International Journal of
Technology and
Systems
(IJTS)

Ransomware Attacks and Their Evolving Strategies: A Systematic Review of Recent Incidents

Journal of Technology and Systems
ISSN : 2788-6344 (Online)
Vol. 6, Issue No. 7, pp 32 – 59, 2024
www.carijournals.org

Ransomware Attacks and Their Evolving Strategies: A Systematic Review of Recent Incidents

Sooraj Sudheer
Gannon University: Erie, US
https://orcid.org/0009-0001-2316-8899

Accepted: 17th Oct 2024 Received in Revised Form: 26th Nov 2024 Published: 14th Dec 2024

Abstract:

Ransomware attacks have emerged as a significant cybersecurity concern, posing intricate risks to individuals, institutions, and governments. Because cybercriminals are always improving their methods, it is important to understand how these changing approaches affect things. This study explores the complexity of ransomware attacks by looking into previous cases to identify trends, tactics, and how economic and technological advancements affect these risks. Through an extensive examination of cutting-edge ransomware tactics, the paper pinpoints a major research void with regard to current, fine-grained incident analyses and sector-specific impacts. A systematic literature review has been done using four ransomware and six cybersecurity keywords. The purpose of this study is to analyze the evolving complexity of ransomware attacks by examining past cases to identify trends, tactics, and the impact of economic and technological advancements on these risks. It also aims to address gaps in detailed incident analyses and sector-specific impacts, providing actionable insights and recommendations for strengthening cybersecurity defenses and legislative measures. The study adds to the body of knowledge by analyzing recent examples, identifying the dynamic nature of threat actor actions, and assessing the efficacy of countermeasures in a variety of industries through qualitative and quantitative data. The conclusions reached provide insightful analysis and practical suggestions for cybersecurity professionals to strengthen defenses, reduce risks, and predict future advancements in ransomware operations. In the end, this report hopes to set the groundwork for stronger cybersecurity standards and well-informed legislative solutions to counteract the increasingly complex ransomware techniques.

Keywords: *Ransomware, Cybersecurity, Cyber threat, security.*

1. Introduction

Within the realm of cyber security, ransomware is a dangerous and ever-evolving threat that is distinguished by its ability to encrypt data on a compromised system and require payment in order to decrypt it[1]. This harmful software concept encrypts files and demands a ransom, usually in bitcoin, for the decryption key after accessing computers through vulnerabilities. Ransomware dates back to the late 1980s, but it has become more common in recent years, in part because of the anonymity that cryptocurrencies offer and the ease with which ransoms may be transferred without being tracked[2]. The workings of ransomware are very simple, but they have far-reaching consequences: it uses security flaws to get into systems, encrypts data to make it unreadable, and then demands a fee to unlock the data[3]. The consequences of ransomware attacks are not limited to the immediate monetary loss resulting from the ransom; they also include data loss, recovery costs, lost operations, and even deterioration of stakeholder confidence[4].

The capacity of ransomware attacks to affect not only major organizations but also small and medium-sized enterprises, healthcare facilities, educational institutions, and government agencies has been well-documented[5]. This broad applicability highlights how vulnerable all industries are to these kinds of assaults, highlighting how important it is for all industries to practice cybersecurity vigilance. The advent of more advanced methods has been a defining characteristic of ransomware's progress[6]. For instance, "double extortion" tactics entail not only the exfiltration of sensitive data but also the encryption of the victim's files, with the attackers threatening to make the material publicly available unless a further ransom is paid[7]. These strategies strengthen the potential harm that ransomware attacks can cause and give attackers more power over their targets. Ransomware has a huge financial impact; the estimated annual global cost of ransomware assaults is in the billions of dollars[8]. In addition to the ransoms paid, this also covers the expenses of data recovery, forensic analysis, lost productivity, downtime, and post-attack security posture upgrading.

2. Is it time to consider Ransomware the biggest Cyber Threat?

The 1989 AIDS Trojan (PC Cyborg Virus) was one of the first ransomware assaults ever recorded. It was distributed via floppy disk. Even though it was a straightforward virus that made use of symmetric cryptography, victims had to spend $189 to a P.O. Box in Panama in order to get back access to their systems [1]. Started from this attack the world has been through several small and big ransomware attacks.

According to DarkReading, the spike in ransomware assaults in 2023—which increased by more than 95% from the year before—brought home the severity of cyberthreats. This sharp increase in instances highlights a worrisome trend: according to Statista, almost 72% of organizations worldwide have experienced these kinds of attacks. The frequency of these attacks has surpassed the entire number of cases documented in 2021 and 2022, indicating a concerning increase in ransomware operations. Based on the amount of exploited vulnerabilities, the media, leisure, and

entertainment sectors were found to be the most susceptible to these attacks. According to another Statista research, 36% of firms had a breach as a result of exploited vulnerabilities. Malicious email and credential compromise came in second and third, respectively, as the main reasons for these breaches [2].

The financial consequences of ransomware attacks are also a cause for concern. As per GetAstra, the average cost of an assault in 2023 was almost US$ 1.85 million. The overall background of data breaches, whose average worldwide cost has surged to US$ 4.45 million, indicating a 15% increase over three years, according to IBM's statistics, exacerbates this financial burden. 51% of firms are preparing for additional security spending due to these financial consequences; these investments will be concentrated in areas like staff training, incident response planning, and improving threat detection and response capabilities. Additionally, IBM emphasizes the enormous cost-saving potential of security AI and automation technologies, which, when widely used, can result in average savings of US$ 1.76 million in comparison to businesses that do not adopt these technologies.

Despite its extensive impact and the considerable disruption, it caused to over 230,000 machines in 150 countries, the WannaCry ransomware attack in May 2017 did not create as much financial damage from ransom payments as one might anticipate given its scope. The victims were told that in order to have their encrypted data back, they needed to pay $300–600 in Bitcoin. Surprisingly, considering the scope of the attack and the possibility of larger money demands, the total ransom paid by victims was not very significant. Runescape estimates that the attackers made about $130,000 in ransom payments. But the actual ransom payments only make up a small portion of the WannaCry attack's total financial damage. Globally, the wider economic ramifications were billions of dollars and included lost productivity, forensic investigation, data recovery, and long-term expenditures related to protecting systems from future attacks. Significant operational disruptions were experienced by crucial industries like government services, finance, and healthcare (such as the UK's National Health Service), which greatly increased the attack's overall economic cost. The WannaCry outbreak brought to light the critical need of maintaining good cybersecurity practices, the necessity of applying software updates on time, and the worldwide difficulties associated with containing and reducing the impact of pervasive cyberthreats[3].

3. Literature Review

3.1 Traditional Method of Ransomware

Many methods have been created in the rapidly changing field of cybersecurity to identify and lessen ransomware assaults, each with pros and cons of their own. An Application Programming Interface (API)-based Ransomware Detection System (API-RDS) is described in Paper [9]. It uses an Android app API package scan and static analysis to identify dangerous and benign apps. It does not require an emulator or sandbox and has a 97% accuracy rate across 2,959 samples; nevertheless, its dynamic analysis capabilities are limited[9].

It presents a thorough method that uses Support Vector Machine (SVM) to create estimators and combines ensemble fusion, anomaly-based estimators, and decision fusion[10]. By employing majority voting and OR logic to identify early phases of ransomware attacks, this method achieves a 99% accuracy rate across 12,000 samples by integrating the judgment of anomaly estimators with the vote result of homogenous ensembles through different OR logic[11]. With a 92% accuracy rate over 24,486 samples, a data analytics-based methodology is given with the goal of detecting ransomware families with a small dataset and little information. However, its credibility is limited by the absence of threat intelligence data[12].

Examines the efficacy of anti-spyware solutions that use malware footprint monitoring to identify, stop, and remove executable files from computers as well as limit network traffic. The method's significant CPU and storage consumption are mentioned as limitations, despite its 93% accuracy rate across 4,951 samples[13].

With a 92% accuracy rate across 2,121 samples, UNVEIL, which is covered in article [14], represents a substantial improvement in detecting evasive ransomware. It does this by simulating user experiences to identify malware interactions and system desktop modifications. However, its application is limited as it does not support kernel-level attacks[15]. A permissions-based ransomware detection system for Android OS is described in Paper [16]. It evaluates different permissions and has a 96.9% accuracy rate with 1,000 samples, while examining fewer features than some other approaches[17]. Though praised for its simplicity, the Cyber Kill Chain (CKC) model in paper [18] is critiqued for its narrow scope of ransomware consideration. It helps the modeling of ransomware attack strategies and hazardous behavior evaluation on endpoint devices[19].

Pay-break, a hybrid strategy that uses key escrow mechanisms for file encryption and achieves 90% accuracy over 1,691 samples, is described in Paper [20]. It is very good at keeping session keys safe in a vault, but it still has trouble deciphering newly discovered ransomware keys[21]. The last solution is presented in paper [22], which is appropriate for huge numbers of files, but focuses exclusively on particular system components. It employs decoy machines to screen files and monitor Windows' Event Sentry in order to identify unwanted access[23]. The research reveals gaps in ransomware detection methods, including limited dynamic analysis, lack of threat intelligence integration, and challenges with scalability and resource efficiency. Many approaches, such as API-RDS and UNVEIL, focus on specific attack surfaces, leaving other vectors unaddressed. Models like the Cyber Kill Chain provide narrow insights, and methods like Pay-break struggle with evolving ransomware, highlighting the need for more adaptive and comprehensive solutions.

3.2 Stages of Ransomware Impact

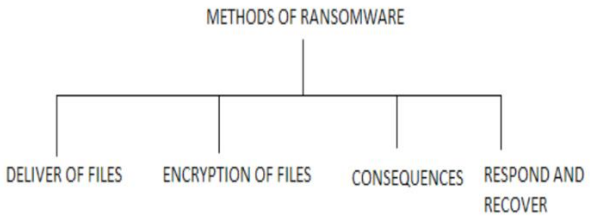


Figure 1[9]

Delivery of Files

The main ways that ransomware spreads are through files, links, or emails, which frequently contain documents and websites that the malware uses to propagate[24]. The two main ways that hackers compromise systems are via email and internet downloads. The majority of attackers use phishing techniques to initiate email-based attacks. Executable files may also be used by them. Crypto-ransomware often propagates via targeted file formats[9].

Encryption of Files

Once installed on a device, the malware activates upon delivery and starts encrypting specific files. For example, Petya concentrates on encrypting the Master Boot Record, whereas TeslaCrypt targets particular file types for encryption. A ransom notice requesting payment in bitcoin or other cryptocurrencies appears on the system after the data has been successfully encrypted[25]. The perpetrators put pressure on the victim by imposing a deadline for payment. The attacker offers to deliver the decryption keys in exchange for payment of the ransom, which will unlock the encrypted system files.

Consequences

Consequences are the results or repercussions of a certain issue, and in the current digital era, security is of utmost importance. The consequences of security breaches can include lost data, monetary losses, damaged reputations, and, in the worst situations, even the death of the victim from the shock and emotional upheaval[26]. Access to these files is extremely limited in cases where files are encrypted, and data is hacked. These kinds of attacks are becoming common, which emphasizes how serious a problem ransomware is. For example, if a ransomware assault hits the database of an educational institution, it may cause the loss of important data and information. As a result, it is crucial to address and mitigate the threats posed by ransomware[9].

Respond and Recover

Disconnecting the device from the internet is the first and most important thing you should do. This stops more dissemination or data transfer. After that, you should check all of your devices

and cloud storage data for vulnerabilities that could have been compromised. If at all feasible, identifying the precise ransomware variant in question can be very helpful in determining the best course of action. To get rid of the ransomware, think about resetting the device and doing a fresh OS installation[27]. To recover deleted data, restore files from backups once the system has been secured. To stop such assaults, it's also critical to constantly assess and upgrade your security software. Finally, in order to record the attack and maybe obtain additional support, it is imperative that you report the occurrence to the appropriate authorities[9].

3.3 Causes of Ransomware Attacks

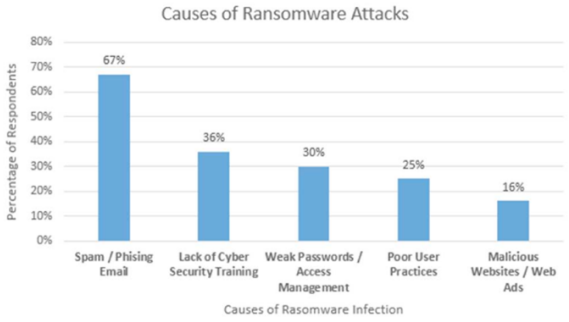


Figure 2[28]

Five key attack vectors are identified by Statista [28] as the primary causes of ransomware assaults. In 67% of cases, ransomware is successfully introduced into the system via spam or phishing emails. Three quarters of successful attacks are attributed to a lack of cyber security training[29]. Thirty percent of successful ransomware assaults were determined to be the result of weak passwords or access management. In addition, dangerous websites and bad user behavior contributed to the rise of ransomware attacks as the main attack vectors[30].

3.4 Ransomware attack steps

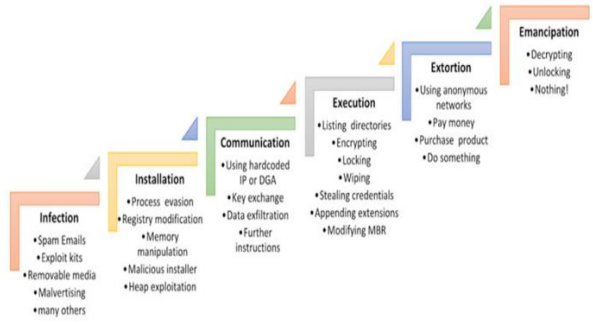


Figure 3 [31]

The first phase is called **infection**, during which the virus uses a variety of techniques to get inside the system[32]. One popular vector is spam emails that contain malicious links or attachments. Another is exploit kits, which look for and take advantage of system vulnerabilities. Additionally, removable media like USB drives that have been infected with ransomware or malvertising—the practice of using web adverts to distribute malware—can also result in infection. Several more techniques are also used to start the attack[31].

The malware embeds itself in the system during the **installation phase**, which comes after infection. To ensure that the virus remains active even after a reboot, this may entail modifying programs or making changes to the system registry in order to avoid detection[33]. In addition, attackers might use memory manipulation to launch a rogue installation that poses as trustworthy software or run ransomware code. Memory space vulnerabilities may be exploited with methods such as heap exploitation[31].

In the following phase, known as **communication**, the ransomware connects to the attacker's server. This sometimes entails utilizing a key exchange to safely transfer encryption keys in addition to a hardcoded IP address or a Domain Generation Algorithm (DGA) for communication[34]. This stage could potentially involve getting more instructions from the attackers or removing private information from the victim's PC[31].

The ransomware executes its malicious operations during the **attack's active phase**. Listing directories could be the first step in finding files for encryption. After that, the virus encrypts, locks, or deletes files to essentially prevent the user from accessing them[35]. During this phase, new extensions for encrypted files may be added and credentials may be stolen. Certain types of ransomware alter the Master Boot Record (MBR), making it impossible for the operating system to start up normally[31].

Extortion is the penultimate stage, during which the assailants make demands of the victim. Typically, this entails using secure anonymous networks to demand a ransom, frequently in bitcoin[36]. The attacker may order the victims to make a payment, buy a product that promises to decrypt files, or carry out another job[31].

The aftermath of the event is finally described in the **emancipation stage**. Once the ransom is paid, victims can utilize a decryption key that unlocks their files, or they can figure out other ways to get access to their machine[37]. Sadly, there are situations where there is no way out and victims are left with nothing since they cannot, no matter how hard they try or how compliant they are, retrieve their encrypted data[31].

3.5 Flowchart of Ransomware implementation

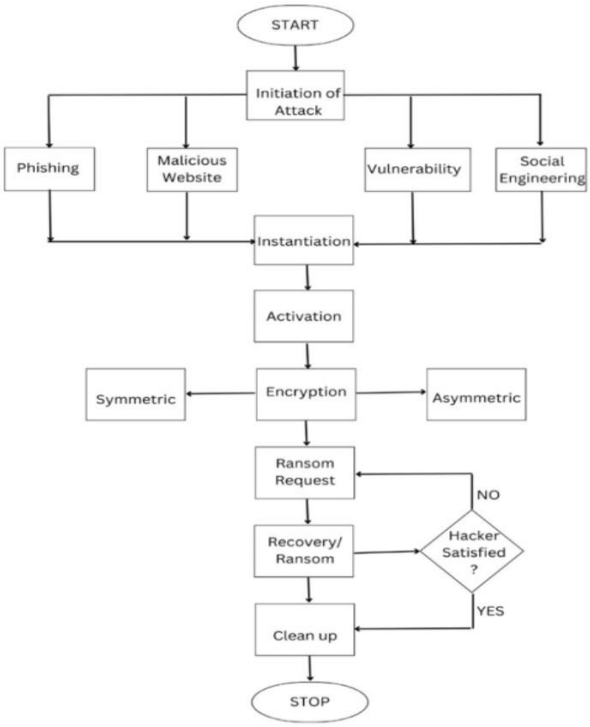


Figure 4[1]

Start: The ransomware assault procedure has begun at this point[1]. **Attack Initiation**: This stage deals with the first techniques employed to start a ransomware attack. It may happen in a number of ways[1]:

- **Phishing** is a type of attack where malicious emails or other false communications are used to fool people into disclosing personal information or downloading malware[38][39][40].
- **Malicious Website**: Websites designed to introduce malware into a user's computer or trick users into divulging personal information are referred to as malicious websites[41][42][43].
- **Vulnerability**: The ability to obtain unauthorized access or do harm by taking advantage of security flaws in software or systems[44][45][46].
- **Social engineering** is the psychological trickery used to coerce someone into doing something or disclosing private information[47][48][49].

Instantiation: After the initial attack vector is successful, the ransomware is established or set up in the system using this step[1].

Activation: The moment the ransomware inside the compromised system initiates its harmful payload[1].

Encryption: Ransomware's primary function is to encrypt the victim's files. It usually does this in one of two ways[1]:

- **Symmetric encryption** is a kind of encryption in which data is encrypted and decrypted using the same key[50].
- **Asymmetric encryption** uses two keys: a public key for encryption and a private key for decryption. This makes it harder to reverse without the private key[51].

Ransom Request: After encrypting the victim's files, the attacker notifies them of the ransom demand and requests payment in order to unlock the contents[1]. **Recovery/Ransom**: At this point, the victim must decide whether to pay the ransom in the hopes that the attacker would supply the decryption key, or try to recover through alternative methods[1].

- If the answer is NO (ransom not paid or recovery not accomplished), the cycle might continue or get worse.
- The procedure advances to the following stage if the answer is YES (ransom paid and hacker satisfied).

Clean Up: Depending on how honest they are, the attacker may either clean up their tracks or fulfill their promise to decrypt files. The victim might also have to restore systems from backups and clean them up[1].

Stop: The ransomware attack's termination, ideally with the machine operating normally again[1].

3.6 Most Common Type of Ransomware

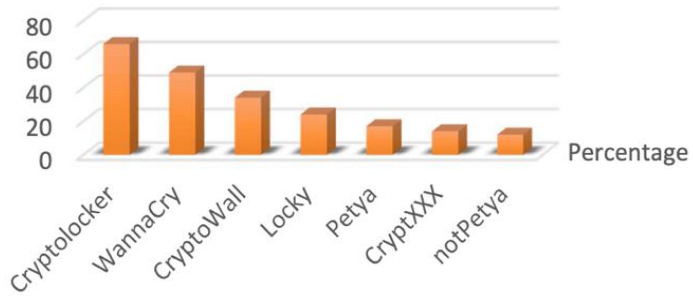


Figure 5[52]

CryptoLocker: This early ransomware first appeared in or around 2013. On compromised Windows PCs, it is well known for encrypting files and requesting a ransom—usually in Bitcoin—for the decryption key[53]. It was one of the earliest ransomware campaigns that demand payment in cryptocurrency and spread mostly through email attachments[52].

WannaCry: In May 2017, one of the most well-known ransomware attacks to date, WannaCry, started to spread over the world[54]. It took advantage of a flaw in Microsoft Windows operating

systems called EternalBlue, which was allegedly created by the National Security Agency of the United States. Hundreds of thousands of machines in 150 countries were impacted by the attack, which caused serious disruptions in a number of industries, including healthcare[52].

CryptoWall: Another ransomware that targets Windows users, CryptoWall initially surfaced in 2014. It behaves in a manner akin to CryptoLocker, encrypting files and requesting a ransom[55]. It has undergone multiple iterations, each bringing new and more advanced methods for evading detection and making it more difficult to get the files without paying the ransom[52]. **Locky**: First discovered in 2016, Locky is mainly distributed via spam emails that have malicious attachments[56]. After it is run, it encrypts several different kinds of files and requests a ransom to decrypt them. Locky is renowned for altering filenames and adding a distinctive extension, which makes it challenging to distinguish between the original files[52].

Petya: Originally identified in 2016, Petya is distinct from conventional ransomware in that it encrypts the master file table (MFT), which keeps the entire file system unreadable, as opposed to encrypting individual files[57]. As a result, it prevents the system from starting normally, thereby encrypting the entire system rather than just particular files[52].

CrypXXX: Initially discovered in 2016, this ransomware encrypts files on compromised systems and requests a payment[58]. It is well renowned for its capacity to encrypt a wide variety of file types in addition to stealing Bitcoin from victims' computers[52].

NotPetya: First identified in 2017, NotPetya was initially believed to be a variation of Petya because of similarities in how both programs encrypt the master boot record[59]. Nevertheless, its true purpose is to propagate via business networks and do damage rather than make money by demanding ransom payments. It spreads by a variety of means and has cost international organizations money and caused serious disruptions[52].

Of the ransomware kinds displayed, CryptoLocker has the largest percentage—well over 60%—making it the most common. Around 40% is also a sizable portion for WannaCry. The remaining ones, which are all below 20%, have notably smaller percentages: CryptoWall, Locky, Petya, CrypXXX, and NotPetya[52][60].

4. Systematic Review

4.1 Introduction

The goal of the aforementioned systematic review is to perform a thorough and rigorous study of the body of literature on ransomware and cybersecurity. The review aims to employ the abundance of previously conducted studies that have been identified, evaluated, and interpreted to create a well-informed response to the research topic that has been addressed. The main goal is to create a comprehensive dataset about cybersecurity tactics and ransomware, understanding how they are changing and identifying how they affect different industries. This compilation will aid in the development of strong countermeasures as well as the knowledge of how various sectors are

impacted. Researchers and practitioners can obtain a comprehensive overview of current trends and defenses in the field through this systematic review, which may result in the development of more potent cybersecurity policies and technologies.

4.2 The Objectives

- To examine the changing approaches and techniques used in ransomware attacks, with focus on current occurrences.
- To determine the main forces that have shaped the development of ransomware tactics, such as the economic forces and technological developments that have shaped the ransomware business model.
- Analyze how ransomware attacks affect different industries, such as the healthcare industry, and essential infrastructure.
- Investigating the methods used by enterprises to respond to and mitigate ransomware threats.

To make suggestions for better public policy and cybersecurity measures to effectively counteract the growing menace of Ransomware attacks.

4.3 Method

We have used The Kitchenham approach for this systematic review. The Kitchenham approach [61][62][63][64][65][66] is a well-established framework consisting of six basic stages that serves as the foundation for this systematic review. Establishing specific research questions that define the parameters and scope of the review is the first step in the process. Creating a thorough search strategy to find pertinent primary research papers is the second step. The critical evaluation of the gathered papers for quality is the third step that comes next. This involves a thorough scan to weed out the papers that don't meet predetermined inclusion and exclusion criteria, paying close attention to titles, abstracts, and other important details. Data extraction from the remaining papers, which have satisfactorily fulfilled all requirements, is the fourth step. The information gleaned from the papers is arranged into tables for additional examination in the fifth stage of data analysis and classification. All of these steps are combined into three main stages for better understanding and orderly development as shown in Figure 6 below.

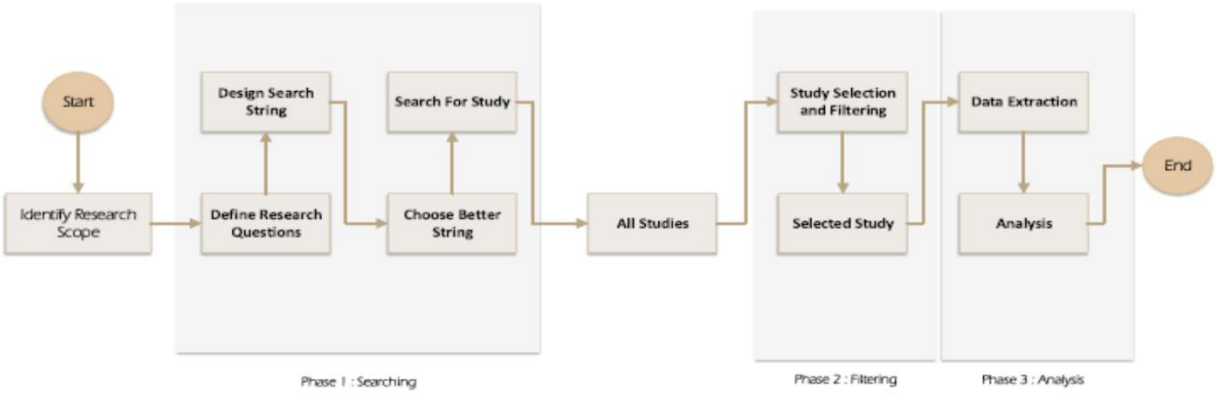


Figure 6 [63].

In Phase 1 Searching: Research questions that direct the entire review are developed, laying the foundation for the study. These inquiries directly impact how the search string is constructed. A search string is finished to guarantee that the material retrieved is strictly applicable to the study's focus following many trials and an experimental refinement process[63].

Phase 2 Filtering: Using a set of criteria, publications are reviewed as part of a selection process where the research is conducted. To filter the literature and keep the most pertinent publications, this is strictly applied to the title, abstract, and eight more inclusion and exclusion criteria[63].

Phase 3, Analysis: In order to directly address the research issues, data are carefully extracted from the 121 main publications that were selected for this study. The data is carefully analyzed and understood through the use of organizational tools such as tables and figures. The steps within these phases will be discussed in the following sections; Figure 6 shows the inputs and outputs of each stage[63].

4.4 Research Questions

1. How does AI help protect against ransomware?
2. How do advanced detection technologies improve real-time cybersecurity against ransomware?
3. What are the key aspects of cybersecurity frameworks to counter new ransomware without compromising privacy or performance?

4.5 Search Strategy

The study that initiated this research demonstrates how much consideration is needed when crafting the perfect search phrase for a systematic review. "Cybersecurity" and "ransomware" were the study's original two main keywords. Six more terms that are related to cyber risks and four more terms that are related to ransomware were added to the list. The goal is to create a search string that works well and produces a reasonable amount of pertinent papers from a list of

databases. In order to do this, a wide range of synonyms taken from earlier research was examined, leading to the creation of twenty-four different search string combinations. Then these words were used in five well-known databases: ACM, AIS, Eric, IEEE, and Sage Journal. The Boolean operators 'AND' and 'OR' were used to combine the search string and add different synonymous expressions. This rigorous process is essential to refine the search terms and ensure the acquisition of pertinent literature for the review.

Table 1: Search String Tries on the Selected Data Bases

Strings	Database	Number of papers
Cyber threats AND Encryption	IEEE AIS SAGE ACM ERIC	16 1 5 Total 2 (24) 0
Cyber threats AND Incident response	IEEE AIS SAGE ACM ERIC	23 1 3 Total 1. (28) 0
Cyber threats AND Vulnerability assessment	IEEE AIS SAGE ACM ERIC	4 0 1 Total 0 (5) 0
Cyber threats AND Data protection	IEEE AIS SAGE ACM ERIC	7 0 1 Total 0. (8) 0
Cyber threats AND Threat analysis	IEEE AIS SAGE ACM ERIC	1 2 0 Total 0. (3) 0
Cyber threats AND Cyber Resilience	IEEE AIS SAGE ACM ERIC	9 0 0 Total 0. (9) 0
Malware attack AND Encryption	IEEE AIS SAGE	10 1 0 Total

	ACM ERIC	1. (13) 1
Malware attack AND Incident response	IEEE AIS SAGE ACM ERIC	2 1 3 Total 0. (6) 0
Malware attack AND Vulnerability assessment	IEEE AIS SAGE ACM ERIC	1 0 2 Total 0. (3) 0
Malware attack AND Data protection	IEEE AIS SAGE ACM ERIC	1 0 3 Total 0. (7) 3
Malware attack AND Threat analysis	IEEE AIS SAGE ACM ERIC	13 0 0 Total(14) 0 1
Malware attack AND Cyber Resilience	IEEE AIS SAGE ACM ERIC	5 0 9 Total(18) 0 4
Crypto ransomware AND Encryption	IEEE AIS SAGE ACM ERIC	19 0 1 Total(27) 7 0
Crypto ransomware AND Incident response	IEEE AIS SAGE ACM ERIC	0 0 0 Total(6) 6 0
Crypto ransomware AND Vulnerability assessment	IEEE AIS SAGE ACM ERIC	0 0 0 Total(0) 0 0
Crypto ransomware AND Data protection	IEEE AIS SAGE	4 0 0 Total(4)

	ACM	0
	ERIC	0
Crypto ransomware AND Threat analysis	IEEE	2
	AIS	2
	SAGE	0 Total(5)
	ACM	1
	ERIC	0
Crypto Ransomware AND Cyber Resilience	IEEE	0
	AIS	0
	SAGE	0 Total(1)
	ACM	1
	ERIC	0
Cybersecurity breach AND Encryption	IEEE	0
	AIS	2
	SAGE	0 Total(3)
	ACM	1
	ERIC	0
Cybersecurity breach AND Incident response	IEEE	2
	AIS	0
	SAGE	0 Total(2)
	ACM	0
	ERIC	0
Cybersecurity breach AND Vulnerability assessment	IEEE	0
	AIS	0
	SAGE	0 Total(0)
	ACM	0
	ERIC	0
Cybersecurity breach AND Data protection	IEEE	2
	AIS	0
	SAGE	0 Total(2)
	ACM	0
	ERIC	0
Cybersecurity breach AND Threat analysis	IEEE	1
	AIS	1
	SAGE	0 Total(1)
	ACM	0
	ERIC	0
Cybersecurity Breach AND Cyber Resilience	IEEE	2
	AIS	0
	SAGE	0 Total(2)
	ACM	0
	ERIC	0

4.6 Paper Selection Criteria

After applying the title, abstract, and full-text reading, the papers were chosen. To choose which papers to read, though, some required reading the entire text. To choose the primary studies, inclusion and exclusion criteria have been employed. The research is contingent upon adherence to the inclusion and exclusion criteria provided by [61][66] [67].

The inclusion criteria

IC1/ Only the full text obtained.

IC2/ Only titles in English language.

IC3/ Only papers that has related titles.

IC4/ Only papers that has related abstract.

IC5/ Available for free download.

IC6/ Only papers depend scientific method.

IC5/ Date of publication (2008-2019).

IC6/ Only peer reviewed.

IC7/ Only related studies

Exclusion Criteria

EC1/ Duplicate titles.

EC2/ Papers are not in English language.

EC3/ None of (editorials, prefaces, discussions, magazines, proposals, summaries of tutorials and panels).

EC4/ None of grey literature (this refers to unpublished material/published in a non-commercial form) like Open Grey (http://www.opengrey.eu/), for example: presentation slides, technical reports, white papers, or books and book chapters.

EC5/ Can not full text Obtained.

EC6/ Not available for download

EC7/ The title is not related.

EC8/ The abstract is not related.

EC9/ Not peer reviewed papers.

EC10/The papers that are not related to our research domain, like the Government sector.

EC11/ The study scope is out of our interest.

Filter 1: This filter excluded the papers that were unobtainable as full text. The final number of paper (199)

Filter 2: Exclude the papers that are not available for download. Some of the papers cannot be downloaded. The final number of paper (199).

Filter 3: Exclude not peer reviewed papers. All the selected papers primary studies should be peer reviewed (conferences, journals, workshops, proceedings, information system association).

The final number of paper (195).

Filter 4: Exclude the duplicate papers (some papers have been found in more than one database). The final number of paper (156)

Filter 5: This filter excluded the papers with titles that were not written English language. The final number of paper (155)

Filter 6: Exclude grey papers (presentation slides, technical reports, white papers, or books and book chapters). The final number of paper (151)

Filter 7: Exclude the papers with not related titles. After reading and analyzing the title, the titles

(115)

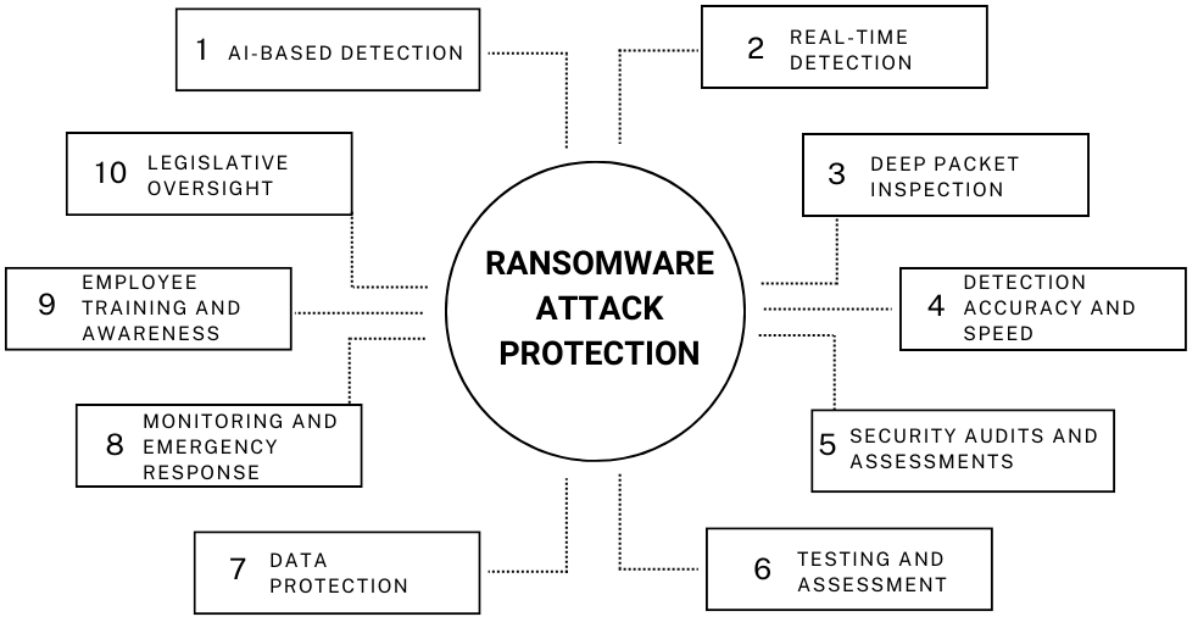
Filter 8: Exclude the papers that have no scientefic method. Some papers are not following a78 scientific method (quantitative or qualtitative study), e.g. political reports. The final number of paper (94)

Filter 9: Take papers published in between 2017 and 2023. The final number of paper (94)

Table 2: The Number of the Primary studies

Data base	**Number of Primary studies**
ACM	7
AIS	6
Eric	4
IEEE	59
Sage 9	18
Total	**94**

5. Detection and Prevention Techniques



1. **AI-Based Detection Systems**: To develop extremely precise ransomware detection systems, make use of artificial intelligence's (AI) capabilities, with a focus on convolutional neural networks (CNNs). By analyzing patterns and abnormalities in data that are indicative of ransomware, these AI models are able to identify any threats early on and stop them before they can do any damage[68].
2. **Real-Time Detection**: Combine Intrusion Detection Systems (IDS) with AI-driven detection algorithms to continually monitor network activities. With the help of this integration, enterprises may quickly identify suspicious actions that could be signs of a ransomware attack and take action to minimize any damage[68].
3. **Deep Packet Inspection**: Examine incoming network traffic by using specific ransomware detection algorithms in conjunction with deep packet inspection techniques. By identifying and isolating ransomware payloads, this examination can stop them from infecting digital systems, especially those in vital infrastructure networks[69].
4. **Enhancement of Detection Accuracy and Response Speed**: Pay attention to research and development in order to improve the accuracy of currently used detection techniques and reduce the latency associated with ransomware identification. This upgrade is essential for operational settings when minimizing the effects of an attack requires quick action[70].
5. **Frequent Testing and Security Assessments**: To find and fix vulnerabilities in advance, test security systems frequently and methodically. These evaluations can indicate whether more extensive security management adjustments are necessary or if possible, security issues can be handled with technological fixes[71].

6. **Monitoring and Emergency Response Procedures**: Set up thorough security monitoring hubs that manage ransomware threats throughout their whole lifecycle. For cybersecurity crises, it is imperative to create and improve emergency response frameworks that include regular simulation drills, fast response teams, defined response protocols, and continuous staff training[71].
7. **Data protection and security management**: To make recovery easier in the event that data is held ransom, classify and encrypt important data and make sure frequent backups are made to offsite or cloud storage. To improve overall security posture, implement strict security management procedures such as asset management, strong identity verification, network segmentation, and strict access controls[70].
8. **Legislative Measures and Oversight**: Promote the creation and application of laws pertaining to ransomware. Establishing uniform protocols for the reporting of ransomware events and payments, elucidating the legal ramifications for launching ransomware attacks online, and fostering a legal climate that discourages cybercrime are all important components of these legislation[72].
9. **Employee Training and Awareness Programs**: Provide ongoing education to all staff members, with a focus on cybersecurity best practices and awareness. Employees with knowledge are the first line of defense against ransomware attacks because they are able to identify possible dangers and steer clear of acts that can jeopardize the digital assets of the company[68].
10. **Consistent Security Audits and Incentivized Assessments**: Establish incentives for frequent security audits by forming alliances with cyberinsurance companies. These audits have the ability to highlight gaps in the present security framework and motivate businesses to keep their security procedures current, which may improve their insurance prices or coverage alternatives[73].

6. Conclusion & Recommendations

The dynamic and evolving nature of ransomware attacks across multiple industries has been critically explored in this research, exposing the sophistication and growing frequency of these cybersecurity threats. This research has shed light on the serious operational and financial consequences that ransomware poses to organizations through a thorough case study analysis. This has underlined the urgent need for strong cybersecurity defenses and a better comprehension of ransomware strategies. The results of the study highlight the significance of ongoing developments in defensive tactics and detection systems that are adapted to changing attack techniques. It is clear that ransomware not only causes a large financial cost but also acts as a trigger for extensive delays to operations. As a result, this study supports a multi-layered security strategy that includes enhanced threat detection systems, frequent personnel security training, and thorough incident response strategies.

The report also recommends improved legal frameworks to ward off fraudsters and safeguard susceptible systems from these ubiquitous attacks. The goal of the paper is to create a collaborative atmosphere that will enable cybersecurity experts, legislators, and business executives to design more efficient anti-ransomware strategies. In conclusion, research and development in cyber defense tactics must advance at a rate commensurate with the rate at which ransomware continues to adapt and elude conventional cybersecurity protections. Future research aiming at reducing the dangers associated with ransomware and strengthening the resilience of digital infrastructures globally should be built upon the lessons gathered from this study.

7. Bibliography

[1] B. J. Chinmaya, S. A. Kudtarkar, and Mohana, "Targeted Ransomware Attacks and Detection to Strengthen Cybersecurity Strategies," in 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India: IEEE, Dec. 2023, pp. 1039–1044. doi: 10.1109/ICACRS58579.2023.10404203.

[2] M. Medhat, M. Essa, H. Faisal, and S. G. Sayed, "YARAMON: A Memory-based Detection Framework for Ransomware Families," in 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST), London, United Kingdom: IEEE, Dec. 2020, pp. 1–6. doi: 10.23919/ICITST51030.2020.9351319.

[3] N. Aldaraani and Z. Begum, "Understanding the impact of Ransomware: A Survey on its Evolution, Mitigation and Prevention Techniques," in 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh: IEEE, Apr. 2018, pp. 1–5. doi: 10.1109/NCG.2018.8593029.

[4] Mulungushi University/Department of Computer Science & Information Technology, Kabwe, 10101, Zambia, A. Zimba, and M. Chishimba, "Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures," IJCNIS, vol. 11, no. 1, pp. 26–39, Jan. 2019, doi: 10.5815/ijcnis.2019.01.03.

[5] J. Chen, C. Wang, Z. Zhao, K. Chen, R. Du, and G.-J. Ahn, "Uncovering the Face of Android Ransomware: Characterization and Real-Time Detection," IEEE Trans.Inform.Forensic Secur., vol. 13, no. 5, pp. 1286–1300, May 2018, doi: 10.1109/TIFS.2017.2787905.

[6] K. Cabaj and W. Mazurczyk, "Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall," IEEE Network, vol. 30, no. 6, pp. 14–20, Nov. 2016, doi: 10.1109/MNET.2016.1600110NM.

[7] F. Aldauiji, O. Batarfi, and M. Bayousef, "Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks: A Survey of the State of the Art," IEEE Access, vol. 10, pp. 61695–61706, 2022, doi: 10.1109/ACCESS.2022.3181278.

[8] M. Husak, "Towards a Data-Driven Recommender System for Handling Ransomware and Similar Incidents," in 2021 IEEE International Conference on Intelligence and Security

Informatics (ISI), San Antonio, TX, USA: IEEE, Nov. 2021, pp. 1–6. doi: 10.1109/ISI53945.2021.9624774.

[9] A. Bertia, S. B. Xavier, G. J. W. Kathrine, and G. M. Palmer, "A Study about Detecting Ransomware by Using Different Algorithms," in 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India: IEEE, May 2022, pp. 1293–1300. doi: 10.1109/ICAAIC53929.2022.9792587.

[10] B. E. M. Yamany and M. A. Azer, "SALAM Ransomware Behavior Analysis Challenges and Decryption," in 2021 Tenth International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, Egypt: IEEE, Dec. 2021, pp. 273–277. doi: 10.1109/ICICIS52592.2021.9694154.

[11] School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, Johor Bahru, Johor 81310, MALAYSIA et al., "Zero-Day Aware Decision Fusion-Based Model for Crypto-Ransomware Early Detection," IJIE, vol. 10, no. 6, Nov. 2018, doi: 10.30880/ijie.2018.10.06.011.

[12] C. G. Akcora, Y. Li, Y. R. Gel, and M. Kantarcioglu, "BitcoinHeist: Topological Data Analysis for Ransomware Detection on the Bitcoin Blockchain," 2019, doi: 10.48550/ARXIV.1906.07852.

[13] D. Javaheri, M. Hosseinzadeh, and A. M. Rahmani, "Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines," IEEE Access, vol. 6, pp. 78321–78332, 2018, doi: 10.1109/ACCESS.2018.2884964.

[14] E. Kirda, "UNVEIL: A large-scale, automated approach to detecting ransomware (keynote)," in 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER), Klagenfurt, Austria: IEEE, Feb. 2017, pp. 1–1. doi: 10.1109/SANER.2017.7884603.

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

[16] S. Alsoghyer and I. Almomani, "On the Effectiveness of Application Permissions for Android Ransomware Detection," in 2020 6th Conference on Data Science and Machine Learning Applications (CDMA), Riyadh, Saudi Arabia: IEEE, Mar. 2020, pp. 94–99. doi: 10.1109/CDMA47397.2020.00022.

[17] B. Reidys, P. Liu, and J. Huang, "RSSD: defend against ransomware with hardware-isolated network-storage codesign and post-attack analysis," in Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating

Systems, Lausanne Switzerland: ACM, Feb. 2022, pp. 726–739. doi: 10.1145/3503222.3507773.

[18] T. Dargahi, A. Dehghantanha, P. N. Bahrami, M. Conti, G. Bianchi, and L. Benedetto, "A Cyber-Kill-Chain based taxonomy of crypto-ransomware features," J Comput Virol Hack Tech, vol. 15, no. 4, pp. 277–305, Dec. 2019, doi: 10.1007/s11416-019-00338-7.

[19] A. Adamov and A. Carlsson, "Reinforcement Learning for Anti-Ransomware Testing," in 2020 IEEE East-West Design & Test Symposium (EWDTS), Varna, Bulgaria: IEEE, Sep. 2020, pp. 1–5. doi: 10.1109/EWDTS50664.2020.9225141.

[20] E. Kolodenker, W. Koch, G. Stringhini, and M. Egele, "PayBreak: Defense Against Cryptographic Ransomware," in Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, Abu Dhabi United Arab Emirates: ACM, Apr. 2017, pp. 599–611. doi: 10.1145/3052973.3053035.

[21] V. Marella, M. Roshan, J. Merikivi, and V. Tuunainen, "Rebuilding Trust in Cryptocurrency Exchanges after Cyber-attacks," presented at the Hawaii International Conference on System Sciences, 2021. doi: 10.24251/HICSS.2021.684.

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

[23] M. Alam, S. Bhattacharya, S. Dutta, S. Sinha, D. Mukhopadhyay, and A. Chattopadhyay, "RATAFIA: Ransomware Analysis using Time And Frequency Informed Autoencoders," in 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA: IEEE, May 2019, pp. 218–227. doi: 10.1109/HST.2019.8740837.

[24] U. Javed Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal, and A. Kumar, "Ransomware Threat and its Impact on SCADA," in 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, United Kingdom: IEEE, Jan. 2019, pp. 205–212. doi: 10.1109/ICGS3.2019.8688327.

[25] S. Yulianto and B. Soewito, "Ransomware Resilience: Investigating Organizational Security Culture and Its Impact on Cybersecurity Practices against Ransomware Threats," in 2023 International Conference on Informatics Engineering, Science & Technology (INCITEST), Bandung, Indonesia: IEEE, Oct. 2023, pp. 1–7. doi: 10.1109/INCITEST59455.2023.10396943.

[26] S. R. B. Alvee, B. Ahn, T. Kim, Y. Su, Y.-W. Youn, and M.-H. Ryu, "Ransomware Attack Modeling and Artificial Intelligence-Based Ransomware Detection for Digital Substations," in 2021 6th IEEE Workshop on the Electronic Grid (eGRID), New Orleans, LA, USA: IEEE, Nov. 2021, pp. 01–05. doi: 10.1109/eGRID52793.2021.9662158.

[27] I. Tunji, A. Chomchoey, N. Phromchan, and K. Chimmanee, "Ransomware Attack Analysis on Banking Systems," in 2023 7th International Conference on Information Technology (InCIT), Chiang Rai, Thailand: IEEE, Nov. 2023, pp. 121–125. doi: 10.1109/InCIT60207.2023.10412895.

[28] J. Johnson, "Leading cause of ransomware infection 2019," Statista. com, Jan, vol. 25, 2021.

[29] D. Zhuravchak, T. Ustyianovych, V. Dudykevych, B. Venny, and K. Ruda, "Ransomware Prevention System Design based on File Symbolic Linking Honeypots," in 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland: IEEE, Sep. 2021, pp. 284–287. doi: 10.1109/IDAACS53288.2021.9660913.

[30] M. N. Olaimat, M. Aizaini Maarof, and B. A. S. Al-rimy, "Ransomware Anti-Analysis and Evasion Techniques: A Survey and Research Directions," in 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia: IEEE, Jan. 2021, pp. 1–6. doi: 10.1109/CRC50527.2021.9392529.

[31] M. Keshavarzi and H. R. Ghaffary, "I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion," Computer Science Review, vol. 36, p. 100233, May 2020, doi: 10.1016/j.cosrev.2020.100233.

[32] H. Fujinoki and L. Manukonda, "Proactive Damage Prevention from Zero-Day Ransomwares," in 2023 5th International Conference on Computer Communication and the Internet (ICCCI), Fujisawa, Japan: IEEE, Jun. 2023, pp. 133–141. doi: 10.1109/ICCCI59363.2023.10210183.

[33] A. Khan and I. Sharma, "Machine Learning-Based Methodology for Preventing Ransomware Attacks on Healthcare Sector," in 2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), Chennai, India: IEEE, Nov. 2023, pp. 1–5. doi: 10.1109/RMKMATE59243.2023.10368971.

[34] C. Zhou et al., "Limits of I/O Based Ransomware Detection: An Imitation Based Attack," in 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA: IEEE, May 2023, pp. 2584–2601. doi: 10.1109/SP46215.2023.10179372.

[35] A. Zahra and M. A. Shah, "IoT based ransomware growth rate evaluation and detection using command and control blacklisting," in 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, United Kingdom: IEEE, Sep. 2017, pp. 1–6. doi: 10.23919/IConAC.2017.8082013.

[36] M. A. Aboud and K. Mariyappn, "Investigation of Modern Ransomware Key Generation Methods: A Review," in 2021 International Conference on Computer Communication and

Informatics (ICCCI), Coimbatore, India: IEEE, Jan. 2021, pp. 1–5. doi: 10.1109/ICCCI50826.2021.9402680.

[37] S. Karunakaran, M. Manimaraboopathy, M. Maharajothi, P. Kirubasagar, T. Subburaj, and S. Varun, "Internet of Things Assisted Automated Ransomware Recognition using Harmony Search Algorithm with Deep Learning," in 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India: IEEE, Nov. 2023, pp. 475–480. doi: 10.1109/ICSCNA58489.2023.10370175.

[38] J.-S. Ko, J.-S. Jo, D.-H. Kim, S.-K. Choi, and J. Kwak, "Real Time Android Ransomware Detection by Analyzed Android Applications," in 2019 International Conference on Electronics, Information, and Communication (ICEIC), Auckland, New Zealand: IEEE, Jan. 2019, pp. 1–5. doi: 10.23919/ELINFOCOM.2019.8706349.

[39] S. A. Wadho, A. Yichiet, G. M. Lee, L. C. Kang, R. Akbar, and R. Kumar, "Impact of Cyber Insurances on Ransomware," in 2023 IEEE 8th International Conference on Engineering Technologies and Applied Sciences (ICETAS), Bahrain, Bahrain: IEEE, Oct. 2023, pp. 1–6. doi: 10.1109/ICETAS59148.2023.10346341.

[40] J. Venkatesh, V. Vetriselvi, R. Parthasarathi, and G. Subrahmanya V.R.K. Rao, "Identification and isolation of crypto ransomware using honeypot," in 2018 Fourteenth International Conference on Information Processing (ICINPRO), Bangalore, India: IEEE, Dec. 2018, pp. 1–6. doi: 10.1109/ICINPRO43533.2018.9096875.

[41] A. Ferreira, "Why Ransomware Needs A Human Touch," in 2018 International Carnahan Conference on Security Technology (ICCST), Montreal, QC: IEEE, Oct. 2018, pp. 1–5. doi: 10.1109/CCST.2018.8585650.

[42] A. Turner, S. Mccombie, and A. Uhlmann, "Follow the money: Revealing risky nodes in a Ransomware-Bitcoin network," presented at the Hawaii International Conference on System Sciences, 2021. doi: 10.24251/HICSS.2021.189.

[43] J. Huang, J. Xu, X. Xing, P. Liu, and M. K. Qureshi, "FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas Texas USA: ACM, Oct. 2017, pp. 2231–2244. doi: 10.1145/3133956.3134035.

[44] S.-C. Hsiao and D.-Y. Kao, "The static analysis of WannaCry ransomware," in 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South): IEEE, Feb. 2018, pp. 153–158. doi: 10.23919/ICACT.2018.8323680.

[45] S. A. Wadho, A. Yichiet, M. L. Gan, L. C. Kang, R. Akbar, and R. Kumar, "Emerging Ransomware Attacks: Improvement and Remedies - A Systematic Literature Review," in 2023

4th International Conference on Artificial Intelligence and Data Sciences (AiDAS), IPOH, Malaysia: IEEE, Sep. 2023, pp. 148–153. doi: 10.1109/AiDAS60501.2023.10284647.

[46] M. M. Ahmadian and H. R. Shahriari, "2entFOX: A framework for high survivable ransomwares detection," in 2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), Tehran: IEEE, Sep. 2016, pp. 79–84. doi: 10.1109/ISCISC.2016.7736455.

[47] E. Btoush, X. Zhou, R. Gururaian, K. Chan, and X. Tao, "A Survey on Credit Card Fraud Detection Techniques in Banking Industry for Cyber Security," in 2021 8th International Conference on Behavioral and Social Computing (BESC), Doha, Qatar: IEEE, Oct. 2021, pp. 1–7. doi: 10.1109/BESC53957.2021.9635559.

[48] S.-B. Cheon, G.-Y. Choi, and D. Kim, "A Cheating Attack on a Whitelist-based Anti-Ransomware Solution and its Countermeasure," in 2023 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA: IEEE, Jan. 2023, pp. 01–04. doi: 10.1109/ICCE56470.2023.10043480.

[49] A. O. Almashhadani, M. Kaiiali, S. Sezer, and P. O'Kane, "A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware," IEEE Access, vol. 7, pp. 47053–47067, 2019, doi: 10.1109/ACCESS.2019.2907485.

[50] A. Alqahtani, M. Gazzan, and F. T. Sheldon, "A proposed Crypto-Ransomware Early Detection(CRED) Model using an Integrated Deep Learning and Vector Space Model Approach," in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA: IEEE, Jan. 2020, pp. 0275–0279. doi: 10.1109/CCWC47524.2020.9031182.

[51] M. Botes and G. Lenzini, "When Cryptographic Ransomware Poses Cyber Threats: Ethical Challenges and Proposed Safeguards for Cybersecurity Researchers," in 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy: IEEE, Jun. 2022, pp. 562–568. doi: 10.1109/EuroSPW55150.2022.00067.

[52] Ekta and U. Bansal, "A Review on Ransomware Attack," in 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India: IEEE, May 2021, pp. 221–226. doi: 10.1109/ICSCCC51823.2021.9478148.

[53] F. Manavi and A. Hamzeh, "A New Method for Ransomware Detection Based on PE Header Using Convolutional Neural Networks," in 2020 17th International ISC Conference on Information Security and Cryptology (ISCISC), Tehran, Iran: IEEE, Sep. 2020, pp. 82–87. doi: 10.1109/ISCISC51277.2020.9261903.

[54] M. Medhat, S. Gaber, and N. Abdelbaki, "A New Static-Based Framework for Ransomware Detection," in 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big

Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Athens: IEEE, Aug. 2018, pp. 710–715. doi: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00124.

[55] D. Garg, A. Thakral, T. Nalwa, and T. Choudhury, "A Past Examination and Future Expectation: Ransomware," in 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE), Paris: IEEE, Jun. 2018, pp. 243–247. doi: 10.1109/ICACCE.2018.8441743.

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

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

[58] T. Nusairat, M. M. Saudi, and A. B. Ahmad, "A Recent Assessment for the Ransomware Attacks Against the Internet of Medical Things (IoMT): A Review," in 2023 IEEE 13th International Conference on Control System, Computing and Engineering (ICCSCE), Penang, Malaysia: IEEE, Aug. 2023, pp. 238–242. doi: 10.1109/ICCSCE58721.2023.10237161.

[59] A. A. M. A. Alwashali, N. A. A. Rahman, and N. Ismail, "A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack," in 2021 14th International Conference on Developments in eSystems Engineering (DeSE), Sharjah, United Arab Emirates: IEEE, Dec. 2021, pp. 92–96. doi: 10.1109/DeSE54285.2021.9719456.

[60] P. Bajpai and R. Enbody, "An Empirical Study of Key Generation in Cryptographic Ransomware," in 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, Ireland: IEEE, Jun. 2020, pp. 1–8. doi: 10.1109/CyberSecurity49315.2020.9138878.

[61] J. Nwokeji, F. Aqlan, A. Anugu, and A. Olagunju, "Big Data ETL Implementation Approaches: A Systematic Literature Review (P)," presented at the The 30th International Conference on Software Engineering and Knowledge Engineering, Jul. 2018, pp. 714–721. doi: 10.18293/SEKE2018-152.

[62] A. Kaplan, K. Busch, A. Koziolek, and R. Heinrich, "Categories of Change Triggers in Business Processes," in 2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), Prague: IEEE, Aug. 2018, pp. 252–259. doi: 10.1109/SEAA.2018.00049.

[63] B. S. Ahmed, K. Z. Zamli, W. Afzal, and M. Bures, "Constrained Interaction Testing: A Systematic Literature Study," IEEE Access, vol. 5, pp. 25706–25730, 2017, doi: 10.1109/ACCESS.2017.2771562.

[64] I. Hydara, A. B. Md. Sultan, H. Zulzalil, and N. Admodisastro, "Current state of research on cross-site scripting (XSS) – A systematic literature review," Information and Software Technology, vol. 58, pp. 170–186, Feb. 2015, doi: 10.1016/j.infsof.2014.07.010.

[65] A. Freire et al., "Investigating gaps on Agile Improvement Solutions and their successful adoption in industry projects - A systematic literature review," presented at the The 30th International Conference on Software Engineering and Knowledge Engineering, Jul. 2018, pp. 40–55. doi: 10.18293/SEKE2018-185.

[66] F. Hujainah, R. B. A. Bakar, M. A. Abdulgabber, and K. Z. Zamli, "Software Requirements Prioritisation: A Systematic Literature Review on Significance, Stakeholders, Techniques and Challenges," IEEE Access, vol. 6, pp. 71497–71523, 2018, doi: 10.1109/ACCESS.2018.2881755.

[67] N. Qureshi, M. Usman, and N. Ikram, "Evidence in software architecture, a systematic literature review," in Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering, Porto de Galinhas Brazil: ACM, Apr. 2013, pp. 97–106. doi: 10.1145/2460999.2461014.

[68] A. Pillai, R. Kadikar, M. S. Vasanthi, and B. Amutha, "Analysis of AES-CBC Encryption for Interpreting Crypto-Wall Ransomware," in 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai: IEEE, Apr. 2018, pp. 0599–0604. doi: 10.1109/ICCSP.2018.8524494.

[69] R. Agrawal, J. W. Stokes, K. Selvaraj, and M. Marinescu, "Attention in Recurrent Neural Networks for Ransomware Detection," in ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, United Kingdom: IEEE, May 2019, pp. 3222–3226. doi: 10.1109/ICASSP.2019.8682899.

[70] M. Sukul, S. A. Lakshmanan, and R. Gowtham, "Automated Dynamic Detection of Ransomware using Augmented Bootstrapping," in 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India: IEEE, Apr. 2022, pp. 787–794. doi: 10.1109/ICOEI53556.2022.9777099.

[71] V. Oujezsky, P. Novak, T. Horvath, M. Holik, and M. Jurcik, "Data Backup System with Integrated Active Protection Against Ransomware," in 2023 46th International Conference on Telecommunications and Signal Processing (TSP), Prague, Czech Republic: IEEE, Jul. 2023, pp. 65–69. doi: 10.1109/TSP59544.2023.10197687.

[72] R. Agarwal, A. Chaudhary, D. Gupta, and D. Das, "Ransomware Vulnerability used in darknet for web application attack," in 2022 2nd International Conference on Emerging

Frontiers in Electrical and Electronic Technologies (ICEFEET), Patna, India: IEEE, Jun. 2022, pp. 1–5. doi: 10.1109/ICEFEET51821.2022.9847925.

[73] R. Upadhyaya and A. Jain, "Cyber ethics and cyber crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet," in 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India: IEEE, Apr. 2016, pp. 143–148. doi: 10.1109/CCAA.2016.7813706.