal of our study is to emphasize the need for ongoing improvements in detection technologies to keep up with the constantly changing ransomware threat landscape. By reviewing a wide range of research and articles, this study evaluates different methods for detecting ransomware, new and promising tools, and identifies gaps in the current studies.

The contributions of this paper are significant. It not only identifies existing knowledge on detecting ransomware but also highlights where more research is needed. The paper examines related studies and real-world ransomware cases, highlighting the urgent need for better and more flexible detection technologies. It discusses the complexities of ransomware attacks and the challenges in detecting them early. Furthermore, it emphasizes how new technologies can help in developing better defense mechanisms.

The importance of this study lies in its potential to improve defenses against ransomware by providing a detailed look at how ransomware works and how effective current detection methods are. This research offers valuable insights for both researchers and professionals in cybersecurity. Moreover, it emphasizes the importance of collaboration among all parties involved to develop effective prevention strategies, thus helping protect important information and infrastructure from these harmful threats. This paper serves as a crucial guide for how to more effectively detect, prevent, and respond to ransomware attacks as we move forward in the digital world.

This paper delves into the topic of ransomware and aims to provide a thorough understanding and analysis of this significant cybersecurity threat. We delve into the background of ransomware, reviewing its types, attack vectors, encryption methods, and detection challenges, and exploring the role of AI in combating such threats. It also addresses preventive measures, legal considerations, and future trends. The discussion focuses on indicators of ransomware incidents, attack frameworks, and behavior patterns, as well as the efficacy of current detection techniques, emerging trends, and avoidance strategies. Real-world ransomware incidents are also discussed, which gives practical insights into the impact of these attacks. Furthermore, this study reviews related studies, providing a critical analysis of the existing literature and identifying research gaps. Open challenges and limitations in ransomware detection and prevention are explored in detail. Future directions for research and development are proposed. Lastly, the paper underscores the importance of enhanced detection capabilities.

The authors of [9] discussed the critical issue of ransomware attacks and how these attacks have become a significant cybersecurity threat affecting organizations across various industries. The study provides a comprehensive overview of the ransomware threat landscape, analyzing the factors contributing to the spread of ransomware and exploring potential recommendations for future research. The main focus of the paper is on the development and implementation of machine learning-based ransomware detection systems. The key findings of the research include the importance of collaboration and data sharing among researchers and organizations to enhance the effectiveness of ransomware detection systems. The study emphasizes the challenges in developing effective machine learning-based ransomware detection systems and highlights the need for advanced techniques

and collaborative efforts to create strong and accurate detection mechanisms. Additionally, the paper discusses the historical background of ransomware attacks, recent literature on automated ransomware detection approaches, and future research directions in the field. However, a limitation of the paper is the lack of detailed case studies or real-world implementation examples of the discussed detection systems. Providing real world examples could provide more practical insights into their effectiveness in detecting and mitigating ransomware attacks. The paper could discuss the specific ML algorithms and techniques used for ransomware detection; moreover, it could include their strengths, weaknesses, and comparative analysis in different scenarios. Providing a detailed evaluation of the performance metrics of these algorithms in detecting ransomware could offer valuable insights for researchers and practitioners. Furthermore, the paper could explore the implications of evolving ransomware techniques and the adaptability of ML models to detect emerging threats effectively.

In [13], the authors discussed the critical issue of combating ransomware attacks. These attacks have become increasingly prevalent and damaging in the realm of cybersecurity. The authors conducted a thorough investigation into various scenarios and compare existing state-of-the-art research with their own contributions. They incorporated a case study on the Djvu ransomware to illustrate the modus operandi of the latest ransomware strains and provide suggestions. The motivation behind the study was the increase in ransomware attacks that impacting businesses and individuals globally. The authors highlighted the need for a comprehensive analysis that addresses the importance of ransomware avoidance techniques due to the complexity of mitigation and recovery processes.

Key findings of the paper include the proposal of the DAM (Detection, Avoidance, and Mitigation) framework, which is a theoretical model for reviewing and classifying tools, techniques, and strategies to detect ransomware effectively. Additionally, the paper discusses the effectiveness of pre-existing detection techniques. They emphasized the development of ML-based solutions to enhance detection capabilities. However, the paper does have some limitations. One notable limitation is the lack of comparing their methods to existing solutions. Furthermore, the paper focuses on a case study of the Djvu ransomware and does not provide any other cases.

The authors of [3] summarized the crucial issue of detecting and dealing with crypto-ransomware attacks, which is a big problem for Internet and mobile users. They highlighted how hard it is to detect ransomware early because there are not enough datasets showing what ransomware does before it encrypts files. They highlighted the need for modern methodologies in the detection process, the limitations of early detection, and the importance of innovative techniques to develop detection capabilities. The authors identified the importance of finding better ways to collect data and choose features to make detection models more accurate and reliable. The survey looks at different ways to detect ransomware. These ways include using ML methods like Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM). Moreover, they talked about how important it is to pick out the right features to design good detection models. The paper talked about the problems with current detection methods and suggested new ways to fix them, like defining boundaries better for the early stages of ransomware and using data from different places to learn more about the behavior. The paper also highlights the efforts provided by researchers and security professionals to prevent different cyberattacks. One limitation of this paper is that the authors focus on detection solutions by using ML techniques, but the paper also needs a detailed description of the other detection techniques. Further, there is no comparison between their work and others to prove the uniqueness of the paper.

Table 7 shows a comparison between our study and other relevant studies.

Table 7. Comparison with other review papers: (✓: the criteria was mentioned and discussed).

Mentioned Criteria	Our Paper	[9]	[13]	[3]	Suggestions for Improvements
Overview of ransomware attacks	✓	✓	✓	✓	
Types of ransomware	✓	✓	✓		Identify the types of ransomware attacks
Ransomware attack vectors	✓		✓		Explain in more detail
Signs of a ransomware attack	✓	✓	✓		Elaborate the different signs of ransomware attacks
Challenges in early detection of ransomware	✓			✓	Explain the challenges in detail
Advanced technologies in detection	✓	✓		✓	Explain the role of advanced technologies in detection
Taxonomy of ransomware	✓		✓		Explain in more detail
Preventive, avoidance, mitigation measures	✓	✓	✓	✓	
Regulatory and legal considerations	✓				Discuss regulatory and legal considerations
Ransomware framework	✓		✓		Explain in more detail
Effectiveness and limitations of current detection methods	✓	✓	✓	✓	
Real-world incidents	✓				Provide some real-world incidents

7. Related Study

This section reviews recent studies in the field and summarizes their key findings concerning ransomware detection and identification. In addition, possible suggested mitigation's to the best of our knowledge are presented in Table 8.

Khammas [68] proposed a new method to prevent and detect ransomware attacks by discussing the limitations of previous dynamic analysis techniques. The proposed method enhances detection speed by taking features from raw bytes using frequent pattern mining, thus avoiding the need for complex processes. The author proposed using the Gain Ratio technique for feature selection. The study identifies 1000 features as the best for effective detection. The research identified the use of a random forest classifier. Evaluating the effects of changing tree and seed numbers on ransomware detection can enhance accuracy and efficiency. The paper results indicate that employing 100 trees with a seed number of 1 output can give the highest accuracy and efficiency. As a result, this proposal achieved a detection accuracy of 97.74 percent. This study developed a valuable method that is efficient in ransomware detection using ML. Specifically, it used random forest to address the growing threat of ransomware attacks.

The authors of [38] discussed the specific challenges of a ransomware attack, highlighting its differences from general malware and the importance of having more advanced detection methods to effectively deal with this threat. The researchers of this paper proposed a two-stage detection model that combines a Markov model with a Random Forest model to improve the accuracy in detecting ransomware attacks. This model functions by analyzing sequences of Windows API calls made by programs as they enter a computer system; this works by identifying unique patterns associated with ransomware activities. The paper presented experimental results and analysis explaining the effectiveness of this approach. Moreover, it categorized ransomware activities into different types such as keyloggers, downloaders, DLL injectors, droppers, and anti-debuggers. Overall, the study offers valuable results to ransomware detection by combining dynamic analysis and ML techniques to provide a strong defense against this attack.

The authors of [69] proposed a new way to detect ransomware attacks using AI and advanced malware analysis techniques. They discussed how ransomware attacks are growing and affecting many sectors like business, healthcare, and education. Their proposed method combines different methods to analyze ransomware at multiple levels,

which include DLL, function call, and assembly levels. They used AI to understand the connections between these levels. In addition, they created and tested models for detecting ransomware. They presented a detection tool called AIRaD. Their method uses ML, Natural Language Processing (NLP), and dynamic binary instrumentation to detect and monitor ransomware behavior. As a result, combining reverse engineering, static and dynamic analyses, and ML, their method can detect ransomware accurately. This makes it a very useful tool in detecting a ransomware attack.

Alqahtani et al. [3] addressed the crucial issue of detecting and dealing with crypto-ransomware attacks, which is being a big problem for Internet and mobile users. They discussed how hard it is to detect ransomware early because there are not enough datasets showing what ransomware does before it encrypts files. The authors identified the importance of finding better ways to collect data and choose features to make detection models more accurate and reliable. The survey looks at different ways to detect ransomware, including using ML methods like CNN and LSTM; discusses how important it is to pick out the right features to produce good detection models; and discusses the problems with current detection methods. Subsequently, they suggested new ways to fix them, like defining boundaries better for the early stages of ransomware and using data from different places to learn more about the behavior. Overall, the study gives a valuable look at how ransomware attacks are changing. In addition, it offers useful ideas for making detection methods better at dealing with this threat.

Kapoor et al. [13] proposed a framework named DAM to detect, prevent, and mitigate ransomware through analyzing and classifying tools, techniques, and strategies. In addition, authors introduced some of the effective ways to avoid ransomware attacks that can be used by different organizations. Furthermore, authors presented a Djvu ransomware case study to illustrate the latest techniques used to spread it along with suggested strategies to reduce its spread.

Mohammad [21] discussed how ransomware are changing over time and become more common. This can provide ideas as to how to find them better. The author emphasizes the complexity and severity of ransomware as a malicious program that can significantly impact both individual users and organizations. Through the review of various studies on ransomware and protection mechanisms, the paper underscores the challenges posed by these attacks and the limitations of existing detection methods. Even though people and companies try to stay safe from ransomware, there is still no one significant solution that always works. Some tools can find some types of ransomware but not all of them. The writer suggests that having good backups of your important files is the best way to protect yourself. Moreover, he thinks that in the future, using smart computers to find ransomware might help.

Three-layer Security (3LS) was proposed in [19], which is a solution that aims to detect, eliminate, and prevent ransomware. 3LS consists of three components that considered as three layers of security mechanisms. The first layer is a browser extension, which is able to detect any malicious websites that tries to download unauthorized files to the system; this first layer of security utilizes two mechanisms to detect malware, which are the Anomaly-based Detection mechanism and Signature-based Detection mechanism. Virtual machine is the second layer of security, which is able to act as a security tool while performing updates to the system. The last layer of security uses anti-malware solutions to detect malicious files within the VM.

A comprehensive survey about how to detect ransomware using ML and dynamic analysis was conducted in [59]. Techniques of detection ransomware in different platforms were briefly explained. Datasets used in this study along with the techniques used to analyze these data, like DL, were also listed. The studies that used DL, ML, or a hybrid of both were also presented. Platforms that faced more attacks than other were highlighted. Research directions that need further investigation were also discussed. Finally, the authors aimed to use different techniques like ML and DL to detect ransomware to obtain precise results and provide a strong ransomware detection system.

In [48], a survey was presented that aimed to using ML as a defense mechanism against ransomware attacks. The experiments that were conducted on seven ransomware and seven benign software samples succeeded in distinguish between benign software and malicious software with low false-negative and false-positive rates. Values from different ransomware, such as DLLs, were extracted in this study. Early detection of ransomware attacks and alerts to the user about the existing threat were considered the main features of this proposed system.

In [63], a novel detection technique for ransomware based on dynamic analysis was proposed. A finite-state machine model to collect information about the victim device was identified. The proposed model aimed to monitor unusual cases in terms of persistence, utilization, lateral movement, and user resources to be able to detect ransomware attacks. When the system discovers malicious activities, alerts will be sent to the decision-making module. In the decision making module, FSM is utilized to analyze the operations and events to detect ransomware attacks. The accuracy, effectiveness, and a few false predictions for the finite-state machine model were discussed in the experiments results.

Fernando et al. [20] investigated how we can detect ransomware attacks using two techniques: ML and DL. The study underlined the destructive nature of ransomware. In addition, highlighting the challenges associated with recovering the system after an attack and emphasizing the importance to detect ransomware before it infects a system. By exploring various ML approaches for ransomware detection, the research focused on the effectiveness of these methods compared to traditional approaches. Moreover, this paper evaluated the strengths and weaknesses of different detection strategies, highlighting how well ML and DL can adjust and detect new types of ransomware attacks. Furthermore, the study tested the detection methods on both the current and older generations of ransomware attacks. These experiments will emphasize the accuracy of these detection methods. Overall, this paper offers valuable results into how ransomware detection is changing and the importance of using emerging advanced technologies to handle this attack.

In [70], an early detection model (CRED) was proposed to specify pre-encryption boundaries and gather data related to this phase more precisely. Process-centric and data-centric detection methods are employed in the CRED model to integrate data from both API and IRP. Then, these data are utilized to train a DL-based model. A data benchmark from real-world crypto-ransomware samples taken from a popular repository was utilized to assess the CRED model. To verify the performance of the CRED model, K-fold cross-validation is taken and compared with other models. Better protection for individuals, companies, and end users' data from ransomware attacks is one of the benefits of the proposed model. Also, the proposed model enhances and increases the defensive power and response to any cyberattacks accurately and on time.

The authors of [71] presented DNAact-Ran, which is a digital DNA sequencing engine to detect ransomware before establishing any attack by using ML. K-mer frequency vector and digital DNA sequencing design constraints are used by DNAact-Ran. In the first stage, DNAact defines primary features from previously processed data using Binary Cuckoo Search (BCS) and Multi-Objective GreyWolf Optimization (MOGWO) algorithms. After that, by using the k-mer frequency vector and the design constraints of DNA, the digital DNA sequence of the selected features is generated. The proposed model was applied to 942 goodware instances and 582 ransomware to assess the performance and efficiency of the proposed model. By comparing the proposed model with other models, the results show that DNAact-Run can detect ransomware more effectively and precisely.

Ahmed et al. [72] proposed a behavioral-based dynamic analysis framework for Highly Survivable Ransomware (HSR) along with sets of valuable features. To choose the most valuable features, Term Frequency-Inverse Document Frequency (TF-IDF) is used. To evolve and apply a detection model based on ML that can realize specific behavioral traits of highly survivable ransomware attacks, Artificial Neural Network (ANN) and Support Vector Machine (SVM) are used. The presented framework achieved a few false positive rates and an area under the ROC curve in the experimental evaluation. From the

experiment results, the proposed framework can accurately predetect a highly survivable ransomware attack.

In [29], a novel detection method for ransomware based on ML algorithms was presented. The proposed model can differentiate between benign files and ransomware, as well as between malware and ransomware. To identify ransomware, six machine-learning algorithms were tested. Using machine-learning algorithms, the proposed model automatically creates the detection model to detect new samples of ransomware. CF-NCF is a modification of TF-IDF. CF-NCF is focused on the appearance feature in every category. Conversely, TF-IDF is focused on the appearance feature in every document. In the end, the experimental findings demonstrate that the suggested method is capable of accurately identifying ransomware among malicious and benign files.

A brief survey about existing trends and future directions for the automated detection of ransomware was presented in [9]. It provided a comprehensive overview and history of ransomware along with their background. Several methods to detect, avoid, mitigate, and recover from ransomware are explained in this survey. This paper analyzes studies from 2017 to 2022. Readers will benefit from having this information to stay up-to-date on the most recent developments in automated ransomware detection, prevention, mitigation, and recovery. For those who are interested in studying ransomware detection, prevention, mitigation, and recovery, this research also highlights open challenges and potential research problems for future research areas.

Davies et al. [73] explored a new way to find files encrypted by ransomware, no matter what type of ransomware is used. It focused on using a method called differential area analysis. This method looks at how random the data in files are (called entropy) and compares them to those of regular files. The key idea is to look at the randomness in the beginning part of the file to determine the difference between normal files and those encrypted by ransomware. The research shows that how random a file's data are can be a good way to detect encrypted files. This could help improve how we detect ransomware. The paper also discussed the importance of using a diverse range of file types. They included new Microsoft formats and files with high randomness in their tests. This makes the detection method stronger and more effective. The study looked closely at the results of their tests and compared them to other research. As a result, they showed that this new method could be really useful in fighting against ransomware attacks.

The authors of [49] proposed a new method for detecting ransomware by focusing on analyzing the PE (Portable Executable) header of executable files instead of running the programs. Traditional detection methods usually watch how a program behaves while it is running, but this might not catch the malware fast enough. The new approach involves taking information from the PE headers of files and turning it into grayscale images. Then, it uses a CNN, a type of AI often used for image analysis, to learn from these images. The goal is to accurately identify whether a file is ransomware or harmless. This method takes advantage of CNNs' ability to extract important features from images. It is practical and effective because it can potentially detect ransomware early without needing to run the suspicious program. The paper approved, through various tests and metrics, that using PE header information and CNNs can improve the detection of ransomware.

The study [74] discussed using ML to detect ransomware. The researchers focused on semi-supervised learning, a method that can build detection models with limited labeled data and a large amount of unlabeled data. They compared different semi-supervised classification techniques to see which one is best for ransomware detection. The study used the CICAndMal 2017 dataset, which includes various ransomware families, to evaluate the effectiveness of these methods. The results showed that a semi-supervised learning approach with a random forest base classifier outperformed other methods, highlighting its potential for improving ransomware detection.

One research paper [75] discussed how to use smart programs to find and detect ransomware attacks on computer systems. The paper explains that while there have been studies on ransomware before, this one focuses specifically on using advanced algorithms

to detect and prevent these attacks. It mentions that DL, a type of AI, is becoming popular for this task because it can handle large amounts of data and solve problems better than traditional methods. Moreover, the paper highlights the need to explore big data analytics, which is another powerful tool, to improve ransomware detection. Overall, the paper aims to guide researchers on how to use these smart technologies to detect ransomware effectively.

Boven et al. [76] explored the serious issue of ransomware attacks on hospitals and their significant impact on patient care based on interviews with healthcare staff. It showed how these attacks cause major disruptions by making technology unavailable, leading to complete computer shutdowns, unavailability of emergency care protocols, and forcing a switch to paper-based charting systems. This switch presented challenges, as staff had difficulty adapting to outdated methods, resulting in lower productivity and problems tracking patient status. The study also addressed ethical considerations, with approval from medical ethics committees and efforts to protect data anonymity. Despite challenges like potential researcher bias and a small sample size, the study provides valuable insights into the immediate effects of ransomware attacks on acute care in hospitals. The findings highlight the urgent need for strategies to protect patient care from increasing cyber threats in the healthcare sector. Hospitals are increasingly targeted by ransomware attacks due to their vulnerability and the potential for severe consequences regarding patient care. When a hospital is hit by a ransomware attack, it may need to shut down its systems to prevent the malware from spreading further. This can lead to disruptions in patient care, longer emergency department stays, delayed treatments, and increased risks for patients. The study emphasizes that hospitals must prioritize cybersecurity to protect patient data and ensure continuity of care in the event of a cyberattack.

Table 8. Existing work in this field.

Reference	Key Findings	Limitations/Research Gaps	Suggested Mitigation
[68]	<ul style="list-style-type: none"> Proposing a new static analysis method for ransomware detection using feature from raw bytes. Identifying 1000 features as the best for effective ransomware detection. Highlighting the significance of feature selection in improving detection accuracy. Exploring the random forest classifier for ransomware detection. Determining that using 100 trees with a seed number of 1 results in the highest accuracy of 97.74 percent. Valuable results into developing an efficient ransomware detection approach using ML techniques, specifically random forest. 	<ul style="list-style-type: none"> Not comparing this ransomware detection method to others that use dynamic analysis or a mix of techniques. Not talking enough about how well this static analysis method would work for different kinds of ransomware. Not looking closely at how much computing power this method needs. Worries about making this method work with bigger sets of data or more complicated ransomware types. Not exploring enough how ransomware makers might try to hack this detection method. Not explaining the results of using the random forest classifier clearly enough for monitoring ransomware. 	<ul style="list-style-type: none"> Compare this new static analysis method with other ransomware detection methods that use dynamic analysis and a mix of techniques. Show why the static analysis approach is effective and different. Talk more about how well this static analysis method works with different types of ransomware. Test it with many kinds of ransomware to see if it can deal with them all. Give a detailed look at how much computer power is needed to use this new method. This helps readers understand if it is practical to use it or not. Think about how this method can handle big sets of data or more complicated ransomware without losing accuracy. Look into ways ransomware creators might try to avoid being detected and come up with ways to stop them. This makes the detection method stronger. Explain how the model decides if something is ransomware or not and which features are most important in making that decision.
[38]	<ul style="list-style-type: none"> It is hard to detect ransomware because it keeps changing with new signatures. This model combines a Markov model and a Random Forest model. Markov model looks at patterns in Windows API calls linked to ransomware. Random Forest helps cut down on wrong detections. This model was 97.3-percent accurate. Looking at the order of Windows API calls is key to detect ransomware. Used dynamic analysis and ML to detect ransomware. 	<ul style="list-style-type: none"> The study focused only on Windows API call sequences and does not mention other important features for detecting ransomware. The dataset used is not big enough to cover all kinds of ransomware. Using Cuckoo Sandbox for testing may not show how well the detection works in real-time scenarios. The study does not compare with other ways of detecting ransomware. 	<ul style="list-style-type: none"> Use a bigger dataset covering all ransomware types; this will make the detection models stronger. Test the detection models in real-time environments to see how well they work. This ensures they can detect ransomware quickly when it appears. Add more features and not focusing on Windows API calls. This can make the detection models better at catching new ransomware behaviors. Compare the new detection methods with other ways of detecting ransomware. This will identify why the new approach is better and different.

Table 8. Cont.

Reference	Key Findings	Limitations/Research Gaps	Suggested Mitigation
[3]	<ul style="list-style-type: none"> Identifying the challenges in detecting ransomware attacks early because there are not enough data to understand the behaviors before files get locked. Defining why it is really important to collect data so we can make better tools to detect ransomware. Exploring computer techniques like CNN and LSTM to see if they can help us in detecting ransomware. Importance of feature extraction and selection to build effective detection models for crypto-ransomware attacks. Discussing the limitations of the existing ways to detect ransomware and the importance of addressing these limitations. Looking at how ransomware attacks are changing over time. 	<ul style="list-style-type: none"> The paper does not address all the different ways to detect crypto-ransomware. There might not be enough real-life examples or data. The research might not go into enough detail about detection challenges, scalability issues, or the impact of evolving ransomware on detection models. The ideas in the paper might not work for every kind of ransomware attack or for different types of companies or organizations. The paper might not compare the different ways to detect ransomware. The paper does not address the limitations and challenges of the proposed method. 	<ul style="list-style-type: none"> Use real-life examples and data from case studies. Compare the different ways to detect ransomware. Discuss the detection challenges, scalability issues, or the impact of evolving ransomware on detection models in detail. Give advice to different types of companies or organizations so they can deal with ransomware better. Offer detailed advice on how to actually use the methods for detecting ransomware, like how to put them into action and how to mix them with other computer systems.
[13]	<ul style="list-style-type: none"> DAM framework provides different strategies to prevent ransomware attacks and avoid financial losses. One of their strategies is avoidance to protect users and organizations from ransomware. Cyber-hygiene is the effective strategy to avoid ransomware at the individual or user level. Predetection is considered as the optimum solution for various types of ransomware. 	<ul style="list-style-type: none"> The need for isolation and detection properties within the browser. DAM is only able to block sites that already exist in a predefined list. 	<ul style="list-style-type: none"> Integrating the browser with security properties and analyzing the behavior of the file before being downloaded. Creation of AI-based browser extension to monitor cyber-hygiene.

Table 8. Cont.

Reference	Key Findings	Limitations/Research Gaps	Suggested Mitigation
[63]	<ul style="list-style-type: none"> A novel detection technique for ransomware based on dynamic analysis was proposed. Finite-state machine model to collect information about the victim device was identified. The proposed model aimed to monitor unusual cases in terms of persistence, utilization, lateral movement, and user resources to detect ransomware attacks. When the system discovers malicious activities, alerts will be sent to the decision-making module. In the decision-making stage, FSM is utilized to analyze the operations and events to detect ransomware attacks. Accuracy, effectiveness, and a few false predictions for the finite-state machine model were highlighted in the experimental results. 	<ul style="list-style-type: none"> Their solution may fail to detect ransomware that uses different ways to enter the system. Ransomware uses different tactics to hide their entity; so, it will be difficult for the proposed model to detect them. The system may not send alerts to the system when the ransomware is not affecting the resources but has access to the system. 	<ul style="list-style-type: none"> Using advanced techniques to determine different methods used by ransomware. Improving the capabilities of the system to deal with variations of ransomware, such as ransomware that uses evasion techniques, through updating detection techniques to better detect and respond to malicious software. Monitoring capabilities need to be updated to monitor unusual cases in terms of persistence, utilization, lateral movement, and user resources to allow for better detection of ransomware attacks.
[69]	<ul style="list-style-type: none"> Using advanced methods to analyze ransomware at different levels like DLL, function calls, and assembly code. Using AI techniques to understand these different levels and teach a computer program to recognize ransomware. Suggested a ransomware detection system that uses AI and made a tool called AIRaD. Mixing different ways of looking at ransomware to achieve better results. Made special rules for detecting ransomware based on how it acts in computer files. Tried out different computer codes and settings to see how well the ransomware detection system worked. Created special rules for detecting ransomware that other researchers and security experts can use. 	<ul style="list-style-type: none"> Limited dataset, which might not show all the different types of ransomware. The tool might not work as well on new types of ransomware that act differently or try to avoid being detected. While the tool did well in tests, we are not sure how it will do in the real world, where ransomware is always changing. We are not sure if the tool can handle a lot of ransomware at once or work quickly in busy places where lots of computers are used. The tool needs other computer programs to work. This could make it easier for attackers to hack these programs. The tool might not be able to detect ransomware immediately, which is important for stopping it quickly. 	<ul style="list-style-type: none"> Include a wider range of ransomware types to make the tool better at detecting different kinds of ransomware. Make sure the tool can handle lots of ransomware at once and still work quickly in real-life situations. Make sure the tool does not rely too much on other computer programs that could make it easier for attackers to hack.

Table 8. Cont.

Reference	Key Findings	Limitations/Research Gaps	Suggested Mitigation
[21]	<ul style="list-style-type: none"> The tools and steps we currently have are not great at detecting and stopping ransomware. No single tool or method can totally protect against it. Malicious emails and links are the main ways ransomware gets into computers. Therefore, it is important to teach people about it and have strict rules for security. In addition, regularly backup important files. Ransomware attacks like CryptoWall3 can cost a lot of money in damage. The future of ransomware detection is likely to rely on AI, particularly ML algorithms. 	<ul style="list-style-type: none"> The paper only talks about detecting ransomware and ignores other important aspects like how to decrypt files or how the ransom money gets paid. Lack of real-world examples. The paper does not look at different tools or plans for finding ransomware. Therefore, readers cannot see which ones work better. 	<ul style="list-style-type: none"> Adding real-world examples about real ransomware attacks and how they were detected can give practical ideas and make the suggestions more useful. Compare different methods, tools, and plans for detecting ransomware to show which ones work best.
[48]	<ul style="list-style-type: none"> Monitoring of basic used operations and the need to focus on the detection and prevention efficiency. The proposed solution consists of 3 virtual environments to report and protect against malware in real time, which are the code analysis of malware, behavior analysis of malware, and malware reporting. The importance of monitoring the operations to detect unusual actions conducted by ransomware, such as analyzing DLLs and providing a brief analysis of the operations. There is a significant variation in the CPU, which was explored by using samples analysis of ransomware like ViraLock. The importance to educate and provide a greater level of awareness to avoid ransomware attacks. 	<ul style="list-style-type: none"> Relying on 3 virtual environments will increase the consumption of the resources and access time, which will decrease the level of protection. The system may not offer protection when the user is offline; in this case, the probability of worms infection is high through using removable drives. The analysis process requires a long time, which may cause a delay in responding to and detecting malicious threats. The difficulty in distinguishing between benign applications and ransomware. False positive or false negative may be shown due to reliance on ML techniques, which may impact the entire process and accuracy of the results. 	<ul style="list-style-type: none"> Integrating multi-techniques to increase the efficiency of the analysis and improve the detection process. A secure connection channel to transfer data that have been collected will help to minimize the infection risk of ransomware on the analysis machine. Early detection systems to detect malicious actions in a short time, which will help to create a zero-trust security approach to protect against ransomware attacks.

Table 8. Cont.

Reference	Key Findings	Limitations/Research Gaps	Suggested Mitigation
[19]	<ul style="list-style-type: none">It is important to understand ransomware properties, backup practices that need to be addressed, and protection mechanisms that need to be implemented.Recertification and retesting are necessary for software that is doing frequent updates to achieve security and compatibility.The need for regular and proper backups to avoid ransomware threats.	<ul style="list-style-type: none">A limited number of simultaneously running virtual machines to prevent infection transmission.Based on the limited number of virtual machines, the number of downloads that are allowed to the user will decrease, which affects the scalability and efficiency of the ransomware prevention and detection mechanism.The need for advancements in technology is important to provide effective protection against ransomware threats.	<ul style="list-style-type: none">Using specific virtual machines for each downloaded file to prevent infection.Improving an efficient and scalable detection and prevention mechanism for ransomware through allocating and optimizing resource management within the system.Improving advancements in technology through providing the additional number of virtual machines that a computer can use to provide effective protection for the user against ransomware threats.
[20]	<ul style="list-style-type: none">Using ML and DL techniques is better than traditional approaches to detecting ransomware attacks.Testing different ways of detecting ransomware on both new and old types helps us see how well they work against new threats.	<ul style="list-style-type: none">The study has more ransomware examples than regular files. This could make it hard to train the model to recognize normal behavior.It could be hard to use the same detection methods on IoT devices. IoT devices work differently to regular computers. As a result, we will need new ways to find ransomware on IoT devices.	<ul style="list-style-type: none">Use more types of ransomware for training to cover a wider range of behaviors, not just focusing on specific ones like Locky and TeslaCrypt.Look at more than just assembly and DLL features to capture the different ways ransomware behaves.Add features that look at how networks are used specifically for IoT devices to make detection methods work better on them.Train the model with more regular files to make a balance between the number of normal and suspicious behaviors.Change the features to match how IoT devices work.

Table 8. Cont.

Reference	Key Findings	Limitations/Research Gaps	Suggested Mitigation
[59]	<ul style="list-style-type: none"> A comprehensive survey about how to detect ransomware using ML and dynamic analysis. Focusing on the security problems that are countered by DL frameworks, exploring protection methods by using DL, and providing a brief dataset to be analyzed. Applying DL to different platforms to be analyzed and evaluated. Assigning red tags to any threats that are conducted by ransomware attacks, like opening a lot of files simultaneously. 	<ul style="list-style-type: none"> The analysis can be bypassed by ransomware due to the lack of details about datasets in the mentioned studies. Limited period analysis may lead to facilitate evasion techniques used by ransomware. In addition, a lack of data availability during initial encryption may pose a problem. Difficult to detect ransomware that uses evasion techniques, especially when the sample is running for a short time. Ransomware detection programs may be infected during run time, which leads to loss of data. Limited analysis in the ransomware detection studies, leading to inaccurate results. 	<ul style="list-style-type: none"> Using advanced technology to face evasion tactics that are utilized by ransomware, such as strong analysis techniques that can be used in changing environments. Providing a brief dataset along with details about the size of samples and methodologies used for analysis to ensure transparency and to come up with reproducible and reliable results. Making the data available during the initial encryption phase will improve the capabilities of detection and provide a better understanding of the behavior of ransomware. During execution, it is necessary to analyze the encryption operations to improve advanced detection techniques and to determine whether ransomware uses evasion techniques. Continuous improvement of the detection systems including static, dynamic, and blend of both to enhance the accuracy of the analysis.
[70]	<ul style="list-style-type: none"> An early detection model (CRED) is proposed to specify pre-encryption boundaries and gather the data related to this phase more precisely. Process-centric and data-centric detection methods are employed in the CRED model to integrate data from both API and IRP. To verify the performance of the CRED model, K-fold cross-validation is taken and compared with other models. The proposed model enhances and increases the defensive power and response to any cyberattacks accurately and on time. 	<ul style="list-style-type: none"> The proposed model needs further stages of validation and development. Concerns regarding the performance of the proposed model and its practical application may arise due to the need for further empirical evidence. 	<ul style="list-style-type: none"> Performing a lot of experiments and testing on real-world examples by using different datasets to verify the effectiveness and performance of the proposed model. Enhancing the proposed model continuously based on conducting tests on the recent types of crypto-ransomware attacks and integrating new technologies to develop the accuracy of detection.

Table 8. Cont.

Reference	Key Findings	Limitations/Research Gaps	Suggested Mitigation
[71]	<ul style="list-style-type: none"> The authors presented DNAact-Ran, a digital DNA sequencing engine, to detect ransomware before establishing any attack by using ML. K-mer frequency vector and digital DNA sequencing design constraints are used by DNAact-Ran. DNAact defines primary features from previously processed data using BCS and MOGWO algorithms. The results show that DNAact-Run can detect ransomware more effectively and precisely. 	<ul style="list-style-type: none"> They used limited datasets for testing and training, which may limit the effectiveness of their proposed method. There is a lack of discussion about the possibility of applying their proposed method to different types of ransomware. Lack of detailed analysis of performance measures used to assess the effectiveness of their proposed method. 	<ul style="list-style-type: none"> Using diverse datasets that consist of different types of ransomware for testing and training will help to enhance the effectiveness of their proposed method. Providing a detailed analysis of performance measures and implementing cross-validation methods to assess the effectiveness of the proposed model.
[72]	<ul style="list-style-type: none"> A behavioral-based dynamic analysis framework for HSR along with sets of valuable features was proposed. TF-IDF used to choose the most valuable features. ANN and SVM are used to evolve and apply a detection model based on ML that can realize specific behavioral traits of highly survivable ransomware attacks. The presented framework achieved a few false-positive rates and an area under the ROC curve in the experimental evaluation. The proposed framework can predetect highly survivable ransomware accurately. 	<ul style="list-style-type: none"> Limited scope of the study due to the limited types of ransomware analyzed and tested. The lack of detailed analysis of performance measures used to assess the effectiveness of their proposed method. The need to practically implement the proposed framework in real-world scenarios. 	<ul style="list-style-type: none"> Using diverse datasets that consist of different types of ransomware for testing and training will help to enhance the effectiveness of their proposed method. Providing a detailed analysis of performance measures and implementing new techniques to assess the effectiveness of the proposed model. Performing a lot of experiments and testing on real-world examples by using different datasets to verify the effectiveness and performance of the proposed model.
[29]	<ul style="list-style-type: none"> A novel detection method for ransomware based on ML algorithms was presented. The proposed model can differentiate between benign files and ransomware. To identify ransomware, six machine-learning algorithms were tested. CF-NCF is a modification of TF-IDF. CF-NCF is focused on the appearance feature in every category. TF-IDF is focused on the appearance feature in every document. The experimental findings demonstrate that the suggested method is capable of accurately identifying ransomware among malicious and benign files. 	<ul style="list-style-type: none"> This study only examined a small number of ransomware samples, which might affect the generalization of their method. Using different detection techniques to detect most ransomware behavior and techniques rather than focusing on API Invocation Sequences. The need to practically implement the proposed method in real-world scenarios. 	<ul style="list-style-type: none"> Using diverse datasets that consist of different types of ransomware for testing and training will help to enhance the effectiveness of their proposed method. Using different sources of data to detect different types of ransomware techniques and behaviors. Performing a lot of experiments and testing on real-world examples by using different datasets to verify the effectiveness and performance of the proposed method.

Table 8. Cont.

Reference	Key Findings	Limitations/Research Gaps	Suggested Mitigation
[9]	<ul style="list-style-type: none"> A brief survey about existing trends and future directions for the automated detection of ransomware was presented. A comprehensive overview and history of ransomware along with their background. Several methods to detect, avoid, mitigate, and recover from ransomware are explained in this survey. Readers will benefit from having this information to stay up-to-date on the most recent developments in automated ransomware detection, prevention, mitigation, and recovery. For those who are interested in studying ransomware detection, prevention, mitigation, and recovery, this research also highlights open challenges and potential research problems for future research areas. 	<ul style="list-style-type: none"> Using different detection techniques to detect most ransomware behavior and techniques rather than focusing on ML techniques. This study only examined a small number of ransomware samples, which might affect the generalization of their method. The lack of detailed analysis of performance measures used to assess the effectiveness of their proposed method. The need to practically implement the proposed method in real-world scenarios. 	<ul style="list-style-type: none"> Using diverse datasets that consist of different types of ransomware for testing and training will help to enhance the effectiveness of their proposed method. Using different sources of data to detect different types of ransomware techniques and behaviors. Providing a detailed analysis of performance measures and implementing new techniques to assess the effectiveness of the proposed model. Performing a lot of experiments and testing on real-world examples by using different datasets to verify the effectiveness and performance of the proposed method.
[73]	<ul style="list-style-type: none"> Differential area analysis is introduced for finding files encrypted by ransomware. The method works to distinguish between regular files and ransomware-generated encrypted files. The randomness of file data (file entropy) is identified as a trustworthy way to detect encrypted files. 	<ul style="list-style-type: none"> The method relies heavily on the accuracy of entropy (randomness) values to tell normal files from encrypted ones. This accuracy can change depending on the type of file and how it is compressed. There might be difficulties in using this technique on a large scale efficiently, especially with a lot of files. The technique has not been tested in real-time situations where ransomware is actively attacking. 	<ul style="list-style-type: none"> Taking into their consideration various types of files and how they are compressed. This will make the method more accurate and reliable. Look into ways to make the differential area analysis method more efficient so it can handle large numbers of files without issues. Test the proposed technique in real-time situations where ransomware attacks are happening to see how well it works in the real world.

Table 8. Cont.

Reference	Key Findings	Limitations/Research Gaps	Suggested Mitigation
[49]	<ul style="list-style-type: none"> A new way to detect ransomware by turning the PE header of executable files into images for analysis. The method makes use of CNNs to effectively uncover hidden features in the created images, leading to better ransomware detection rates. This approach achieves a 93.3-percent accuracy rate in detecting ransomware, which identifies it as an effective early detection tool. It successfully separates harmless files from ransomware by analyzing the unique patterns and features found in the PE header data. 	<ul style="list-style-type: none"> The study does not clearly specify how long to monitor programs to accurately assess their behavior. The approach relies heavily on the PE header format, making it less effective for non-PE files. 	<ul style="list-style-type: none"> Extend the feature extraction process beyond the PE header to include other file characteristics. Expand the dataset to include more samples and ensure it covers a broader range of ransomware types.
[74]	<ul style="list-style-type: none"> Intelligent algorithms are effective in detecting ransomware attacks. DL algorithms show promise in handling large datasets for ransomware detection. There is a growing interest in using advanced algorithms for ransomware defense. Some ransomware families, like Sage and Hidden Tear, are frequently encountered in the literature. 	<ul style="list-style-type: none"> Challenges in differentiating ransomware traffic from normal traffic patterns. Limited application of certain DL architectures for ransomware detection. Potential failure of systems during data recovery from ransomware attacks. 	<ul style="list-style-type: none"> Explore more DL architectures for improved ransomware detection. Develop hybrid DL algorithms for detecting ransomware on big data platforms. Implement ML approaches to enhance ransomware detection accuracy. Address challenges through research in DL and big data analytics for better defense against ransomware attacks.
[75]	<ul style="list-style-type: none"> Wrapper RF classification and Chi-squared or OneR feature selection methods are effective for semi-supervised ransomware detection. Ransomware detection using family datasets separately is more effective than binary classification. The Simplified Silhouette Filter (SSF) unsupervised feature selection method yielded poor results. Semi-supervised feature selection methods need to be explored for improved ransomware detection in future works. 	<ul style="list-style-type: none"> The applied feature selection methods were supervised, limiting the effectiveness of the study. The collective IBK method did not perform well for ransomware classification. The SSF unsupervised feature selection method did not provide satisfactory results. 	<ul style="list-style-type: none"> Investigate and propose semi-supervised feature selection methods for ransomware detection in future research. Explore alternative feature selection techniques that are more suitable for semi-supervised learning. Consider the effectiveness of feature selection methods in improving ransomware detection accuracy.

Table 8. Cont.

Reference	Key Findings	Limitations/Research Gaps	Suggested Mitigation
[76]	<ul style="list-style-type: none">• Loss of technology availability during attacks, leading to complete computer downtime and unavailability of emergency care protocols.• Transition to paper-based charting systems, causing inefficiencies and challenges in tracking patient status.• Staff reliance on paper charting forms, despite being unfamiliar with traditional methods.• Use of whiteboards to replace digital tracking systems, resulting in confusion and difficulties in patient status reporting.• Hospitals facing significant disruptions in patient care and operational efficiency during ransomware attacks.• Importance of hospitals being prepared to respond effectively to cyber threats to safeguard patient care.	<ul style="list-style-type: none">• Limited willingness of healthcare organizations to participate in the study due to concerns about the sensitivity of the topic.• Small number of participants per incident, ranging from one to three interviewees, which may limit the depth of understanding for each case.• Potential selection bias as the study focused on major ransomware attacks, possibly overlooking minor incidents or successful cyber-defense cases.• Small sample size of incidents (n=4), which may impact the generalizability of the findings.• Challenges in increasing the sample size and participation rate, indicating the need for reassurance and further studies on barriers to participation in cyberattack research in healthcare.	<ul style="list-style-type: none">• Address concerns about the sensitivity of the topic to increase willingness of healthcare organizations to participate in the study.• Increase the number of participants per incident to provide a broader understanding of each case.• Consider including minor incidents and successful cyber-defense cases in future studies to provide a more comprehensive analysis.• Provide reassurance to potential participants about the safety and confidentiality of their involvement in the study to encourage participation.• Conduct further research on barriers and facilitators of participation in studies on cyberattacks in healthcare to improve engagement and data collection.

Table 9 presents a comparison of different ransomware detection tools that were presented in the previous studies.

Table 9. Comparison of different ransomware detection tools.

Ref.	AI	ML/DL	Semi-Supervised Learning	Static/Dynamic Analysis	Behavioral Analysis	Anomaly/Signature-Based Detection	Differential Area Analysis
[38]		✓		✓			
[69]	✓	✓		✓			
[3,29,68,70,71,75]		✓					
[13,72]		✓		✓	✓		
[19]						✓	
[63]				✓			
[73]							✓
[49]	✓						
[74]			✓				
[9,20,21,48,59]	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Table 10 presents a comparison of different mechanisms to detect ransomware including the methodology, parameters, platforms, objectives of the paper, proposed solutions, and results.

Table 10. Comparison of different mechanisms to detect ransomware.

Ref.	Proposed Method Name	Methodology	Parameters	Platform	Objective	Solution	Results
[70]	CRED	Process and data-centric detection techniques and DL	Performance	Cross-validation of k fold	Enhanced the accuracy of the detection and reduced false alarm rates.	Accurate determination of pre-encryption stage boundaries.	Only proposal, not implemented yet.
[19]	3LS	Signature and anomaly-based detection	Security	N/A	Decrease, identify, and prevent different types of attacks.	Virtual machine (VM), browser extension, and anti-malware solutions are used within the VM.	Their proposed model can isolate suspicious files before executing any harmful activity, but it will be difficult for a computer to run multiple VMs simultaneously.
[63]	Not identified	Finite-state machine model	Accuracy	NET Framework 4.5.2	Detect different types of ransomware accurately with low numbers of false predictions.	Identifying ransomware attacks based on the current state of the computer system.	The experiment results show that the proposed model can identify ransomware attacks efficiently with 99.55% accuracy and 0% FPR.
[48]	Not identified	ML	Security and performance	Random forest, decision tree, and neural network	Predetection of ransomware attacks.	Applying the analysis on 7 ransomware, 41 benign software, and 34 malware samples.	The experiment results show that the proposed method can differentiate between benign apps and ransomware with low false-positive and -negative rates.

Table 10. Cont.

Ref.	Proposed Method Name	Methodology	Parameters	Platform	Objective	Solution	Results
[73]	Not identified	Using Shannon entropy to distinguish between high-entropy files and encrypted files	Performance	Isolated target machine	Determine the time when the encrypted files are created.	Model to classify encrypted files reliably even if we have a dataset that consists of high-entropy files.	The experiment results prove that the proposed model has a high level of accuracy with a success rate higher than 99.96% when examining the first 192 bytes of a file.
[71]	DNAact-Ran	Digital DNA sequencing design constraints and k-mer frequency vector	Performance and accuracy	Java (version 1.8)	Predetection of ransomware before occurs.	Ransomware detection using ML and a Digital DNA sequencing engine.	The experiment results show that the proposed method can accurately and effectively detect ransomware.
[77]	An adaptive pre-encryption model	Dynamic analysis and Annotated term frequency-inverse document frequency technique	Accuracy	Not implemented yet	The ability to detect different types of ransomware that change their behavior continuously and have updated knowledge about the behavior of the attack.	Ransomware predetection model before encryption by using different datasets and different chosen features, which help to train this model in the detection process.	Not implemented yet.
[78]	DeepRan	Utilizing TF-IDF and Conditional Random Fields (CRF) model and incremental learning method	Accuracy	The LSTM model is used to train the processed data to detect suspicious logs	DL-based detector DeepRan is developed to detect and classify ransomware early to prevent network-wide data encryption.	Using a fully connected (FC) layer and attention-based bi-directional Long Short-Term Memory (BiLSTM), DeepRan models the normalcy of hosts in an enterprise system in operation and identifies anomalous activity from massive amounts of data.	According to experimental results, DeepRan generates an F1-score of 99.02 percent, or 99.87% detection accuracy, for early ransomware detection.

8. Open Challenges and Limitations

Early detection of ransomware is tough because cybercriminals keep changing their methods quickly, making it hard for security systems to catch up. They continuously create new types of attacks that older security systems cannot recognize. This means security tools that look for known ransomware do not work well against new or unknown attacks. Also, ransomware can hide by looking like normal software, making it even harder to detect early. Moreover, keeping up with the latest ransomware trends is challenging because there is so much information to track and the attackers are spread out all over the world. Another problem is finding the right balance between watching for ransomware and respecting user privacy. More aggressive monitoring might detect ransomware better but could violate users' privacy.

Detecting ransomware attacks early is key to avoid their severe consequences. However, there are significant challenges and limitations to achieve this goal starting from the complexity of ransomware tactics, the diversity of attack vectors, and the limitations of current detection technologies.

Moreover, the encryption methods that ransomware use present another challenge. Today's ransomware uses complex encryption that is hard to notice until it is too late and files are already locked. The way ransomware hides its actions is by appearing as a normal computer process, which makes it harder to detect.

The diversity of attack vectors also complicates early detection. Ransomware can enter through phishing emails, malicious websites, or software vulnerabilities. Each entry point requires different detection strategies. As a result, it is difficult for organizations to guard all possibilities effectively. Moreover, there is an increasing trend of fileless ransomware attacks, which do not rely on traditional files and leave fewer footprints; this poses a significant challenge for existing security tools.

Lastly, the human factor remains a critical weakness. Effective ransomware attacks often begin with social engineering tactics that trick individuals into initiating the infection process themselves. Training users to recognize these tactics is challenging, and a single mistake can lead to a successful attack.

9. Future Directions

Advancements in detection algorithms are essential for combating ransomware effectively. There is a critical need to develop more sophisticated algorithms that utilize ML, DL, and AI. These technologies have the potential to greatly enhance our ability to predict and identify ransomware activities before they cause harm. ML and DL algorithms can learn from vast amounts of data. They also can recognize patterns and signs that indicates a ransomware attack. This learning process enables the detection of new and evolving ransomware chains that traditional and signature-based antivirus tools might miss. AI can further increase these capabilities by automating decision-making processes and enabling systems to respond quickly to detect threats. Early detection is crucial because it allows for immediate action to prevent or minimize damage. Therefore, investing in the research and development of advanced detection algorithms is necessary for the cybersecurity community. This effort not only improves our defense against ransomware but also sets the stage for proactive measures against future cybersecurity threats.

9.1. Development of New Detection Algorithms

The continuous evolution of ransomware techniques necessitates the development of novel detection algorithms that can adapt and respond to new threats effectively. Future research should focus on creating algorithms that are not only robust but also capable of real-time detection and mitigation of ransomware attacks. Current detection methods often rely on signature-based approaches, which can be insufficient against new or modified ransomware strains. Therefore, there is a pressing need to explore heuristic and behavior-based algorithms that can identify malicious activities based on patterns and anomalies in system behavior. Furthermore, hybrid algorithms that combine multiple

detection techniques could enhance the accuracy and efficiency of ransomware detection. Researchers should also investigate the use of automated and self-learning systems that can continuously update and improve their detection capabilities without manual intervention.

9.2. Integration of AI and ML

AI and ML have shown significant promise in enhancing cybersecurity measures, including ransomware detection. Future research should delve into the integration of AI and ML techniques to develop intelligent systems capable of identifying and responding to ransomware attacks swiftly. ML models, especially those leveraging DL, can analyze vast amounts of data to detect subtle indicators of ransomware that traditional methods might miss. Research should also focus on the development of unsupervised learning techniques that can detect new ransomware variants without requiring labeled training data. Moreover, the use of reinforcement learning could enable systems to learn optimal defense strategies through continuous interaction with the environment. By incorporating AI, researchers can create more adaptive and proactive ransomware detection systems.

9.3. Impact of Emerging Technologies

Emerging technologies such as blockchain, IoT, and 5G networks present both opportunities and challenges for ransomware detection. Future research should investigate how these technologies can be leveraged to enhance security measures against ransomware. For instance, blockchain technology can be used to create decentralized and tamper-proof records, making it harder for ransomware to disrupt or manipulate data. On the other hand, the proliferation of IoT devices and the advent of 5G networks increase the potential attack surface for ransomware. Researchers need to explore how to secure these technologies and develop detection mechanisms that can operate in such dynamic and heterogeneous environments. Additionally, understanding the impact of quantum computing on cryptographic algorithms used by ransomware can help in developing future-proof security solutions. By examining these emerging technologies, researchers can anticipate future trends and prepare more effective defenses against ransomware.

9.4. Improved Data Collection and Sharing

Effective ransomware detection relies heavily on the availability of high-quality data for analysis and training of detection models. Future research should emphasize the development of standardized frameworks for data collection and sharing among organizations. This can include creating centralized repositories that anonymize and aggregate data from various sources, ensuring privacy while providing a rich dataset for researchers. Collaboration between public and private sectors can also be encouraged to facilitate the exchange of threat intelligence and real-time ransomware indicators. By improving data collection and sharing practices, researchers can build more comprehensive and accurate detection systems.

9.5. Development of Resilient Backup Solutions

Backups are a critical defense mechanism against ransomware attacks; yet, many organizations still struggle with implementing effective backup strategies. Future research should focus on developing resilient backup solutions that can withstand ransomware attacks and ensure quick recovery. This includes exploring innovative backup technologies, such as immutable backups and air-gapped systems, that are resistant to tampering and encryption by ransomware. Additionally, researchers should investigate best practices for backup frequency, storage, and recovery procedures to minimize data loss and downtime. By advancing backup solutions, organizations can improve their ability to recover from ransomware attacks without succumbing to ransom demands.

10. Conclusions

Our exploration of ransomware underscores the critical nature of safeguarding digital infrastructure against these malicious attacks. Ransomware, with its ability to encrypt victim's files and demand ransom for their release, presents a critical challenge that continues to evolve alongside technological advancements. This paper has delved into the multifaceted aspects of ransomware attacks, ranging from their mechanisms, types, and vectors to the encryption techniques employed. We have also identified the signs of an attack and the inherent challenges in early detection, highlighting the potential of AI in combating these threats. Preventive measures, best practices, and the legal framework surrounding ransomware have been explored to offer a clear understanding of the current landscape and suggest a proactive solution against such attacks.

Our literature review and discussion emphasize the necessity for immediate and efficient detection techniques to mitigate the impact of ransomware attacks. There are various strategies and tools aimed at identifying and preventing these attacks. However, there remains a substantial gap in the effectiveness and reliability of these measures. The dynamic and sophisticated nature of ransomware needs continuous research and development to enhance detection and prevention methods that can adapt to evolving attack patterns.

The significance of this study lies in its comprehensive analysis of ransomware. A collaborative effort is required from individuals, organizations, and governments to enhance digital defenses. It underscores also the urgent need for enhanced detection capabilities, strong prevention strategies, and a clear understanding of ransomware to safeguard sensitive information and critical infrastructure. Our investigation into the taxonomy of ransomware detection techniques, along with the real-world ransomware incidents and emerging trends, offers valuable insights into the complexity of these attacks. Furthermore, it highlights the necessity for a comprehensive approach to cybersecurity.

In conclusion, as ransomware attacks continue to pose a significant threat to global digital security, it is important that the cybersecurity community, policymakers, and stakeholders enhance defenses against these malicious activities. Future research should focus on closing the existing gaps in detection and prevention, explore the potential of emerging technologies, and propose an environment of collaboration and information sharing. As a result, we can hope to stay a step ahead of cybercriminals and protect our digital world from ransomware attacks.

Author Contributions: Conceptualization, L.A. and S.A.; methodology, L.A., S.A. and M.M.H.R.; software, L.A. and S.A.; validation, L.A., S.A. and M.M.H.R.; formal analysis, L.A., S.A. and M.M.H.R.; investigation, L.A. and S.A.; resources, L.A. and S.A.; writing original draft preparation, L.A. and S.A.; writing review and editing, L.A., S.A. and M.M.H.R.; supervision, M.M.H.R.; project administration, M.M.H.R.; funding acquisition, M.M.H.R. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [GRANT No. KFU241479].

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [GRANT No. KFU241479]. The authors would like to thank the anonymous reviewers for their insightful scholastic comments and suggestions, which improved the quality and clarity of the paper.

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

Abbreviations

The following abbreviations are used in this manuscript:

SLR	Systematic Literature Review
SMB	Server Message Block
AES	Advanced Encryption Standard
ECC	Elliptic Curve Cryptography
DLLs	Dynamic Link Libraries
MFA	Multi-factor authentication
APIs	Application programming Interfaces
DAM	Detection, Avoidance, and Mitigation
CNN	Convolutional Neural Networks
LSTM	Long Short-Term Memory
AI	Artificial Intelligence
NLP	Natural Language Processing
3LS	Three-Layer Security
ML	Machine Learning
BCS	Binary Cuckoo Search
MOGWO	Multi Objective GreyWolf Optimization
HSR	Highly Survivable Ransomware
TF-IDF	Term Frequency-Inverse Document Frequency
ANN	Artificial Neural Network
SVM	Support Vector Machine
PE	Portable Executable
SSF	Simplified Silhouette Filter
DL	Deep Learning
VM	Virtual Machine
CRF	Conditional Random Fields

References

- Ozer, M.; Varlioglu, S.; Gonen, B.; Bastug, M. A prevention and a traction system for ransomware attacks. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 5–7 December 2019; pp. 150–154.
- Xia, T.; Sun, Y.; Zhu, S.; Rasheed, Z.; Shafique, K. Toward a network-assisted approach for effective ransomware detection. *arXiv* **2020**, arXiv:2008.12428.
- Alqahtani, A.; Sheldon, F.T. A survey of crypto ransomware attack detection methodologies: An evolving outlook. *Sensors* **2022**, *22*, 1837. [\[CrossRef\]](#) [\[PubMed\]](#)
- 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. [\[CrossRef\]](#) [\[PubMed\]](#)
- Razaulla, S.; Fachkha, C.; Markarian, C.; Gawanmeh, A.; Mansoor, W.; Fung, B.C.; Assi, C. The age of ransomware: A survey on the evolution, taxonomy, and research directions. *IEEE Access* **2023**, *11*, 40698–40723. [\[CrossRef\]](#)
- The Latest Ransomware Statistics (Updated June 2024) | AAG IT Support. Available online: <https://aag-it.com/the-latest-ransomware-statistics/> (accessed on 19 June 2024).
- Altulaihan, E.; Alismail, A.; Hafizur Rahman, M.; Ibrahim, A.A. Email Security Issues, Tools, and Techniques Used in Investigation. *Sustainability* **2023**, *15*, 10612. [\[CrossRef\]](#)
- The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. Available online: <https://www.bmj.com/content/372/bmj.n71> (accessed on 19 June 2024).
- Alraizza, A.; Algarni, A. Ransomware detection using machine learning: A survey. *Big Data Cogn. Comput.* **2023**, *7*, 143. [\[CrossRef\]](#)
- Ransomware Payments Exceed 1 Billion in 2023, Hitting Record High after 2022 Decline. Available online: <https://databreaches.net/2024/02/09/ransomware-payments-exceed-1-billion-in-2023-hitting-record-high-after-2022-decline/> (accessed on 7 February 2024).
- Arslanian, M.; Roberts, H.; Welfer, J.; Xie, S.; Chen, B. The WannaCry Ransomware. Available online: <https://verifythesource.org/posts/wannacry> (accessed on 20 April 2024).
- Permana, G.R.; Trowbridge, T.E.; Sherborne, B. Ransomware mitigation: An analytical investigation into the effects and trends of ransomware attacks on global business. *PsyArXiv* **2022**. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)

14. Cen, M.; Jiang, F.; Qin, X.; Jiang, Q.; Doss, R. Ransomware early detection: A survey. *Comput. Netw.* **2024**, *239*, 110138. [\[CrossRef\]](#)
15. Kovács, A. Ransomware: A comprehensive study of the exponentially increasing cybersecurity threat. *Insights Reg. Dev.* **2022**, *4*, 96–104. [\[CrossRef\]](#)
16. DS, K.P.; HR, P.K. A Systematic Study on Ransomware Attack: Types, Phases and Recent Variants. In Proceedings of the 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 11–12 March 2024; pp. 661–668.
17. Chaithanya, B.; Brahmananda, S. Detecting ransomware attacks distribution through phishing URLs Using Machine Learning. In *Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT 2021*; Springer: Singapore, 2022; pp. 821–832.
18. Fuertes, W.; Arévalo, D.; Castro, J.D.; Ron, M.; Estrada, C.A.; Andrade, R.; Peña, F.F.; Benavides, E. Impact of social engineering attacks: A literature review. In *Developments and Advances in Defense and Security: Proceedings of MICRADS 2021*; Springer: Singapore, 2022; pp. 25–35.
19. Ren, A.; Liang, C.; Hyug, I.; Broh, S.; Jhanjhi, N. A three-level ransomware detection and prevention mechanism. *EAI Endorsed Trans. Energy Web* **2020**, *7*, e6. [\[CrossRef\]](#)
20. Fernando, D.W.; Komninos, N.; Chen, T. A study on the evolution of ransomware detection using machine learning and deep learning techniques. *IoT* **2020**, *1*, 551–604. [\[CrossRef\]](#)
21. Mohammad, A.H. Ransomware evolution, growth and recommendation for detection. *Mod. Appl. Sci.* **2020**, *14*, 68. [\[CrossRef\]](#)
22. Humayun, M.; Jhanjhi, N.; Alsayat, A.; Ponnusamy, V. Internet of things and ransomware: Evolution, mitigation and prevention. *Egypt. Inform. J.* **2021**, *22*, 105–117. [\[CrossRef\]](#)
23. Dand, P.; Chudasama, D. A Comparative Study about the Ransomware. *J. Adv. Database Manag. Syst.* **2021**, *8*, 8–15.
24. Begovic, K.; Al-Ali, A.; Malluhi, Q. Cryptographic ransomware encryption detection: Survey. *Comput. Secur.* **2023**, *132*, 103349. [\[CrossRef\]](#)
25. Cicala, F.; Bertino, E. Analysis of encryption key generation in modern crypto ransomware. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 1239–1253. [\[CrossRef\]](#)
26. Reshmi, T. Information security breaches due to ransomware attacks—A systematic literature review. *Int. J. Inf. Manag. Data Insights* **2021**, *1*, 100013. [\[CrossRef\]](#)
27. Mohammad, A.H. Analysis of ransomware on windows platform. *Int. J. Comput. Sci. Netw. Secur.* **2020**, *20*, 21–27.
28. Vasoya, S.; Bhavsar, K.; Patel, N. A systematic literature review on Ransomware attacks. *arXiv* **2022**, arXiv:2212.04063.
29. Bae, S.I.; Lee, G.B.; Im, E.G. Ransomware detection using machine learning algorithms. *Concurr. Comput. Pract. Exp.* **2020**, *32*, e5422. [\[CrossRef\]](#)
30. Lemmou, Y.; Lanet, J.L.; Souidi, E.M. A behavioural in-depth analysis of ransomware infection. *IET Inf. Secur.* **2021**, *15*, 38–58. [\[CrossRef\]](#)
31. Anand, V.K.; Bamanjogi, K.; Shaw, A.R.; Faheem, M. Comparative study of ransomwares. In Proceedings of the 2022 7th International Conference on Computing, Communication and Security (ICCCS), Seoul, Republic of Korea, 3–5 November 2022; pp. 1–9.
32. Olaimat, M.N.; Maarof, M.A.; Al-rimy, B.A.S. Ransomware anti-analysis and evasion techniques: A survey and research directions. In Proceedings of the 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29–31 January 2021; pp. 1–6.
33. August, T.; Dao, D.; Niculescu, M.F. Economics of ransomware: Risk interdependence and large-scale attacks. *Manag. Sci.* **2022**, *68*, 8979–9002. [\[CrossRef\]](#)
34. Lee, I.; Roh, H.; Lee, W. Encrypted malware traffic detection using incremental learning. In Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 1348–1349.
35. Mahajan, A.; Chakrabarty, N.; Majithia, J.; Ahuja, A.; Agarwal, U.; Suryavanshi, S.; Biradar, M.; Sharma, P.; Raghavan, B.; Arafath, R.; et al. Multisystem imaging recommendations/guidelines: In the pursuit of precision oncology. *Indian J. Med. Paediatr. Oncol.* **2023**, *44*, 002–025. [\[CrossRef\]](#)
36. Ghouti, L.; Imam, M. Malware classification using compact image features and multiclass support vector machines. *IET Inf. Secur.* **2020**, *14*, 419–429. [\[CrossRef\]](#)
37. Akhtar, M.S.; Feng, T. Malware analysis and detection using machine learning algorithms. *Symmetry* **2022**, *14*, 2304. [\[CrossRef\]](#)
38. 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. [\[CrossRef\]](#)
39. 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: Cham, Switzerland, 2021; pp. 189–198.
40. Saadat, S.; Joseph Raymond, V. Malware classification using CNN-XGBoost model. In *Artificial Intelligence Techniques for Advanced Computing Applications: Proceedings of ICACT 2020*; Springer: Cham, Switzerland, 2021; pp. 191–202.
41. Shah, K.; Patel, H.; Sanghvi, D.; Shah, M. A comparative analysis of logistic regression, random forest and KNN models for the text classification. *Augment. Hum. Res.* **2020**, *5*, 12. [\[CrossRef\]](#)

42. Faruk, M.J.H.; Shahriar, H.; Valero, M.; Barsha, F.L.; Sobhan, S.; Khan, M.A.; Whitman, M.; Cuzzocrea, A.; Lo, D.; Rahman, A.; et al. Malware detection and prevention using artificial intelligence techniques. In Proceedings of the 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 15–18 December 2021; pp. 5369–5377.
43. Stoian, N.A. Machine Learning for Anomaly Detection in Iot Networks: Malware Analysis on the Iot-23 Data Set. Bachelor's Thesis, University of Twente, Enschede, The Netherlands, 2020.
44. Goyal, M.; Kumar, R. The pipeline process of signature-based and behavior-based malware detection. In Proceedings of the 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 30–31 October 2020; pp. 497–502.
45. Sun, N.; Ding, M.; Jiang, J.; Xu, W.; Mo, X.; Tai, Y.; Zhang, J. Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1748–1774. [\[CrossRef\]](#)
46. 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. [\[CrossRef\]](#)
47. 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. [\[CrossRef\]](#)
48. Arabo, A.; Dijoux, R.; Poulain, T.; Chevalier, G. Detecting ransomware using process behavior analysis. *Procedia Comput. Sci.* **2020**, *168*, 289–296. [\[CrossRef\]](#)
49. Manavi, F.; Hamzeh, A. A new method for ransomware detection based on PE header using convolutional neural networks. In Proceedings of the 2020 17th International ISC Conference on Information Security and Cryptology (ISCISC), Tehran, Iran, 9–10 September 2020; pp. 82–87.
50. Singh, D.; Mohanty, N.P.; Swagatika, S.; Kumar, S. Cyber-hygiene: The key concept for cyber security in cyberspace. *Test Eng. Manag.* **2020**, *83*, 8145–8152.
51. Kitchen, D.E.; Valach, A.P. How to Avoid the Ransomware Onslaught. *Natl. Def.* **2020**, *105*, 18–19.
52. Möller, D.P. Ransomware Attacks and Scenarios: Cost Factors and Loss of Reputation. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*; Springer: Cham, Switzerland, 2023; pp. 273–303.
53. Berrueta, E.; Morato, D.; Magaña, E.; Izal, M. Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic. *Expert Syst. Appl.* **2022**, *209*, 118299. [\[CrossRef\]](#)
54. Lubin, A. The Law and Politics of Ransomware. *Vand. J. Transnat'l L.* **2022**, *55*, 1177.
55. Uandykova, M.; Lisin, A.; Stepanova, D.; Baitenova, L.; Mutaliyeva, L.; Yüksel, S.; Dincer, H. The social and legislative principles of counteracting ransomware crime. *Entrep. Sustain. Issues* **2020**, *8*, 777–798. [\[CrossRef\]](#)
56. Force, R.T. *Combating Ransomware*; Intel Security Group: Plano, TX, USA, 2021.
57. Ryan, P.; Fokker, J.; Healy, S.; Amann, A. Dynamics of targeted ransomware negotiation. *IEEE Access* **2022**, *10*, 32836–32844. [\[CrossRef\]](#)
58. AlSabeih, A.; Safa, H.; Bou-Harb, E.; Crichigno, J. Exploiting ransomware paranoia for execution prevention. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
59. Urooj, U.; Al-rimy, B.A.S.; Zainal, A.; Ghaleb, F.A.; Rassam, M.A. Ransomware detection using the dynamic analysis and machine learning: A survey and research directions. *Appl. Sci.* **2021**, *12*, 172. [\[CrossRef\]](#)
60. Chittooparambil, H.J.; Shanmugam, B.; Azam, S.; Kannoopatti, K.; Jonkman, M.; Samy, G.N. A review of ransomware families and detection methods. In *Recent Trends in Data Science and Soft Computing: Proceedings of the 3rd International Conference of Reliable Information and Communication Technology (IRICT 2018)*; Springer: Cham, Switzerland, 2019; pp. 588–597.
61. Sechel, S. A comparative assessment of obfuscated ransomware detection methods. *Inform. Econ.* **2019**, *23*, 45–62. [\[CrossRef\]](#)
62. Bijitha, C.; Sukumaran, R.; Nath, H.V. A survey on ransomware detection techniques. In *Secure Knowledge Management in Artificial Intelligence Era: 8th International Conference, SKM 2019, Goa, India, 21–22 December 2019*; Proceedings 8; Springer: Cham, Switzerland, 2020; pp. 55–68.
63. Ramesh, G.; Menen, A. Automated dynamic approach for detecting ransomware using finite-state machine. *Decis. Support Syst.* **2020**, *138*, 113400. [\[CrossRef\]](#)
64. Puat, H.A.M.; Abd Rahman, N.A. Ransomware as a service and public awareness. *PalArch's J. Archaeol. Egypt/Egyptol.* **2020**, *17*, 5277–5292.
65. Beerman, J.; Berent, D.; Falter, Z.; Bhunia, S. A review of colonial pipeline ransomware attack. In Proceedings of the 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), Bangalore, India, 1–4 May 2023; pp. 8–15.
66. Zimba, A.; Chishimba, M. On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems. *Eur. J. Secur. Res.* **2019**, *4*, 3–31. [\[CrossRef\]](#)
67. Liliashvili, G.B. Cyber risk mitigation in higher education. *Law World* **2021**, *17*, 15.
68. Khammas, B.M. Ransomware detection using random forest technique. *ICT Express* **2020**, *6*, 325–331. [\[CrossRef\]](#)
69. Poudyal, S.; Dasgupta, D. AI-powered ransomware detection framework. In Proceedings of the 2020 IEEE Symposium Series on Computational Intelligence (SSCI), Canberra, ACT, Australia, 1–4 December 2020; pp. 1154–1161.
70. Alqahtani, A.; Gazzan, M.; Sheldon, F.T. A proposed crypto-ransomware early detection (CRED) model using an integrated deep learning and vector space model approach. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 0275–0279.

71. Khan, F.; Ncube, C.; Ramasamy, L.K.; Kadry, S.; Nam, Y. A digital DNA sequencing engine for ransomware detection using machine learning. *IEEE Access* **2020**, *8*, 119710–119719. [[CrossRef](#)]
72. Ahmed, Y.A.; Kocer, B.; Al-rimy, B.A.S. Automated analysis approach for the detection of high survivable ransomware. *KSII Trans. Internet Inf. Syst. (TIIS)* **2020**, *14*, 2236–2257.
73. Davies, S.R.; Macfarlane, R.; Buchanan, W.J. Differential area analysis for ransomware attack detection within mixed file datasets. *Comput. Secur.* **2021**, *108*, 102377. [[CrossRef](#)]
74. Noorbehbahani, F.; Saberi, M. Ransomware detection with semi-supervised learning. In Proceedings of the 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 29–30 October 2020; pp. 024–029.
75. 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](#)]
76. van Boven, L.S.; Kusters, R.W.; Tin, D.; van Osch, F.H.; De Cauwer, H.; Ketelings, L.; Rao, M.; Dameff, C.; Barten, D.G. Hacking acute care: A qualitative study on the health care impacts of ransomware attacks against hospitals. *Ann. Emerg. Med.* **2024**, *83*, 46–56. [[CrossRef](#)]
77. Urooj, U.; Maarof, M.A.B.; Al-rimy, B.A.S. A proposed adaptive pre-encryption crypto-ransomware early detection model. In Proceedings of the 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29–31 January 2021.
78. Roy, K.C.; Chen, Q. Deepran: Attention-based bilstm and crf for ransomware early detection and classification. *Inf. Syst. Front.* **2021**, *23*, 299–315. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.