Journal of Engineering Faculty

| cumfad.cumhuriyet.edu.tr | Founded: 2023 Available online, ISSN Publisher: Sivas Cumhuriyet Üniversitesi

A systematic literature review on ransomware detection by evidence-based software engineering method

Engin Kuzu[1,a,] , Hakan Kekül[2,b*], Halil Arslan[3,c]

[1]Sivas Cumhuriyet University, Institute of Science, Sivas, Türkiye
[2]Sivas Cumhuriyet University, Faculty of Technology, Software Engineering, Sivas, Türkiye
[3]Sivas Cumhuriyet University, Faculty of Engineering, Computer Engineering, Sivas, Türkiye.
**Corresponding author*

Research Article

History

Received: 16/10/2024
Accepted: 07/11/2024

ABSTRACT

Ransomware attacks, which aim to take ransom by encrypting the files they infect with unbreakable passwords, have become an increasing threat in recent years. Decrypting encrypted files without data loss is nearly impossible without the encryption key. This often obliges ransomware victims to pay the amount of the ransom demanded. The purpose of our study is to present a systematic literature review of ransomware detection research. The method we base on while performing a systematic literature review is the Evidence-Based Software engineering approach. This approach is based on the Evidence-Based Medicine method, which has been successfully applied in many fields. Six steps of Evidence-Based Software Engineering have been implemented in sequence. For this purpose, 114 scientific articles, which fall within the scope of our research questions, were researched from the studies conducted between 2017 and 2022 on ransomware detection. According to our quality evaluation rules, 49 articles meeting our quality criteria were analyzed. The answers to our research questions, which we determined through the analyzed articles, are presented in detail.

Keywords: Evidence-Based Software Engineering; EBSE; Malware; Ransomware Detection; Ransomware Analysis

[a] *engin.kuzu@cumhuriyet.edu.tr* *0009-0008-2470-6944*
[c] *harslan@cumhuriyet.edu.tr* *0000-0003-3286-5159*
[b] *hakankekul@cumhuriyet.edu.tr* *0000-0001-6269-8713*

How to Cite: Kuzu E, Kekül H, Arslan H (2024) A systematic literature review on ransomware detection by evidence-based software engineering method, Journal of Engineering Faculty, 2(2): 64-77

Introduction

Evidence-based software engineering (EBSE) approach is based on the evidence-based medicine (EBM) approach. Evidence-based medicine is a method that aims to increase the clinical experience and treatment processes of physicians by presenting the best scientific evidence [1]. The main purpose of the EBM system is to publish valid and appropriately obtained evidence. In this way, doctors will be able to use proven methods obtained with EBM in the treatment process of the diseases they encounter. However, the main problem here is that there are many different researches and publications, and doctors do not have the opportunity to research all of these so-called primary sources for a particular disease. A systematic literature review standard was provided by scanning primary sources with the EBM system, which was produced as a solution to this problem [2]. Kitchenham et al. [3]Noting that this method, which is used in the field of medicine, has been successfully applied in many different fields, they announced Evidence-based software engineering (EBSE) studies in the field of software engineering.

With this study, a systematic review of the studies conducted in the literature on the detection of ransomware, which is one of the working areas of cyber security, was carried out with the EBSE method. A ransom is characterized as "cash paid with a specific end goal to free someone who has been captured" and "something demanded or paid to enable someone in captivity to be released from captivity" [4].

Ransomware is expressed ransomware, which is a combination of the words ransom (ransom) and software (software) in English. In fact, it is one of the types of malware. It is also referred to as blackmail software or ransom virus in some sources. Recently, they have become one of the most common threats due to their prevalence and ever-evolving nature. Its working principle is based on trying to extort money from the user by locking the target computer system or systems or by encrypting some or all of the files, preventing the user from accessing them [5].

Ransomware, which uses very advanced encryption schemes, can be used for many different purposes in the system they infiltrate by using software vulnerabilities, system weaknesses, social engineering weaknesses and user errors. Moreover, today's ransomware leaves almost no possibility to recover encrypted files [6]. Ransomware is defined as "a type of malicious software that restricts users from accessing their systems by locking/encrypting the system screen or users' files unless the ransom is paid." Malicious professionals reach their goals by developing a wide variety of methods and tactics and the possibility of being exposed to this situation becames a nightmare for users [7].

Technological advances create new opportunities for hackers. Malware has become a commercial sector by malicious people who are trying to gain financial gain by taking advantage of these opportunities. Moreover, this situation has turned into a challenge between software developers who prepare updates and security patches for security vulnerabilities and hackers who try to exploit these vulnerabilities. This vicious circle reveals how important the analysis is to ensure the working principles, impact and discovery of malware. Malware analysis is the process of revealing the potential effects of malicious software such as viruses, trojan horses, backdoors, rootkits, worms, determining their source and examining their functions. [8]. Thanks to this analysis, how malware works, its effects and harms can be understood. In addition, as a result of these analyzes, damages can be reduced or prevented. For this reason, the detection and prevention of ransomware, which has recently become one of the most effective and dangerous malware, has become an important research topic. Basically, the goal is to classify and isolate ransomware and benign software from each other. The basic requirement for the analysis of ransomware is to reveal the features of such software accurately. This is essential for developing an effective analysis algorithm [9].

What ransomware basically does is to render valuable data unusable with unbreakable encryption algorithms [10]. Considering the financial gain compared to other malware, ransomware threatens both companies and users [11]. The user who is exposed to a ransomware attack must choose to pay a certain amount of ransom or lose their data to decrypt their files. Hacker's generaliy demand ransoms in cryptocurrency. It is seen that the most demanded ransom is preferred as bitcoin. Another behavioral feature observed in ransomware is that it tries to communicate with a command-and-control server (C2C) to receive instructions. The purpose here is to download encryption keys and required additional files [7].

Vulnerabilities that have not yet been detected and fixed and are open to exploitation are called zero-day vulnerabilities. Although the effects of these vulnerabilities are more devastating, they are seen rarely. Therefore, an effective update and patch policy is important in preventing many cybersecurity threats. Otherwise, a system's vulnerability is open to exploitation until updates or patches are made. According to statistics, it has been observed that zero-day deficits that appeared once a week in 2015 occurred once a day on average in 2021 [12]. In parallel with this increase, exploit codes and malware also increase in direct proportion.

Although the financial damages of ransomware cannot be determined precisely, it is seen that the global cost of the damage is expressed in billions of dollars. For instance, according to published security reports, it is estimated that attacks with WannaCry and NotPetya ransomware cost the global economy $8 billion in 2017. Moreover, GrandCrab ransomware infected tens of thousands of systems in 2018. In recent years, ransomware has also targeted mobile systems, and this has increased the danger more. Furthermore, eventhough it is stated that the motivation for the emergence of ransomware is basically to gain financial gain, it has recently been seen that it is also used in cyber terrorism-oriented attacks in areas such as finance, infrastructure and production sectors [11].

Considering that internet connection can be delivered to the most remote areas of the world via satellites, malware infecting a system can pose a threat to systems all over the world. For this reason, it is very important to have information about malicious software, to examine its behavior and to reveal its effects [13]. It is equally important to share the information obtained from the studies on such an important subject with the stakeholders of the subject. However, it is a very difficult and time-consuming task for any security expert or software developer to analyze all primary sources one by one. Within the scope of this study, the approach of collecting and presenting the information in primary sources, which has been used successfully in the field of medicine for years and then used in the field of software engineering along with different fields, in a secondary source with an evidence-based method has been adopted. For this purpose, a systematic literature review is presented with the evidence-based software engineering approach of studies on ransomware detection.

This article can make a significant contribution to the development of effective detection and defense methods against ransomware. Ransomware poses a serious threat to cybersecurity with its advanced encryption techniques and complex attack methods. The victims targeted by ransomware attacks include critical infrastructures such as hospitals, financial institutions and government institutions, and the risks posed by these attacks endanger social security as well as major economic losses. Using the Evidence-Based Software Engineering (EBSE) approach, this study systematically analyzes current research in the field of ransomware detection and reveals the most effective detection methods in the field. The article provides a comprehensive resource for security experts and researchers, shedding light on defense mechanisms that can be developed against ransomware and new research areas. In this context, the study provides a comprehensive guide that aims not only to evaluate the effectiveness of current security technologies but also to be prepared against the future evolution of ransomware.

Other parts of the study are organized as follows. In the second part, the literature that guided the study was examined in detail. In the third chapter, the research methodology used is explained in detail. The obtained results are given in the fourth chapter in detail. In chapter five, there was a discussion of the results, and in the last chapter, the conclusions of the study were presented and future work was expressed.

Literature Review

Analysis and discovery of ransomware are areas of academic study that have received intense attention in recent years. As a result, there are many published studies.

Netto et al. [7] analyzed the techniques of ransomware coders in their models using static and dynamic analysis techniques. Their basic approach is to examine the packets coming and going from the system through trap files in the file systems with static analysis tools. In addition, it is seen that they analyze the details of the network packets meticulously with dynamic analysis tools. Their main recommendation is to flag network packets and add IP addresses to firewalls so that systems can take minimal damage from ransomware.

Kara et al. [9] analyzed the characteristic behaviors of the 3rd generation Cerber ransomware using static and dynamic analysis tools. Their purpose is to detect the source of the attacks. They examined the ransomware attack on an official institution and showed that the whois information of the IP addresses they found by analyzing the network movements could be tracked.

Akbanov et al [14] explored the use of software-defined networking (SDN) to detect and mitigate advanced ransomware threats. To prove their research, they examined the WannaCry ransomware. Based on the results obtained, they designed an SDN detection and mitigation framework and developed a solution based on the OpenFlow communication protocol.

Davies [15] focused their research on the idea that digital forensic analysis tools could be used to detect encryption keys of malicious ransomware. As a result of their research, they stated that digital forensic analysis tools can be used in the detection of encryption keys. For this purpose, they try to detect encryption keys by taking memory dump from a system that has been exposed to ransomware attack.

Kok et al [16] have proposed their methodology, which they call the Pre-Encryption Detection Algorithm (PEDA). The main purpose of their work is to detect a ransomware without performing an encryption process. It is a two-step algorithm. The first step is to compare known ransomware signatures. For this, it uses the SHA-256 (Secure Hash Algorithm) algorithm. The second phase is the use of Learning Algorithm (LA) based on the application program interface (API) of the ransomware.

Humayun et al. [17], in their study, examined the effects of ransomware on IoT devices in detail. The main purpose of their work is to prevent and mitigate the effects of ransomware on IoT systems. In a significant part of their studies, they included the features and effects of ransomware. They also provide up-to-date information for ransomware analysis and detection.

Arabo et al.'s [18], in their study, analyzed a dataset consisting of 7 different ransomware and 41 benign and 34 malicious software. Their focus is on creating a defense mechanism against ransomware that mimics the human immune system. To achieve their goal, they investigated the correlation in the nature and behavior of ransomware.

Patel et al [19], propose a defense mechanism against ransomware in their study using the honeypot technique. They use a large file for the honeypot that takes time to encrypt. They offer suggestions to prevent ransomware and ensure the security of the system, during the time it takes to encrypt the large fake file by the ransomware. They proved their suggestions by getting useful results in the virtual environment they tested.

When the studies above are examined, it is seen that many academic studies on the detection and analysis of ransomware have been carried out on different fields. The fact that so many different methodologies and field-specific studies have been conducted shows that a systematic literature review is a necessity for experts in the field. In this respect, our study fills an important gap. Moreover, our study, which was carried out with an evidence-based software engineering approach, reveals an original result with this aspect.

Methodology

It aims to enable the experts in the field of evidence-based software engineering to reach the most accurate solution in the fastest way against the problems they will encounter in their professional lives. For this, it is based on the evidence-based medicine approach, which has been successfully applied for years. According to this approach, a doctor cannot solve the problems he has faced throughout his career with the knowledge he has graduated from. For this reason, it should be ensured that it reaches successfully applied and proven methods for similar problems. This is possible by scientific publication of proven methods. However, it is not possible for an expert to examine all publications specific to the problem faced [20]. Therefore, it is necessary to effectively summarize and systematically present the literature specific to a particular field. Moreover, for such a procedure, a standardized procedure is needed in all studies. Evidence-Based Medicine (EBM) approach has been proposed to find a solution to this problem [1].

The success of the Evidence-Based Medicine approach has led experts to ask whether this method can be used in different fields. As a result of this, it has been observed that the use of this method in different fields gives successful results as in the field of Medicine [21]. Kitchenham et al. [3]stated that this approach should be adopted and used by researchers working in the field of software engineering. In their later work, they explained how to use this method for practitioners [22].

Kitchenham et al.'s [3]methods prompted us to conduct a Systematic Literature Review (SLR). As emphasized in the related study, Evidence-Based Medicine carries the point of view of a physician. Kitchenham et al [22] deal with rhe issue again from a software engineer's perspective. The main motivation is to have sufficient evidence to choose the most effective technology to be used while developing a project. Generally, those with decision-making authority make bad decisions in adopting new technologies. A technology with sufficient evidence can reduce project relevance, cost and inherent risks [23]. For example, in the years when Object Oriented Programming became widespread, there was a belief that hierarchical deep object models were useful, but studies have proven that this situation poses a great risk of error. However, developers tend to prefer mature technologies and generally accepted methods. Evidence-Based Software Engineering, on the other hand, aims to provide a decision-making mechanism in this regard [22].

As can be seen in Figure 1, Evidence-Based Software Engineering consists of six different steps [3]. The first step is answerable question defining. At this step, the research questions for which the evidence is to be found should be determined. The second step is to find the results that provide the best evidence. At this step, the search strategy should be determined to find the best results corresponding to the research questions identified. The third step is to evaluate the evidence critically. In this step, the right selection criteria should be determined and adopted. The next step is to integrate critical assessment with software engineering expertise. At this point, quality assessment rules should be determined. In the fifth step, data extraction methods should be defined for the evaluation of the process, and finally, how extracted data are synthesized for evidence-based software engineering [22]. In the continuation of this section, the application of the steps of the Evidence-Based Software Engineering approach is presented within the scope of our study.

Step 1. Defining Answerable Questions - Research Questions

It has been expressed as “A well-defined question should consist of three steps as its effect on the study area, its effect on the context of the problem to be solved, and the effect of its results”. [1]. The questions within the scope of this study were determined by adhering to these three principles. As our primary goal is to detect ransomware attacks, the following research questions have been developed.

RQ 1: What techniques are used to detect ransomware attack?

RQ 2: What techniques are used in ransomware analysis?

RQ 3: What are the datasets used to detect ransomware attacks?

RQ 4: What will be the future status of ransomware?

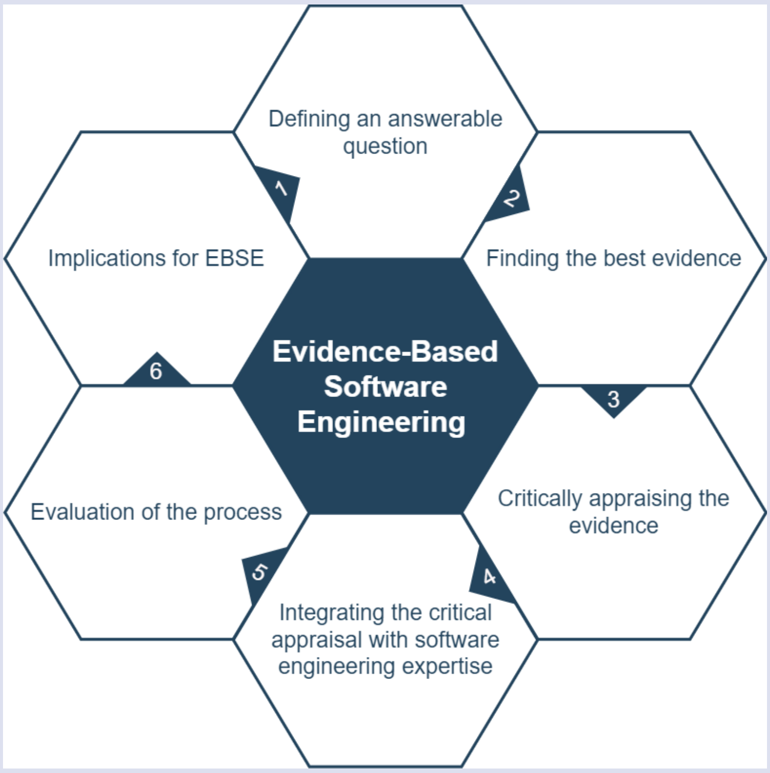
Defining an answerable question
1
2
Implications for EBSE
Finding the best evidence
Evidence-Based Software Engineering
6
3
Evaluation of the process
Critically appraising the evidence
5
4
Integrating the critical appraisal with software engineering expertise

Figure 1. Steps of Evidence-Based Software Engineering [3]

Step 2. Finding the Best Evidence - Research Strategy

The second step of evidence-based software engineering, finding the best evidence, is determining research strategies. While creating our search strategy, first of all, search terms were determined. In the second step, reliable literature sources were selected to be used to carry out the searches. Finally, it is completed with the search process. All the steps are presented in full detail below. It is recommended to [22]evaluate all possible outcomes in order to make a rational decision while determining the research terms. That's why, the search terms are pretty broad and it would be a better choice to research on the main terms. Our search terms are based on our research questions. In addition, searches were performed with Boolean (AND-OR) operations with similar search terms. The search words used in this study were determined by referring to the concept of ransomware detection. In the second step of this step, literature sources were made through databases that were generally accepted and recommended by all researchers [22]. These are; IEEE Xplore (http://ieeexplore.ieee.org), ACM Digital Library (www.acm.org/dl), ISI Web of Science (www.isinet.com/products/citation/wos), Science Direct (https: //www.sciencedirect.com/), Google Scholar (http://scholar.google.com). In addition, all libraries were scanned with the search words determined during the search process and the results were evaluated with the principles of inclusion and exclusion in the selection of the study.

Step 3. Critically Appraising the Evidence - Study Selection (Inclusion/Exclusion)

As a result of the research we conducted using our search terms from the literature sources we determined, 114 scientific studies were found in the last 5 years (2017-2002). A detailed analysis was made by the authors on the articles found at this stage of our study. The purpose of this review is to ensure that only relevant studies are included in the analysis. First of all, review and survey studies were eliminated by the authors. Identical studies from different sources were identified and extracted. To improve the quality of the study, inclusion and exclusion criteria were applied to focus on the studies that best fit our research questions before applying the quality assessment rules. Our defined inclusion and exclusion criteria were determined as whether the study offered solutions to detect ransomware or included discussion on ransomware analysis. In addition, whether or not it contains ransomware detection techniques was another criterion. Articles focusing on malware analysis and detection in a broad sense were excluded from our study. As a result, 49 articles meeting our criteria were included in the study.

Step 4. Integrating the Critical Appraisal with Software Engineering Expertise - Quality Assessment Rules (QARs)

Quality assessment rules (QAR), one of the important steps of evidence-based software engineering, were determined at this stage. For our study, ten QARs were decided by the authors. The extent to which an article meets the QAR criteria is represented by a total score ranging from 0 to 10. For each QAR, the articles were scored as 0 not meeting expectations, 0.25 below expectations, 0.5 average, 0.75 above expectations, and 1 fully meeting expectations. Articles with a total score of 5 and above in the QAR evaluation were included in the study. In order to increase the quality of the articles examined in the study, a score of 5 was chosen as the limit, as we think that it meets our expectations at a minimum level. Results of 49 articles included in the study with a quality score of 5 and above are detailed in Appendix A.

QAR1: Are the goals and boundaries of the study clearly defined?

QAR2: Is the technical background of the ransomware provided?

QAR3: Is the recommended Ransomware detection methodology clearly defined?

QAR4: Have the suggested methods been implemented and tested?

QAR5: Is the contribution of the methodology to the literature highlighted?

QAR6: Are limitations that threaten the validity of the proposed methodology specified?

QAR7: Is a detailed discussion of the findings included?

QAR8: Is there a comparison with other methods in the literature?

QAR9: Has sufficient information been given about the data set used?

QAR10: Does it have an industrial contribution in terms of results?

Step 5. Evaluation of the Process - Data extraction strategy and data synthesis

In order to find the answers to our research questions, the information extraction phase from the articles was carried out in this step. The transaction was carried out with an information form created. The titles of the information form are the title of the article, publishers, year of publication, type of publication (conference or journal article), ransomware detection technique used, and datasets. The purpose of this step of the study is to try to gather the necessary information about whether all the collected articles can contribute to the research questions.

Step 6. Implications for Evidence-Based Software Engineering

The final step of evidence-based software engineering envisages making implications from the data obtained. The answers to the research questions are tried to be determined. All the analyzes and the findings obtained for this purpose are presented in detail under the heading Results in the next section.

Results

The findings of the study are presented in this section. Additionally, this section provides an overview of the scientific articles and ransomware dedection studies selected to address the research questions outlined above. The results of each research question are analyzed in depth in the following four sections. Finally, 49 research articles were selected within the scope of the study. Intrusion detection techniques are presented in Table 1, artificial intelligence algorithms used in Table 2, ransomware analysis techniques in Table 3, and datasets used in the literature are presented in Table 4. The list of selected articles is given in Appendix A. The analyzed research articles consist of articles published between 2017 and 2022. In addition, a quality assessment rule criteria was used as stated above and the scores of the selected articles are listed in Appendix B.

What techniques are used to detect ransomware attacks?

The question of what techniques are used to detect ransomware attack, RQ1 is answered in this section. Algorithms used in the detection of ransomware attacks and suggested solution methods have been systematically determined from the reviewed articles. Ransomware attacks are long-lasting and take instructions from different connections. For this reason, it is important to detect the detection of attacks before the attack is completed, in order to reduce the damage. In our study, the most used algorithms and related studies in ransomware attack detection are listed.

As shown in Table 1, we have identified several techniques applied by researchers in the development of ransomware detection solutions. The most commonly used ransomware detection approaches in this review; Software Defined Networks (SDN), Honeypot, Pre-encryption detection algorithm (PEDA), Static Analysis, Dynamic Analysis, DNAact-Ran, Graph Based Detection methods.

According to Table 2, it was seen that the researchers used Random Forest, Naïve Bayes and MLP artificial intelligence algorithms to detect ransomware attacks. According to the articles we reviewed, the most frequently used artificial intelligence algorithm is the Random Forest algorithm.

What techniques are used in ransomware analysis?

In this section, we focus on answering AS 2 by introducing the various detection methods used to detect ransomware. Additionally, we provide details on ransomware detection techniques that can identify beaconing during ransomware attacks. We classify the data we obtain as a result of our analyzes in four categories: Machine Learning, Deep Learning, Network-Based and Signature-Based in ransomware analysis.

Machine Learning based methods; Are methods based on finding common features and correlating different malware activities using different algorithms such as SVM, Random Forest, Decision Tree, Naïve Bayes etc.

Deep learning-based techniques based on artificial neural networks such as Convolutional Neural Networks (CNN), Artificial neural network (ANN), Long short-term memory (LSTM) are used in the analysis of network traffic. The features in the network traffic are determined by using the ability to automatically extract the features in the data, which is one of the main features of deep learning algorithms. In this way, network traffic can be represented as a vector. In this way, different characteristics and patterns of network traffic can be extracted. As a result, suspicious situations and anomalies in network traffic can be detected.

Network-based techniques based on direct thinning of network traffic analyze network delays, spikes in network traffic, and unusual connections. Basically, it is trying to detect unusual situations and anomalies in the network traffic. It is intended to distinguish between benign network activities and malicious situations.

Signature-based methods are a technique based on comparing the signatures of pre-determined and identified ransomware with the signatures of the analyzed software. It is generally based on the principle that existing ransomware has been previously detected, analyzed and patterns extracted. However, it has a disadvantage in detecting an updated or new ransomware.

Table 1. Ransomware Attack Detection Techniques

Detection Technique	Reference	Frequency
SDN	[24][25][26][14][27][28][29]	7
Honey Cubes	[30][31][32]	3
PEDA	[33]	1
Static Analysis	[34][7][35][36][37][38][39]	7
Dynamic Analysis	[40][41][7][42][43][44][45][46][47][48][35][49][37][38][50][39][32]	17
DNAact-Ran	[51]	1
Graph Based Detection	[52][53]	2

Table 2. Artificial Intelligence Algorithms Used to Detect Ransomware Attacks

Artificial Intelligence Alg.	Reference	Frequency
Random Forest	[25][43] [45][54][35][48][49][53][55]	9
Naive Bayes	[43][54][28][36][50]	5
MLP	[56][49]	2

Table 3. Ransomware Detection Techniques

Sign Detection Technique	Reference	Frequency
Machine Learning based detection	[56][57][58][41][42][43][26][27][59][60][45][46][28][61][35] [51][48][18][62][49][49][36][37][63][50][64][53][39][55][32]	30
Deep Learning	[40][65][66][52][62][67][68]	7
Network Based	[24][25][14]	3
Signature Based Detection	[47]	1

Table 4. Datasets Used to Detect Ramsomware Attacks

Reference	Dataset
[58][24][14][28][47][49]	WannaCry[69]
[33] [41][60][33][62]	theZoo[70]
[57][41][34][43][57][44][60][33][35][47][49][71][36][37]	VirusTotal[72]
[50]	UNSW-NB15[73]
[51]	PSJoshi[74]
[59]	CICAndMal2017[75]
[41][42][54][48][52]	virusshare[76]

What are the datasets used to detect ransomware attacks?

In this section, we lookink for answers to AS3. For this purpose, we present a detailed analysis of the datasets and data sources used in ransomware detection methods and solutions proposed by researchers. The datasets used are listed in Table-4.

WannaCry is specifically for Microsoft Windows operating systems and therefore Windows users are at higher risk. Once infected, WannaCry encrypts files using private keys and claims that payment is the only way to access them. The fee that WannaCry requests payment is usually stated in Bitcoin and the user is threatened with permanent encryption of files if the fee is not paid [69] .

theZoo is an open-source virus and malware collection. This collection includes currently working and researched viruses and malware and provides detailed information about this software. The collection can be used as a reference resource for researchers, security professionals and other interested parties [70].

VirusTotal is a virus scanning and analysis service. To determine if a file is potentially harmful, this service sends it to many different virus scanning programs and collects the results of these programs about the file. This way, you can get a broader idea of how reliable a file is [72].

The UNSW-NB 15 dataset was created by the IXIA PerfectStorm tool at the University of New South Wales (UNSW), Canberra Cyber Range Laboratory. The network packets contain 100GB of raw data containing real modern normal activities and synthetic contemporary attack behaviors. There are nine types of attacks in this dataset, namely Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms [73].

The PSJoshi dataset contains a total of 1524 records. Of that data, it has 30970 features, of which 582 are ransomware and 942 are good software applications. It contains real world data. Therefore, it can be used to evaluate the accuracy in detecting ransomware [74].

CICAndMal2017 dataset is an Android malware dataset containing 4354 malware and 6500 benign software collected by the Canadian Cybersecurity Institute via GooglePlay in 2015, 2016, 2017. The dataset collects malicious software in four groups: Adware, Ransomware, Scareware and SMS Malware. There are 42 completely different malware families in the dataset [75].

The VirusShare dataset is a repository of malware samples available to researchers. For security reasons, an e-mail access must be requested to access the dataset. Live malware can be accessed through the dataset. All data is presented in encrypted compressed files for security reasons [76].

What will be the future status of ransomware?

We respond to AS 4 in this section to inform about the future status of ransomware attack types. Ransomware is a type of malware known as malware, and it usually restricts access to a computer's data and demands a payment from the user. It is difficult to predict what the future status of such software will be. Because with the development of technology, new technologies that threaten systems are being developed. It would not be wrong to say that the reason for the prevalence of ransomware today is the ease of hackers in obtaining financial gain and the situation of not being caught. With technology advancing, there are always possibilities for hackers to develop a more profitable and, in their own way, safe malware. However, it would not be wrong to say that ransomware will still be a big and developing threat today and in the near future [77].

To get an idea of the future of ransomware, statistics showing its near-term effects are helpful. In recent years, we have seen an increase in ransomware attacks. Many important companies and institutions were affected by these attacks. Trends show that ransomware attacks continue to increase in 2022 and will continue to be a significant threat to all industries [78]. What's more, ransomware damage is estimated to cost the global economy more than $20 billion [79].

The ransomware called WannaCry has become a global threat in 2017, affecting more than 200 thousand systems in more than 150 countries. It affected the health system in England and caused chaos. It also infiltrated railway companies and telecom networks, causing disruption of services [80]. It is known that WannaCry ransomware, which is effective in developed countries such as America, Spain, Germany and

France, has earned about 52 BTC [81]. Wannacry, NotPetya, SimpleLocker, CryptoLocker, TB-Locker and WinLock are the most well-known ransomware in the world. According to security reports , there has been a great increase in ransomware in recent years , both in number and in terms of damage to the world economy [82].

Ransomware attacks, a threat that can be used against end users without any technical knowledge, will continue to increase in the future. In addition, the insecure behaviors exhibited by end users in cyber environments and the fact that many companies do not have the manpower to take the necessary precautions and raise awareness for cyber security measures increase the gravity of the situation [78]. New emerging technologies bring with them many unexplored security vulnerabilities. This provides new opportunities for ransomware attackers. Especially IoT and 5G network technologies will be exposed to the greatest threat in the future. This situation requires security companies to pay more attention to ransomware discovery analysis [83].

Discussion

The unstoppable increase of ransomware in recent years and its consequences are obvious. The potential risks of ransomware threaten not only large systems but also end-user systems. When many end users are exposed to a ransomware attack, they usually prefer to pay the small sums required if they want to recover their data, and often do not even report this to the authorities. This shows that the financial damage of ransomware is much higher than known or estimated. The magnitude of the threat reveals the importance of studies in the field of ransomware discovery and analysis. At this point, our study is a systematic literature review based on the Evidence-Based Software Engineering framework of studies in this field. With the research, the articles published between 2017 and 2022 were examined. After parsing according to our inclusion and exclusion criteria, 160 articles remained. We continued to work with 49 articles in the scoring made according to our quality evaluation rules on these articles.

Throughout our study, we tried to find answers to four different research questions. As a result of our investigations, Software Defined Networks (SDN), Honeypot, Pre-encryption detection algorithm (PEDA), Static Analysis, Dynamic Analysis, DNAact-Ran, Graph-Based Detection methods are the most used techniques in attack detection. Among these methods, it was seen that the dynamic analysis approach was preferred the most. In addition, it is seen that Random Forest, Naive Bayes and MLP artificial intelligence algorithms are used to detect ransomware. According to the information obtained from the studies reviewed, the basic techniques used in ransomware beaconing detection are machine learning-based techniques. In recent years, it is seen that the use of Deep Learning-based techniques has increased. It is also used in Network and Signature Based techniques.

When we look at the datasets used by recent studies, [69]it is seen that datasets such as WannaCry , theZoo [70], VirusTotal [72], UNSW-NB15 [73], PSJoshi [74], CICAndMal2017 [75]and Virusshare [76] are used. It is seen that VirusTotal is the most preferred among these datasets. The analysis of the future of ransomware shows us that ransomware will still remain a major threat in the near future.

Conclusion

Today, when people and institutions carry out many transactions with the support of information systems, malicious programs such as ransomware pose a great threat in digital societies. According to the reports of security companies, the total damage caused by cyber security threats to the global economy is expressed in billions of dollars, and material losses are increasing. In addition to its financial effects, theft, disclosure or inaccessibility of personal and corporate data, which is one of the most valuable elements of today, creates irreparable results. A lot of work is being done to prevent ransomware attacks or to minimize their damage. However, it is not possible for experts in the field to follow and examine all studies. In order to find solutions to such problems, it has been suggested that primary sources should be analyzed with evidence-based studies that guarantee a certain quality and transformed into a systematic literature review. Our study, which uses this method, which is called the evidence-based software engineering approach, will fill an important gap in the field.

In this study, techniques used in existing solutions to detect ransomware attacks are analyzed and compared. In addition, various artificial intelligence algorithms used in beaconing techniques for the detection of ransomware independently from the attack were examined. A list of databases used in all analyzes has been made and explained with references.

As a result, the studies examined reveal the importance of the knowledge gained in detecting and analyzing ransomware. Determining the most effective detection methods, especially in the face of ransomware's complex structures and constantly evolving attack techniques, is one of the main contributions of the study. Reviewed studies show that machine learning and deep learning algorithms offer high success in detecting ransomware, and dynamic analysis methods play a critical role in distinguishing malware in the initial stages of attacks. Additionally, it appears that SDN-based security solutions and defensive strategies such as Honeypot have the potential to protect systems before they are attacked. This information provides an effective guide to security experts fighting ransomware threats and provides important knowledge to strengthen existing security measures and develop new defense strategies. In this context, the study not only provides a comprehensive evaluation of current detection techniques, but also contributes to the development of strategic solutions that can be applied in the future against the ransomware threat.

In our study, the use of different techniques such as machine learning and artificial neural networks for these problems is presented. In addition, challenges in the field and some areas that could inspire future work in this research area were identified. Especially recently, all researchers recommend that studies on deep learning should be carried out. In addition, studies can be expanded by examining data in different databases. In this way, the consistency of the data presented by different databases and the importance of databases other than generally accepted database providers can be revealed.

Acknowledgements

This study was produced as a part of the Master Thesis study of Engin Kuzu.

Appendix A. Selected Research Papers

Title	Medicine	Year	Ref
An Integrated Approach for Detecting Ransomware Using Static and Dynamic Analysis	Conference	2018	[7]
Ransomware detection by mining API call usage	Conference	2018	[42]
A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware	Article	2018	[27]
Ransomware detection and mitigation using software-defined networking: The case of WannaCry	Article	2019	[14]
Detecting Ransomware Using Process Behavior Analysis	Article	2020	[18]
Software-define d networking-base d crypto ransomware detection using HTTP traffic characteristics	Article	2018	[24]
R-Sentry: Deception based ransomware detection using file access patterns	Article	2022	[31]
Evaluation metric for crypto-ransomware detection using machine learning	Article	2020	[33]
Ransomware Detection using Random Forest Technique	Article	2020	[35]
A Comparative Assessment of Obfuscated Ransomware Detection Methods	Article	2019	[44]
Dynamic Ransomware Detection for Windows Platform Using Machine Learning Classifiers	Article	2022	[50]
Machine Learning-Based Detection of Ransomware Using SDN	Article	2018	[25]
A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning	Article	2020	[51]
A Comprehensive API Call Analysis for Detecting Windows-Based Ransomware	Article	2022	[39]
Analysis of Machine Learning Techniques for Ransomware Detection	Conference	2019	[59]
Attention In Recurrent Neural Networks For Ransomware Detection	Conference	2019	[65]
Evaluating Shallow and Deep Networks for Ransomware Detection and Classification	Conference	2017	[56]
Machine Learning Algorithms and Frameworks in Ransomware Detection	Article	2022	[64]
Exploiting Ransomware Paranoia For Execution Prevention	Conference	2020	[47]
A New Static-based Framework for Ransomware Detection	Conference	2018	[34]
Two -Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques	Article	2020	[48]
A novel approach for ransomware detection based on PE header using graph embedding	Article	2022	[53]
Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier	Article	2022	[68]
A framework for supporting ransomware detection and prevention based on hybrid analysis	Article	2021	[38]
Reducing False Negatives in Ransomware Detection: A Critical Evaluation of Machine Learning Algorithms	Article	2022	[55]
A Multi-Level Ransomware Detection Framework using Natural Language Processing and Machine Learning	Article	2019	[60]
Ransomware detection, prevention and protection in IoT devices using ML techniques based on dynamic analysis approach	Article	2022	[32]
Convolutional Neural Network-Based Cryptography Ransomware Detection for Low-End Embedded Processors	Article	2021	[67]
Towards resilient machine learning for ransomware detection	Article	2018	[43]
Machine Learning Based Ransomware Detection Using Storage Access Patterns Obtained From Live-forensic Hypervisor	Conference	2019	[45]
Ransomware detection using process mining and classification algorithms	Conference	2019	[54]
Deep learning LSTM based ransomware detection	Conference	2017	[40]
Feature-Selection-Based Ransomware Detection with Machine Learning of Data Analysis	Conference	2018	[26]
Android ransomware detection using reduced opcode sequence and image similarity	Conference	2017	[57]
Intrusion and ransomware detection system	Conference	2018	[30]
Large Scale Ransomware Detection by Cognitive Security	Conference	2017	[58]
Detecting Ransomware using GURLS	Article	2018	[41]
A New Method for Ransomware Detection Based on PE Header Using Convolutional Neural Networks	Conference	2020	[52]
Leveraging Deep Learning Models for Ransomware Detection in the Industrial Internet of Things Environment	Conference	2019	[66]

An experimental study to evaluate the performance of machine learning alogrithms in ransomware detection	Article	2020	[62]
Industrial Internet of Things Based Ransomware Detection using Stacked Variational Neural Network	Article	2019	[46]
Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments	Article	2019	[28]
Machine Learning Based File Entropy Analysis for Ransomware Detection in Backup Systems	Article	2019	[61]
Automated Analysis Approach for the Detection of High Survivable Ransomware	Article	2020	[49]
Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection	Article	2019	[71]
Android Ransomware Detection Based on Dynamic Obtained Features	Article	2020	[36]
LooCipher Ransomware Detection Using Lightweight Packet Characteristics	Article	2020	[29]
A Behavior based Ransomware Detection using Neural Network Models	Article	2021	[63]
A Multi-Tier Streaming Analytics Model of 0-Day Ransomware Detection Using Machine Learning	Article	2020	[37]

Appendix B. QAR Scores

Reference	Year	QAR1	QAR2	QAR3	QAR4	QAR5	QAR6	QAR7	QAR8	QAR9	QAR10	TOTAL
K. Cabaj et al. [24]	2018	one	one	0.5	one			one		one	one	6.5
M. Akbanov and others [14]	2019	one	one	0.5	one			one		one	one	6.5
S.Sheen and others[31]	2022	one	one	0.5	one		one	one		one	one	7.5
SH Coke and others[33]	2020	one	one	0.5	one	one		one		one	one	7.5
Ban Mohammed Khammas [35]	2020	one	one	0.5	one	one		one	one	one	one	8.5
F. KHAN et al.[51]	2020	one	one	0.5	one	one		one	one	one	one	8.5
AO Almashhadani and others[27]	2019	one	one	0.5	one	one		one	one	one	one	8.5
M. Medhat and others[34]	2018	one	one	0.5	one		one	one	one	one	one	8.5
F. Noorbehbahani and others[59]	2019	one	one	0.5	one			one	one	one	one	7.5
R. Agrawal et al.[65]	2019	one	one	0.5				one		one	one	6.5
Vinayakumar[56]	2022	one	one	0.5	one	one	one		one	one	one	8.5
D. Smith et al.,[64]	2022	one	one	0.5	one			one	one	one	one	7.5
F. Manavi and others[53]	2022	one	one	0.5	one	one		one	one	one	one	8.5
U. Zahoora and others [68]	2022	one	one	0.5	one			one	one	one	one	7.5
G.Cusack[25]	2018	one	one	0.5	one			one	one	one	one	7.5
M. Izham and others[50]	2022	one	one	0.5	one	one		0.5	one	one	one	8
Sergiu SECHEL [44]	2019	one	one	0.5	one			one		one	one	6.5
A. AlSabeh et al.[47]	2020	one	one		one			0.5	one	one	one	6.5
J.Hwang[48]	2020	one	one	0.5	one			0.5	0.75	one	one	6.75

DF Netto and others[7]	2018	one	one	0.75	one	0.5			0.25	one	one	6.5
S.Sheen and others[42]	2018	one	one	0.75	one	0.5		0.5	0.5	one	one	7.25
PM Anand and others[39]	2022	one	one		one		one	0.5	0.75	one	one	7.25
Francesco Mercaldo [38]	2021	one	one		one		0.5	0.5	one	one	one	6.5
R. Bold et al. [55]	2022	one	one	0.75	one	0.5			one	one	one	7.25
S. Poudyal and others[60]	2019	one	one	one	one			0.5	one	one	one	7.5
P. Sharma and others[32]	2022	one	one		one	0.5		0.5		one	one	6
H. Kim and others[67]	2021	one	one		one		one	0.5		one	one	6.5
L.Chen and others [43]	2018	one	one		one			one		one	one	6
M. Hirano et al.[45]	2019	one	one		one			one		one	one	6
A. Bahrani and others[54]	2019	one	one		one			one		one	one	6
S. Maniath et al.[40]	2018	one	one		one		0.5	one		one	one	6.5
Y.Wan et al.[26]	2018	one	one	0.5	one		0.5	0.5		one	one	6.5
A. Karimi and others[57]	2017	one	one		one		one	0.5	one	one	one	7.5
A. El-Kosairy and others[30]	2018	one	one		one		0.5	one		one	one	6.5
J. Silva et al.[58]	2018	one	one		one					one	one	5
NB Harikrishnan and others[41]	2018	one	one	0.5	one				0.5	one	one	6
F. Manavi et al.[52]	2020	one	one	0	one			0.5		one	one	5.5
M. Al-Hawawreh et al. [66]	2019	one	one		one			0.5	0.75	one	one	6.25
Y Dion and others[62]	2020	one	one		one			0.5		one	one	5.5
M AL-Hawawreh et al.[46]	2019	one	one		one				0.75	one	one	5.75
LF Maimo and others[28]	2019	one	one		one			0.5		one	one	5.5
K LEE and others[61]	2019	one	one		one					one	one	5
YA Ahmed and others[49]	2020	one	one	0.5	one				0.75	one	one	6.25
BAS Alrimy and others[71]	2020	one	one		one		0.5		0.75	one	one	6.25
Z. Abdullah and others[36]	2020	one	one		one				0.5	one	one	5.5
T. Liu and his values[29]	2020	one	one		one					one	one	5
E. Ketzaki et al.[63]	2021	one	one		one			0.5	0.5	one	one	6
H. Zuhair et al.[37]	2020	one	one		one				0.5	one	one	5.5
A. Arabo et al.[18]	2020	one	one		one				0.5	one	one	5.5

References

[1] D. L. Sackett, W. M. C. Rosenberg, J. A. M. Gray, R. B. Haynes, and W. S. Richardson, "Evidence based medicine: what it is and what it isn't. 1996.," Clinical orthopaedics and related research, vol. 455, no. 7023. British Medical Journal Publishing Group, pp. 3–5, 2007. doi: 10.1136/bmj.312.7023.71.

[2] O. A. Uysal, "Kanıta dayalı Tıp (KdT)," Tıp Fakültesi Klinikleri Dergisi, vol. 2, no. 3. Istanbul Aydin University, atk@aydin.edu.tr, pp. 83–89, 2019.

[3] B. A. Kitchenham, T. Dybå, and M. Jørgensen, "Evidence-based software engineering," in Proceedings - International Conference on Software Engineering, 2004, pp. 273–281. doi: 10.1109/icse.2004.1317449.

[4] S. Saxena and H. K. Soni, "Strategies for ransomware removal and prevention," in Proceedings of the 4th IEEE International Conference on Advances in Electrical and Electronics, Information, Communication and Bio-Informatics, AEEICB 2018, 2018, pp. 1–4. doi: 10.1109/AEEICB.2018.8480941.

[5] A. Gazet, "Comparative analysis of various ransomware virii," Journal in Computer Virology, vol. 6, no. 1, pp. 77–90, 2010, doi: 10.1007/s11416-008-0092-2.

[6] S. ÇELİK and B. ÇELİKTAŞ, "Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar," CyberPolitik Journal, vol. 3, no. 5, pp. 105–132, 2018.

[7] D. F. Netto, K. M. Shony, and E. R. Lalson, "An Integrated Approach for Detecting Ransomware Using Static and Dynamic Analysis," in 2018 International CET Conference on Control, Communication, and Computing, IC4 2018, 2018, pp. 410–414. doi: 10.1109/CETIC4.2018.8531017.

[8] T. Dumitras, "When Malware Changed Its Mind: How" Split Personalities" Affect Malware Analysis and Detection," 2023.

[9] I. Kara and M. Aydos, "Static and Dynamic Analysis of Third Generation Cerber Ransomware," in International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, IBIGDELFT 2018 - Proceedings, 2019, pp. 12–17. doi: 10.1109/IBIGDELFT.2018.8625353.

[10] J. S. Aidan, Zeenia, and U. Garg, "Advanced Petya Ransomware and Mitigation Strategies," in ICSCCC 2018 - 1st International Conference on Secure Cyber Computing and Communications, 2018, pp. 23–28. doi: 10.1109/ICSCCC .2018.8703323.

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

[12] A. Fagioli, "Zero-day recovery: the key to mitigating the ransomware threat," Computer Fraud and Security, vol. 2019, no. 1, pp. 6–9, 2019, doi: 10.1016/S1361-3723(19)30006-5.

[13] H. Ö. Baktır, B. Çelik, and S. Işık, "REMnux Linux Dağıtımının İncelenmesi ve Örnek bir Kötücül Yazılım Analiz Uygulaması. Review of REMnux Linux Distro and a Sample Malware Analysis - PDF Free Download".

[14] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "Ransomware detection and mitigation using software-defined networking: The case of WannaCry," Computers and Electrical Engineering, vol. 76, pp. 111–121, 2019, doi: 10.1016/j.compeleceng.2019.03.012.

[15] S. R. Davies, R. Macfarlane, and W. J. Buchanan, "Evaluation of live forensic techniques in ransomware attack mitigation," Forensic Science International: Digital Investigation, vol. 33, p. 300979, 2020, doi: 10.1016/j.fsidi.2020.300979.

[16] S. H. Kok, A. Abdullah, and N. Z. Jhanjhi, "Early detection of crypto-ransomware using pre-encryption detection algorithm," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 5, pp. 1984–1999, 2022, doi: 10.1016/j.jksuci.2020.06.012.

[17] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention," Egyptian Informatics Journal, vol. 22, no. 1, pp. 105–117, Mar. 2021, doi: 10.1016/J.EIJ.2020.05.003.

[18] A. Arabo, R. Dijoux, T. Poulain, and G. Chevalier, "Detecting ransomware using process behavior analysis," Procedia Comput Sci, vol. 168, pp. 289–296, 2020, doi: 10.1016/j.procs.2020.02.249.

[19] A. Patel and J. Tailor, "A malicious activity monitoring mechanism to detect and prevent ransomware," Computer Fraud and Security, vol. 2020, no. 1, pp. 14–19, 2020, doi: 10.1016/S1361-3723(20)30009-9.

[20] D. Berry, W. T.-I. T. on Software, and undefined 2003, "Comments on" Formal methods application: an empirical tale of software development"," ieeexplore.ieee.org.

[21] M. Jorgensen, ... T. D.-11th I. I., and undefined 2005, "Teaching evidence-based software engineering to university students," ieeexplore.ieee.org.

[22] T. Dybå, B. A. Kitchenham, and M. Jorgensen, "Evidence-based software engineering for practitioners," IEEE Softw, vol. 22, no. 1, pp. 58–65, Jan. 2005, doi: 10.1109/MS.2005.6.

[23] M. V Zelkowitz, D. Binkley, D. R. Wallace, and D. W. Binkley, "Experimental validation of new software technology," World Scientific, pp. 229–263, Mar. 2003, doi: 10.1142/9789812795588_0006.

[24] K. Cabaj, M. Gregorczyk, and W. Mazurczyk, "Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics," Computers and Electrical Engineering, vol. 66, pp. 353–368, 2018, doi: 10.1016/j.compeleceng.2017.10.012.

[25] G. Cusack, O. Michel, and E. Keller, "Machine learning-based detection of ransomware using SDN," in SDN-NFVSec 2018 - Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization, Co-located with CODASPY 2018, 2018, pp. 1–6. doi: 10.1145/3180465.3180467.

[26] Y. L. Wan, J. C. Chang, R. J. Chen, and S. J. Wang, "Feature-Selection-Based Ransomware Detection with Machine Learning of Data Analysis," 2018 3rd International Conference on Computer and Communication Systems, ICCCS 2018, pp. 392–396, 2018, doi: 10.1109/CCOMS.2018. 8463300.

[27] 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.

[28] L. F. Maimó, A. H. Celdrán, Á. L. Perales Gómez, F. J. García Clemente, J. Weimer, and I. Lee, "Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments," Sensors (Switzerland), vol. 19, no. 5, 2019, doi: 10.3390/s19051114.

[29] T. M. Liu, D. Y. Kao, and Y. Y. Chen, "Loocipher ransomware detection using lightweight packet characteristics," Procedia Comput Sci, vol. 176, pp. 1677–1683, 2020, doi: 10.1016/j.procs.2020.09.192.

[30] A. El-Kosairy and M. A. Azer, "Intrusion and ransomware detection system," ieeexplore.ieee.org, pp. 1–7, 2018, doi: 10.1109/cais.2018.8471688.

[31] S. Sheen, K. A. Asmitha, and S. Venkatesan, "R-Sentry: Deception based ransomware detection using file access patterns," Computers and Electrical Engineering, vol. 103, p. 108346, 2022, doi: 10.1016/j.compeleceng.2022.108346.

[32] P. Sharma, S. Kapoor, and R. Sharma, "Ransomware detection, prevention and protection in IoT devices using ML techniques based on dynamic analysis approach," International Journal of System Assurance Engineering and Management, 2022, doi: 10.1007/s13198-022-01793-0.

[33] S. H. Kok, A. Azween, and N. Z. Jhanjhi, "Evaluation metric for crypto-ransomware detection using machine learning," Journal of Information Security and Applications, vol. 55, p. 102646, 2020, doi: 10.1016/j.jisa.2020.102646.

[34] M. Medhat, S. Gaber, and N. Abdelbaki, "A new static-based framework for ransomware detection," in Proceedings - IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, IEEE 16th International Conference on Pervasive Intelligence and Computing, IEEE 4th International Conference on Big Data Intelligence and Computing and IEEE 3, 2018, pp. 710–715. doi: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018. 00124.

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

[36] Z. Abdullah, F. W. Muhadi, M. M. Saudi, I. R. A. Hamid, and C. F. M. Foozy, "Android Ransomware Detection Based on Dynamic Obtained Features," Advances in Intelligent Systems and Computing, vol. 978 AISC, pp. 121–129, 2020, doi: 10.1007/978-3-030-36056-6_12.

[37] H. Zuhair, A. Selamat, and O. Krejcar, "A multi-tier streaming analytics model of 0-day ransomware detection using machine learning," Applied Sciences (Switzerland), vol. 10, no. 9, 2020, doi: 10.3390/app10093210.

[38] F. Mercaldo, "A framework for supporting ransomware detection and prevention based on hybrid analysis," Journal of Computer Virology and Hacking Techniques, vol. 17, no. 3, pp. 221–227, Sep. 2021, doi: 10.1007/S11416-021-00388-W.

[39] P. Mohan Anand, P. V. Sai Charan, and S. K. Shukla, "A Comprehensive API Call Analysis for Detecting Windows-Based Ransomware," in Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience, CSR 2022, 2022, pp. 337–344. doi: 10.1109/CSR54599. 2022.9850320.

[40] S. Maniath, A. Ashok, P. Poornachandran, V. G. Sujadevi, A. U. P. Sankar, and S. Jan, "Deep learning LSTM based ransomware detection," 2017 Recent Developments in Control, Automation and Power Engineering, RDCAPE 2017, pp. 442–446, 2018, doi: 10.1109/RDCAPE.2017.8358312.

[41] N. Harikrishnan and K. Soman, "Detecting Ransomware using GURLS," Proceedings of 2018 2nd International Conference on Advances in Electronics, Computers and Communications, ICAECC 2018, 2018, doi: 10.1109/ ICAECC.2018.8479444.

[42] S. Sheen and A. Yadav, "Ransomware detection by mining API call usage," in 2018 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2018, 2018, pp. 983–987. doi: 10.1109/ICACCI. 2018.8554938.

[43] L. Chen, C.-Y. Yang, A. Paul, and R. Sahita, "Towards resilient machine learning for ransomware detection," Dec. 2018.

[44] S. SECHEL, "A Comparative Assessment of Obfuscated Ransomware Detection Methods," Informatica Economica, vol. 23, no. 2/2019, pp. 45–62, 2019, doi: 10.12948/issn14531305/23.2.2019.05.

[45] M. Hirano and R. Kobayashi, "Machine Learning Based Ransomware Detection Using Storage Access Patterns Obtained from Live-forensic Hypervisor," 2019 6th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2019, 2019, doi: 10.1109/IOTSMS48152.2019.8939214.

[46] M. AL-Hawawreh and E. Sitnikova, "Industrial internet of things based ransomware detection using stacked variational neural network," ACM International Conference Proceeding Series, pp. 126–130, Aug. 2019, doi: 10.1145/3361758.3361763.

[47] A. Alsabeh, H. Safa, E. Bou-Harb, and J. Crichigno, "Exploiting Ransomware Paranoia for Execution Prevention," in IEEE International Conference on Communications, 2020, pp. 1–6. doi: 10.1109/ICC40277.2020.9149005.

[48] J. Hwang, J. Kim, S. Lee, and K. Kim, "Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques," Wirel Pers Commun, vol. 112, no. 4, pp. 2597–2609, 2020, doi: 10.1007/s11277-020-07166-9.

[49] Y. A. Ahmed, B. Koçer, and B. A. S. Al-Rimy, "Automated Analysis Approach for the Detection of High Survivable Ransomware," KSII Transactions on Internet and Information Systems, vol. 14, no. 5, pp. 2236–2257, 2020, doi: 10.3837/tiis.2020.05.021.

[50] M. Izham Jaya and M. F. A. Razak, "Dynamic Ransomware Detection for Windows Platform Using Machine Learning Classifiers," International Journal on Informatics Visualization, vol. 6, no. 2, pp. 469–474, 2022, doi: 10.30630/joiv.6.2-2.1093.

[51] F. Khan, C. Ncube, L. K. Ramasamy, S. Kadry, and Y. Nam, "A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning," IEEE Access, vol. 8, pp. 119710–119719, 2020, doi: 10.1109/ACCESS.2020.3003785.

[52] F. Manavi and A. Hamzeh, "A New Method for Ransomware Detection Based on PE Header Using Convolutional Neural Networks," Proceedings of 17th International ISC Conference on Information Security and Cryptology, ISCISC 2020, pp. 82–87, 2020, doi: 10.1109/ISCISC51277.2020. 9261903.

[53] F. Manavi and A. Hamzeh, "A novel approach for ransomware detection based on PE header using graph embedding," Journal of Computer Virology and Hacking Techniques, vol. 18, no. 4, pp. 285–296, 2022, doi: 10.1007/s11416-021-00414-x.

[54] A. Bahrani and A. J. Bidgly, "Ransomware detection using process mining and classification algorithms," Proceedings of 16th International ISC Conference on Information Security and Cryptology, ISCISC 2019, pp. 73–77, 2019, doi: 10.1109/ISCISC48546.2019.8985149.

[55] R. Bold, H. Al-Khateeb, and N. Ersotelos, "Reducing False Negatives in Ransomware Detection: A Critical Evaluation of Machine Learning Algorithms," Applied Sciences (Switzerland), vol. 12, no. 24, 2022, doi: 10.3390/app12241 2941.

[56] R. Vinayakumar, K. P. Soman, K. K. S. Velan, and S. Ganorkar, "Evaluating shallow and deep networks for ransomware detection and classification," in 2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017, 2017, pp. 259–265. doi: 10.1109/ICACCI.2017.8125850.

[57] A. Karimi and M. H. Moattar, "Android ransomware detection using reduced opcode sequence and image similarity," 2017 7th International Conference on Computer and Knowledge Engineering, ICCKE 2017, vol. 2017-Janua, pp. 229–234, 2017, doi: 10.1109/ICCKE.2017.8167881.

[58] J. A. H. Silva and M. Hernandez-Alvarez, "Large scale ransomware detection by cognitive security," 2017 IEEE 2nd Ecuador Technical Chapters Meeting, ETCM 2017, vol. 2017-Janua, pp. 1–4, 2018, doi: 10.1109/ETCM.2017.8247484.

[59] F. Noorbehbahani, F. Rasouli, and M. Saberi, "Analysis of machine learning techniques for ransomware detection," Proceedings of 16th International ISC Conference on Information Security and Cryptology, ISCISC 2019, pp. 128–133, Aug. 2019, doi: 10.1109/ISCISC48546.2019.8985139.

[60] S. Poudyal, D. Dasgupta, Z. Akhtar, and K. Gupta, "A multi-level ransomware detection framework using natural language processing and machine learning," in 14th International Conference on Malicious and Unwanted Software" MALCON, 2019.

[61] K. Lee, S. Y. Lee, and K. Yim, "Machine Learning Based File Entropy Analysis for Ransomware Detection in Backup Systems," IEEE Access, vol. 7, pp. 110205–110215, 2019, doi: 10.1109/ACCESS.2019.2931136.

[62] Y. L. Dion and S. N. Brohi, "An experimental study to evaluate the performance of machine learning algorithms in ransomware detection," Journal of Engineering Science and Technology, vol. 15, no. 2, pp. 967–981, 2020.

[63] E. Ketzaki, P. Toupas, K. M. Giannoutakis, A. Drosou, and D. Tzovaras, "A Behaviour based Ransomware Detection using Neural Network Models," 2020 10th International Conference on Advanced Computer Information Technologies, ACIT 2020 - Proceedings, pp. 747–750, 2020, doi: 10.1109/ACIT49673.2020.9208974.

[64] D. Smith, S. Khorsandroo, and K. Roy, "Machine Learning Algorithms and Frameworks in Ransomware Detection," IEEE Access, vol. 10, pp. 117597–117610, 2022, doi: 10.1109/ACCESS.2022.3218779.

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

[66] M. Al-Hawawreh and E. Sitnikova, "Leveraging Deep Learning Models for Ransomware Detection in the Industrial Internet of Things Environment," 2019 Military Communications and Information Systems Conference, MilCIS 2019 - Proceedings, 2019, doi: 10.1109/ MilCIS.2019.8930732.

[67] H. Kim, J. Park, H. Kwon, K. Jang, and H. Seo, "Convolutional neural network-based cryptography ransomware detection for low-end embedded processors," Mathematics, vol. 9, no. 7, Apr. 2021, doi: 10.3390/math9070705.

[68] U. Zahoora, A. Khan, M. Rajarajan, S. H. Khan, M. Asam, and T. Jamal, "Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier," Sci Rep, vol. 12, no. 1, p. 15647, 2022, doi: 10.1038/s41598-022-19443-7.

[69] "WannaCry Fidye Yazılımı Hakkında Bilmeniz Gereken Her Şey." Accessed: Apr. 14, 2023. [Online]. Available: https://www. kaspersky.com.tr/resource-center/threats/ ransomware-wannacry

[70] "GitHub - ytisf/theZoo: A repository of LIVE malwares for your own joy and pleasure. theZoo is a project created to make the possibility of malware analysis open and available to the public." Accessed: Apr. 14, 2023. [Online]. Available: https://github.com/ytisf/theZoo

[71] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection," Future Generation Computer Systems, vol. 101, pp. 476–491, Dec. 2019, doi: 10.1016/j.future.2019.06.005.

[72] "VirusTotal - Home." Accessed: Apr. 14, 2023. [Online]. Available: https://www.virustotal.com/gui/home/upload

[73] "The TON_IoT Datasets | UNSW Research." Accessed: Apr. 14, 2023. [Online]. Available: https://research.unsw.edu.au/ projects/toniot-datasets

[74] "PSJoshi (Pradyumna Joshi) · GitHub." Accessed: Apr. 14, 2023. [Online]. Available: https://github.com/PSJoshi

[75] "Android Malware 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB." Accessed: Apr. 14, 2023. [Online]. Available: https://www.unb.ca/cic/datasets/ andmal2017.html

[76] "VirüsShare.com." Accessed: Apr. 14, 2023. [Online]. Available: https://virusshare.com/

[77] "2022 Data Breach Investigations Report | Verizon." Accessed: Apr. 19, 2023. [Online]. Available: https://www.verizon.com/business /resources/reports/dbir/

[78] "Ransomware is here to stay and other cybersecurity predictions for 2022." Accessed: Mar. 10, 2023. [Online]. Available: https://quointelligence.eu/2022/01/ransomware -and-other-cybersecurity-predictions-for-2022/

[79] P. Sharma, S. Kapoor, and R. Sharma, "Ransomware detection, prevention and protection in IoT devices using ML techniques based on dynamic analysis approach," International Journal of System Assurance Engineering and Management, vol. 14, no. 1, pp. 287–296, 2023, doi: 10.1007/s13198-022-01793-0.

[80] "WannaCry Ransomware Attack (What Happened & How to Protect Yourself)." Accessed: Apr. 17, 2023. [Online]. Available: https://www.webopedia.com/definitions/wannacry /

[81] "The Biggest Cybersecurity Disasters of 2017 So Far | WIRED." Accessed: Apr. 17, 2023. [Online]. Available: https://www.wired. com/story/2017-biggest-hacks-so-far/

[82] "Symantec Internet Security Threat Report." Accessed: Apr. 17, 2023. [Online]. Available: https://www.crn.com /tag/Symantec% 20Internet%20Security%20Threat%20Report

[83] "Defending Against Ransomware | Deloitte US." Accessed: Mar. 14, 2023. [Online]. Available: https://www2.deloitte. com/us/en/pages /risk /articles/defending-against-ransomware.html