A Systematic Literature Review of Ransomware Detection Methods and Tools for Mitigating Potential Attacks

Mujeeb ur Rehman[1](✉), Rehan Akbar[1], Mazni Omar[2], and Abdul Rehman Gilal[3]

[1] Computer and Information Sciences Department, Universiti Teknologi PETRONAS, Seri Iskandar, Malaysia
mujeeb_22007910@utp.edu.my
[2] School of Computing, Universiti Utara Malaysia, 06010 Sintok, Malaysia
[3] School of Computing, University of Portsmouth, Portsmouth, UK

Abstract. In today's world, cybersecurity is critical in the field of information technology. With the rise of cyber-attacks, including ransomware attacks, protecting user data has become a top priority. Despite the various strategies employed by governments and companies to counteract cybercrime, ransomware continues to be a major concern. Therefore, there is a need to detect and obfuscate viruses in a better way. This immutable impact on the target is what recognizes ransomware attacks from traditional malware. Ransomware attacks are expected to become more problematic in the future. Attackers might use new encryption methods or obfuscation techniques to make ransomware detection and analysis a difficult job. To protect against such attacks, organizations and users employ various tools, guidelines, security guards, and best practices. However, despite these efforts, cyber-attacks have increased exponentially in recent years. Among the most devastating of these attacks is ransomware, which can encrypt user files or lock their devices' interfaces, rendering them unusable. This research paper provides a valuable resource for researchers, practitioners, and policymakers seeking to enhance their understanding of ransomware detection and mitigation. It also examines defense tactics, such as system backups and network breakdowns, which can help mitigate the impact of an attack. Finally, the paper considers upcoming challenges in the field of cybersecurity and the importance of staying vigilant in protecting against cyber threats.

Keywords: Cyberattack · Cybersecurity · Ransomware detection · Ransomware mitigation

1 Introduction

The Internet is currently the fastest-growing infrastructure, and modern technologies are transforming human activities. However, the widespread use of technology has resulted in increased cybercrime and the vulnerability of personal information [1]. The term "ransomware" originated from the word "ransom" and "malware," and it has become a

N. H. Zakaria et al. (Eds.): ICOCI 2023, CCIS 2001, pp. 80–95, 2024.
https://doi.org/10.1007/978-981-99-9589-9_7

significant contributor to the surge in cyberattacks as it can generate profits for attackers. In the past, hackers had difficulties profiting from their attacks, but this is no longer the case. Cybercriminals are increasingly using ransomware attacks where they gain access to a victim's data, encrypt it, and demand payment [2].

Ransomware is a type of virus that can prevent users from accessing their computer system. It frequently spreads through malicious websites that take advantage of flaws in hardware and software. Some of the most common ransomware viruses include CryptoLocker, Petya, Bad Rabbit, Ryuk and Maze [3]. These viruses primarily target document storage files, such as MS office, PDF, and CSV files, and use strong encryption to make them virtually inaccessible without a specific decryption key. Once infected, the attacker demands payment from the victim and provides instructions on how to retrieve the encrypted files. If the ransom is paid, the attacker will post a message on the computer screen with information on how to retrieve the files, thus ending the attack. This technique is known as cryptovirology [4].

Ransomware, which can appear as Crypto or Locker variations, is a highly hazardous and complex form of malware. Targeting and seizing control of crucial infrastructure and computer systems is its main goal. These assaults are generally carried out for financial gain, either directly by requesting ransom payments in exchange for decryption keys or indirectly. Researchers have thoroughly examined scholarly literature on the inner workings of ransomware, including its particular assault patterns and tactics, in the hunt for viable solutions [5, 6]. These effects can include data loss as a consequence of file encryption, significant costs for incident response and other security-related issues, and, in the worst cases, even fatalities as a result of unanticipated failures of vital medical equipment [7, 8].

Prior systematic reviews in academic literature have mostly focused on the effects of ransomware within specialized industries, such as healthcare, while ignoring the larger fact that ransomware assaults are prevalent across multiple areas. This study aims to fill this specific vacuum by providing a thorough analysis of the complete ransomware attack lifecycle and an understanding of its unique characteristics. This thorough study is meant to act as a basis for future research projects in this area. The report also explores current approaches for the detection and prevention of ransomware, offering a comprehensive evaluation of their relative benefits and drawbacks. Additionally, the article provides details on a variety of preventive techniques that may be used to reduce the risk associated with malicious activities.

1.1 Prior Research

Computer networks may be vulnerable to attacks that compromise the system or its users by taking advantage of connection or network flaws. These assaults may be roughly divided into two categories: active and passive, with each using a variety of strategies and ways to illegally obtain data, identities, or financial assets. While passive attacks only observe or eavesdrop on network activity without doing any harm, active attacks are intentional attempts to manipulate or harm the network [9].

Joseph L. Popp is known as the "father of ransomware" for creating the first ransomware virus in 1989. This set the stage for modern ransomware threats, which can

be spread through infected USB drives or phishing emails containing malicious attachments or links. Ransomware has become a serious threat, often encrypting user data and demanding payment through difficult-to-trace bitcoin. Figure 1 provides a visual representation of ransomware.

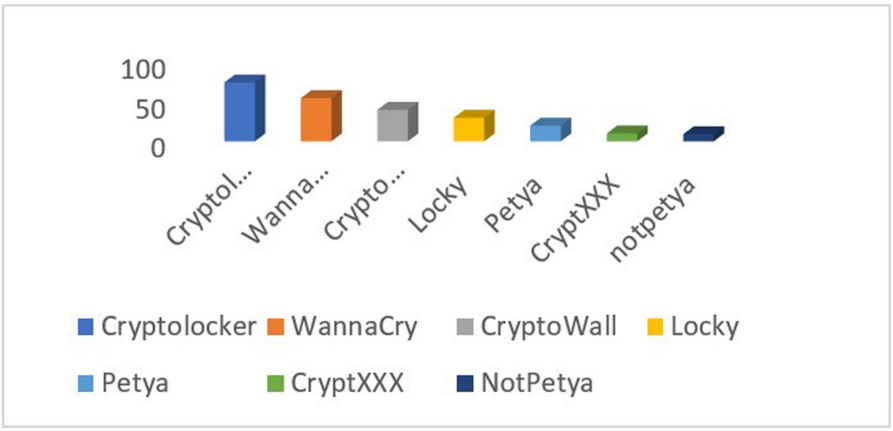

Fig. 1. List of Ransomware Attack [9]

1.2 Types of Ransomware Attacks

1) Crypto-Ransomware- Encrypts files on the victim's computer and demands a ransom for decryption. WannaCry, WannaCry, Petya, CryptoLocker [10].
2) Locker-Ransomware Locks the victim out of their system entirely, preventing access to any files or applications. Win locker, Police Trojan, FBI Virus [11].
3) Scareware Ransomware- Displays false warning messages to trick the victim into paying the ransom. Fake antiviruses, Tech support frauds.
4) RaaS (Ransomware-as-a-Service)- A business model where cybercriminals sell ransomware to other attackers for a share of the profits. Satan, Shark, Philadelphia.
5) Mobile Ransomware- target mobile devices, locking the user out or encrypting data on the device. Simplocker Android/Filecoder.C.

However, the role of operating systems in ransomware attacks cannot be overlooked. Observations have shown that devices utilizing the Windows operating system tend to be more susceptible to these attacks and are frequently singled out as targets [12]. Nevertheless, it's essential to recognize that other operating systems, such as iOS and MacOS, are not exempt from vulnerability. This underscores the fact that the threat of ransomware is pervasive and no operating system is impervious to it [13]. Figure 2 demonstrated in various instances.

Ransomware is a form of cyber-attack that involves the use of encryption to block access to a victim's data, and a demand for payment in exchange for the decryption key [14]. According to research conducted in the field, ransomware can be traced back to the

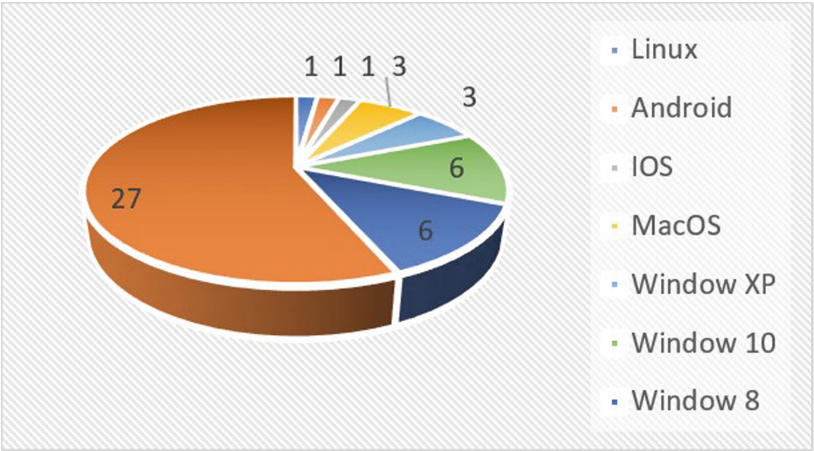

Fig. 2. Operating system effected by ransomware.

early 1990s, when cryptography was first used for exploitation purposes. However, at that time, it was not possible to demand money from victims because it was easy to trace the recipient. It was only with the introduction of cryptocurrency that the idea of using ransomware as a means of making money became viable. Therefore, the emergence of cryptocurrency can be linked to the rise of ransomware attacks.

Furthermore, a critical analysis of the impact of ransomware attacks on organizations in different countries was conducted. The analysis revealed that in 2021, approximately 50% of organizations in several countries were affected by ransomware attacks. The figure below depicts the countries where the highest number of organizations were negatively impacted by ransomware attacks (Fig. 3).

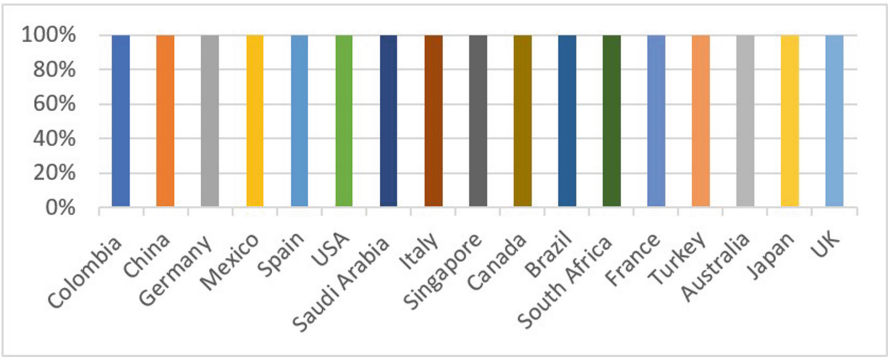

Fig. 3. Ransomware attack success rates in the past 12 months vary by country.

1.3 Major Problem

Previous systematic reviews of ransomware have mainly focused on its impact in specialized industries such as healthcare, and government organizations neglecting the fact that ransomware is not limited to specific domains. To address this limitation, this paper proposes a comprehensive evaluation of the detecting and mitigating of ransomware, serving as a starting point for further research. Furthermore, the paper discusses existing methods for detecting ransomware, analyzing their pros and cons. Lastly, prevention tools for ransomware attacks are discussed, providing valuable insights for organizations looking to enhance their security measures against ransomware threats.

1.4 Study Objectives

The aim of this study is to examine prior research, consolidate its findings, and concentrate on analyzing ransomware attacks, risks, mitigation, and prevention methods to control ransomware attacks. The study also aims to provide recommendations for the use of these techniques and tools, as well as identify areas for future research in this field. Ultimately, the objective would be to contribute to the development of more effective strategies for mitigating the impact of ransomware attacks. To achieve this goal, three research questions have been formulated, as shown in Table 1.

Table 1. Formulated Questions and discussion

Research Question	Discussion
What are the current state-of-the-art techniques and tools used for detecting ransomware?	The aim is to explain ransomware detection approaches without excessive technical detail. However, these techniques are not foolproof as attackers constantly develop new methods to evade detection [15, 16]
How effective are existing mitigation strategies in preventing ransomware attacks and their associated damages?	Ransomware prevention strategies (backup, antivirus, intrusion detection, and employee training) have limitations (zero-day attacks, updates) and effectiveness depends on an organization's security posture and threat landscape
What are the most common tactics and techniques used by ransomware attackers and how can these be thwarted?	To prevent ransomware attacks, use a multi-layered approach with technological and behavioral solutions, including multifactor authentication, regular backups, and system updates, as attackers use various tactics [15]

1.5 Contribution and Structure

This systematic literature review provides a valuable resource for individuals seeking to advance their knowledge in ransomware attacks and cyber security. By synthesizing previous research, it builds upon existing knowledge and makes new research, as discussed in Table 1.

- Our review identified 31 papers that are relevant to the topics of cyber security and ransomware threats and detection. This set of studies can serve as a resource for other researchers who seek to further investigate these areas.
- Organize and classify different methods of ransomware attacks into a specific taxonomy.
- We investigated the conditions utilized for evaluating defense, detection, mitigation, and prevention techniques against ransomware attacks.
- We identified available research data for a future analysis of ransomware and provided guidelines to assist in further research in this field.

The structure of this paper unfolds as follows: Sect. 2 explains the methodology employed to systematically select primary studies for our comprehensive analysis. In Sect. 3, we present the outcomes derived from our scrutiny of the selected primary research studies. Finally, Sect. 4 serves as the result of our research efforts, offering conclusions drawn from our findings and suggesting recommendations for future investigations.

2 Methodology

The research methodology section of this paper describes the systematic approach taken to look at previous studies about prospective ransomware attacks and their corresponding detection systems. Article offer details on the inclusion and exclusion criteria used to choose relevant research, also describe how we locate articles, papers, books, and journals about ransomware attacks.

2.1 Source Material

The study utilized a specific search engine and focused on entering relevant keywords to ensure the retrieval of primary research that would address the research questions. The selected keywords were carefully chosen to optimize the development of relevant findings. Boolean operators were limited to AND and OR. The search terms used were: (insert the specific keywords used).

(“ransom” OR “ransom-ware” OR “ransomware” OR “Mal-ware” OR “Malware” OR “ransomware attacks”) AND “information security” (“ransomware” OR “ransom” OR “Malware AND (“security” OR “cybersecurity” OR “cyber-security”).

In the first phase, the task to be performed for the quality of research is to undertake an exhaustive literature search. Therefore, a search was conducted using six different electronic libraries namely IEEE Xplore, Science Direct, ACM, Springer, Web of Science, and Google Scholar to search for the relevant materials.

The search process for relevant studies involved using titles, keywords, and abstract depending on the platform used. All studies published up to a certain point were included and filtered based on the selection/eligibility criteria provided in Sect. 2.2. The search process was conducted iteratively, both forward and backward, until no further publications that met the selection criteria could be found.

According to [3, 17], ransomware refers to a type of malicious software that encrypts data and demands payment in exchange for its release. This literature review includes both published and ongoing research studies related to ransomware attacks. The review methodology involves a four-step process, which is illustrated in Fig. 4. The process includes library searches and various steps to identify and select relevant articles for analysis.

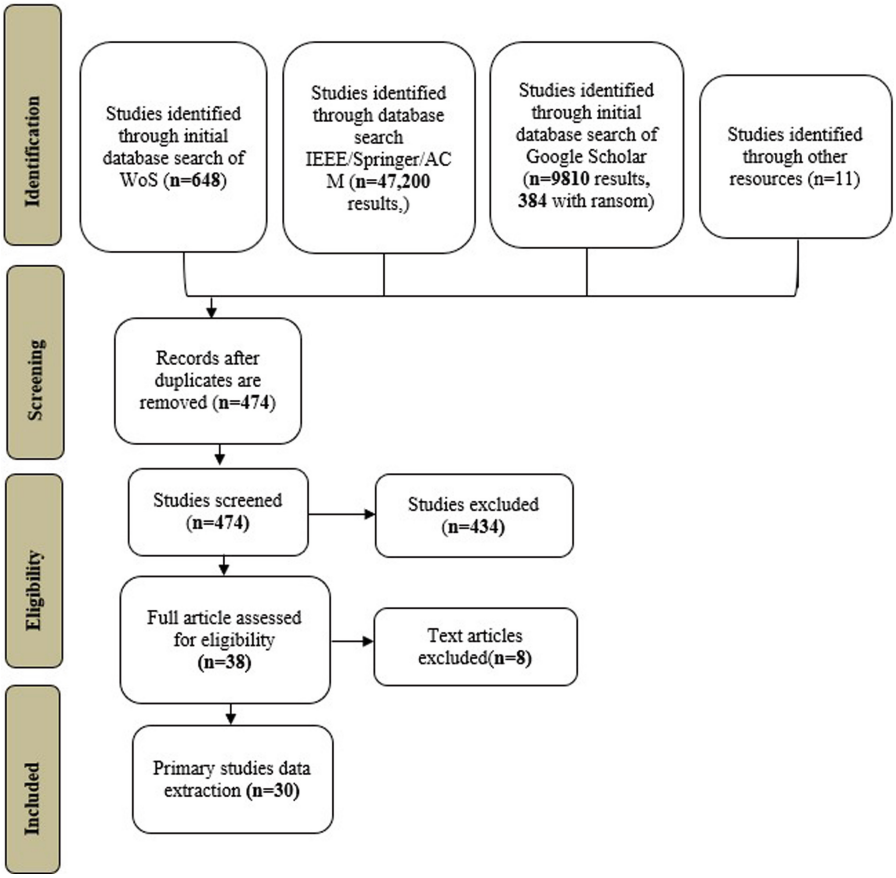

Fig. 4. Scoping Literature review process

To conduct the literature search, various search options were used in different databases. In IEEE, the search option "anywhere" was selected, while in Google Scholar,

the "anywhere in the article" option was used. For Web of Science, the search was limited to the "subject" parameter. The search included a variety of publication types, such as journal articles, book sections, working papers, conference papers, dissertations, and reports.

Advanced search filters were used to refine search results, including past 13 years, document types, and English language. New keywords like "cyber risk" and "challenges and analysis" were added. A slimming approach was used to analyze articles, removing duplicates, and considering only English-language textual sources. 30 journal articles were selected for the literature study, as shown in Fig. 4.

2.2 Inclusion and Exclusion Criteria

A systematic literature review requires empirical evidence from case studies, new ransomware attacks, and advancements in ransomware mitigation technologies. English-written, peer-reviewed studies must meet standards, and only updated ones within recent years are considered. Google Scholar results may not meet standards, so all results are evaluated for compliance (Table 2).

Table 2. Inclusion and exclusion criteria for primary studies

Inclusion Criteria	Exclusion Criteria
The article offers insights and practical advice to protect against ransomware attacks and other cyber threats	The article should discuss papers that investigate the impact of ransomware attacks on businesses or the legal system
The document should provide an in-depth examination of ransomware or any other relevant technological advancement in your writing	Governmental documents and blogs should not be included in the article
The article must be a peer-reviewed paper published in a journal or conference proceedings	non-English publications

2.3 Selection Results

A total of 648 studies were searched, but duplicates were removed, leading to 474. After evaluating, 38 publications were identified. The criteria were applied again, reducing the number to 30 papers.

2.4 Quality Assessment

The primary studies were assessed for quality in accordance with the guidelines. The evaluation aimed to determine the relevance of the papers to the research questions while considering any possible research bias and the reliability of the experimental findings.

The evaluation process was modeled after similar literature reviews. To evaluate the effectiveness of randomly selected papers, a specific quality assessment procedure was implemented.

Step 1: Ransomware: The article should discuss multiple forms of ransomware attacks or security breaches and offer insightful commentary on a specific issue.
Step 2: Perspective: The research's objectives and conclusions should be properly contextualized to ensure a comprehensive understanding of the study.
Step 3: Ransomware detection Strategy: Study must provide enough information to show how technology is used to detect attacks and answer research questions, including specific tools and techniques used for detection and mitigation.
Step 4: Defense context: The document should explain the security issue to help answer research questions, including its nature, potential consequences, and challenges in addressing it.
Step 5: Security measures: The application of diverse security measures to alleviate several types of ransomware attacks.
Step 6: Data Recovery: Specifics on data collection, measurement, and reporting must be provided to assess accuracy.

2.5 Data Extraction

The data completeness and accuracy of articles were assessed by extracting data from quality-approved papers. The technique was tested on a preliminary investigation before being applied to the full set of research. Data was categorized and entered into a spreadsheet using the following categories.

Context Data: Information involving the study's performed objectives.

Qualitative Data: The author's findings and opinions.

Quantitative Data: Information collected through tests and research has been used in the study.

2.6 Meaningful Keywords Count

A keyword analysis was conducted on all 38 studies to identify the common themes among the selected primary research. The frequency of various words used across all studies was compiled and presented in Table 3. As observed in the table, "Machine Learning" is the third most frequent term in the dataset, following "ransomware" and "Trojan," and preceded only by the author's chosen keywords "ransomware" and "security".

Table 3. Keywords count from primary studies.

Keywords	Count
Ransomware	2451
Trojan	1752
Security	1664
Machine learning	1356
Information	853
Cybersecurity	334
Deep learning	675
Software	1320
Privacy	598
Attacks	486
Malware	475

3 Findings

Table 4 summarizes relevant qualitative and quantitative data extracted from the main research papers. Each primary study had a specific objective or theme related to previous research on ransomware attacks, which is also indicated in the table.

Table 4. Finding of the primary studies

PS	Key Qualitative	Type of research
[26]	The article covers the methodology and threats of Petya ransomware, as well as strategies for awareness and mitigation	effects
[27]	Healthcare companies can improve system defense through user-focused tactics like simulation and training on proper computer and network application usage [19]	Mitigation
[25]	The paper covers the impact of ransomware attacks on cloud service users and providers and proposes mitigating tactics.[28]	
[29]	To provide the decryption key for encrypted user data, hackers often demand a ransom or payment, typically in the form of digital currencies	
[19]	The paper stresses the importance of a written information security program mandated by Massachusetts law or other security frameworks	security
[30]	Memory forensics was conducted on volatile memory dumps of virtual machines using the Volatility framework for analysis	Detection
[9]	The report introduces Net Converse, a machine learning study for detecting ransomware network traffic reliably	
[18]	The article proposes DNA act-Ran, a digital DNA sequencing engine that uses machine learning to detect ransomware, utilizing frequency vectors and design limitations for digital sequencing	

3.1 RQ1: What Are the Current State-of-the-Art Techniques and Tools Used for Detecting Ransomware?

Ransomware detection techniques include behavioral analysis, signature-based detection, and machine learning. Popular tools include antivirus software, specialized ransomware detection tools, and managed detection and response services [32]. A combination of these techniques and tools can help detect and protect systems from ransomware attacks.

- Signature-based detection: Signature-based detection compares known malware signatures to identify malware (Malwarebytes)
- Heuristic-based detection: Heuristic-based detection analyzes the behavior of files or processes to detect malware. This can be more effect in detecting new or unknown ransomware
- Machine learning-based detection: Machine learning-based detection uses machine learning models to identify ransomware based on its behavior or characteristics, it may not be able to detect very new ransomware (Crowed strike falcon)
- Behavioral analysis: Behavioral analysis monitors process behavior to identify suspicious activity that may indicate the presence of ransomware, may generate false positive (McAfee)
- Network traffic analysis: Network traffic analysis examines network traffic to identify suspicious activity that may indicate the presence of ransomware
- Sandboxing: Sandboxing runs files or processes in a controlled environment to observe their behavior and identify ransomware

3.2 RQ2: How Effective Are Existing Mitigation Strategies in Preventing Ransomware Attacks and Their Associated Damages?

Mitigation strategies such as regular data backups, patch management, user education, and antivirus software can be effective in preventing ransomware attacks and their damages. However, their effectiveness depends on proper implementation and maintenance

Table 5. Mitigation Strategy

Mitigation Strategy	Effectiveness
Regular Data Backups	High
User Education and Awareness	High
Multi-factor Authentication	High
Network Segmentation	High
Vulnerability Patching	High
Endpoint Protection Software	Moderate
Intrusion Detection and Prevention Systems	Moderate
Security Information and Event Management (SIEM)	Moderate
Email Filtering and Spam Detection	Moderate
Encryption	Low
Incident Response Planning	Low

[33]. Organizations and individuals should prioritize these strategies to minimize the risk of ransomware attacks illustrated in Tables 5 and 6.

Table 6. Ransomware Tactic techniques

Tactic/Technique	Description	Possible Mitigations
Phishing Emails	Social engineering tricks users into clicking malicious links or opening infected attachments	User education and awareness, email filtering and spam detection, multi-factor authentication
Exploit Kits	Attackers use software vulnerabilities to gain access to systems or networks	Regular vulnerability patching, network segmentation; intrusion detection and prevention systems [27, 35]
Remote Desktop Protocol (RDP) Attacks	Attackers use brute-force methods to gain access to RDP connections [34]	Secure RDP access with strong passwords, MFA, IP whitelisting
Fileless Attacks	Fileless techniques evade detection and analysis, execute code sans disk [26]	Endpoint detection and response tools, intrusion detection and prevention systems, regular system auditing
Supply Chain Attacks	Attackers target third-party software providers to gain access to systems and networks [36]	Vendor risk management, regular patching and updates, network segmentation
Zero-Day Exploits	Attackers exploit unknown software vulnerabilities to access systems/networks [37]	Ensure security with scanning, IDS/IPS, and network segmentation

3.3 What Are the Most Common Tactics and Techniques Used by Ransomware Attackers and How Can These Be Thwarted?

Ransomware attackers commonly use social engineering, phishing, and software vulnerabilities to gain access to systems and demand payment [30]. To thwart these attacks, user education, software patching, data backups, network segmentation, and access controls can help prevent these attacks and limit their impact.

4 Mitigation and Prevention Techniques of Ransomware

Preventing ransomware is crucial to protect against its damaging effects on individuals and corporations. In case of infection, data recovery can be challenging and may require the help of a trusted specialist. Pre-encryption mitigation refers to the security measures taken before the encryption process to minimize the risk of security breaches.

- Implementing strict access policies, network segmentation, regular software, and hardware updates, password management and employee training and awareness
- Quarantine suspicious emails, inspect attachments in malware sandbox
- To identify unknown ransomware at pre-encryption stage
- During detection of ransomware, false positives, and false negatives high
- To prevent execution of exploits in a user's system
- Hibernate system to interrupt encryption and recover file encryption key
- To block ransomware when ransomware starts encryption, it is recommended

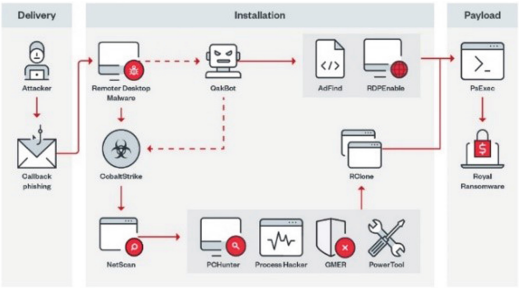

Fig. 5. Ransomware attack life cycle [32]

5 Recommendations

Ransomware is a major cybersecurity threat, with limitations in current prevention and detection methods. Improved prediction techniques are necessary to identify future attacks, along with cyber profiling and transaction tracing to track ransom payments and attackers. Despite significant research efforts, finding a long-term solution to pre-encryption of ransomware remains a critical challenge due to its dynamic nature. Organizations can minimize the risk of security breaches and protect sensitive information from unauthorized access, which can help them avoid costly security incidents and reputational damage (Fig. 5 and 6).

The ransomware mitigation paradigm focuses on defining parameters for the pre-encryption phase of the lifecycle, allowing the model to respond before sabotage occurs. This allocation prevents premature cutoff issues and allows for sufficient data collection. A temporally correlated pre-encryption description technique, based on the IRP-API, links resources to cryptography-related APIs. This API separates the pre-encryption phase and encryption phase for user-related files. Machine learning algorithms are applied to forecast ransomware or benign attacks, using pre-encryption border entries to identify ransomware instances [38].

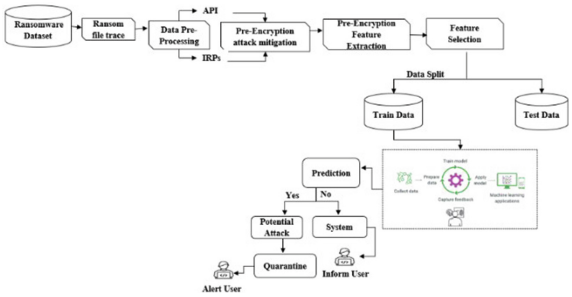

Fig. 6. Ransomware pre-encryption attack mitigation model

6 Conclusion

This paper discusses the emerging cyber-threat of ransomware and its monetary impact on organizations. It analyzes various security measures and proposes a model for preventive measures to avoid pre-encryption attacks. Tools like endpoint protection solutions, intrusion detection systems, and advanced threat detection technologies can help organizations detect and prevent ransomware attacks. Utilizing these tools enhances defense strategy effectiveness. In the future ransomware can be detected at early stage and also pre-encryption can be implemented with machine learning algorithm to reduce false positive and false negative rates, also can be improved using heuristic based to detect new and unknown ransomware.

Acknowledgement. This research work was supported by the Universiti Technologi PETRONAS, Malaysia STIRF Research Grant Project (Cost Centre No. 015LA0-036).

References

1. Kamil, S., Siti Norul, H.S.A., Firdaus, A., Usman, O.L.: The rise of ransomware: a review of attacks, detection techniques, and future challenges. In: 2022 Int. Conf. Bus. Anal. Technol. Secur. ICBATS 2022 (2022). https://doi.org/10.1109/ICBATS54253.2022.9759000
2. Yazdinejad, A., Parizi, R.M., Dehghantanha, A., Zhang, Q., Choo, K.K.R.: An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. IEEE Trans. Serv. Comput.Comput. **13**(4), 625–638 (2020). https://doi.org/10.1109/TSC.2020.2966970
3. Ekta, Bansal, U.: A review on ransomware attack. In: ICSCCC 2021 - Int. Conf. Secur. Cyber Comput. Commun., pp. 221–226 (2021). https://doi.org/10.1109/ICSCCC51823.2021.9478148
4. Sittig, D.F., Singh, H.: A socio-technical approach to preventing, mitigating, and recovering from Ransomware attacks. Appl. Clin. Inform. **7**(2), 624–632 (2016). https://doi.org/10.4338/ACI-2016-04-SOA-0064
5. Monika, P.Z., Lindskog, D.: Experimental analysis of ransomware on windows and android platforms: evolution and characterization. Procedia Comput. Sci. **94**, 465–472 (2016). https://doi.org/10.1016/j.procs.2016.08.072
6. Yazdinejad, A., Parizi, R.M., Dehghantanha, A., Choo, K.K.R.: P4-to-blockchain: a secure blockchain-enabled packet parser for software defined networking. Comput. Secur.. Secur. **88**, 101629 (2020). https://doi.org/10.1016/j.cose.2019.101629

7. Zimba, A.: Malware-free intrusion: a novel approach to ransomware infection vectors. Int. J. Comput. Sci. Inf. Secur. **15**(2), 317–325 (2017). https://search.proquest.com/docview/1879494467?accountid=15977%5Cnhttp://su3pq4eq3l.search.serialssolution.com?ctx_ver=Z39.882004&ctx_enc=info:ofi/enc:UTF8&rfr_id=info:sid/ProQ%3Acriminaljusticeperiodicals&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.ge
8. Zimba, A., Wang, Z., Chen, H.: Multi-stage crypto ransomware attacks: a new emerging cyber threat to critical infrastructure and industrial control systems. ICT Express **4**(1), 14–18 (2018). https://doi.org/10.1016/j.icte.2017.12.007
9. Cohen, A., Nissim, N.: Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory. Expert Syst. Appl. **102**, 158–178 (2018). https://doi.org/10.1016/j.eswa.2018.02.039
10. Reshmi, T.R.: Information security breaches due to ransomware attacks - a systematic literature review. Int. J. Inf. Manage. Data Insights **1**(2). Elsevier Ltd, Nov. 01, 2021. doi: https://doi.org/10.1016/j.jjimei.2021.100013
11. Maigida, A.M., Abdulhamid, S.M., Olalere, M., Alhassan, J.K., Chiroma, H., Dada, E.G.: Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. J. Reliab. Intell. Environ. **5**(2), 67–89 (2019). https://doi.org/10.1007/s40860-019-00080-3
12. Alenezi, M.N., Alabdulrazzaq, H., Alshaher, A.A., Alkharang, M.M.: Evolution of malware threats and techniques: a review. Int. J. Commun. Networks Inf. Secur. **12**(3), 326–337 (2020). https://doi.org/10.17762/ijcnis.v12i3.4723
13. Yazdinejad, A., Dehghantanha, A., Parizi, R.M., Hammoudeh, M., Karimipour, H., Srivastava, G.: Block hunter: federated learning for cyber threat hunting in blockchain-based IIoT networks. IEEE Trans. Ind. Informatics **18**(11), 8356–8366 (2022). https://doi.org/10.1109/TII.2022.3168011
14. Abdullahi, M., Ngadi, M.A., Abdulhamid, S.M.: Symbiotic Organism Search optimization based task scheduling in cloud computing environment. Futur. Gener. Comput. Syst.. Gener. Comput. Syst. **56**, 640–650 (2016). https://doi.org/10.1016/j.future.2015.08.006
15. Urooj, U., Al-Rimy, B.A.S., Zainal, A., Ghaleb, F.A., Rassam, M.A.: Ransomware Detection using the dynamic analysis and machine learning: a survey and research directions. Appl. Sci. **12**(1) (2022). https://doi.org/10.3390/app12010172
16. Nadir, I., Bakhshi, T.: Contemporary cybercrime: a taxonomy of ransomware threats & mitigation techniques. In: 2018 Int. Conf. Comput. Math. Eng. Technol. Inven. Innov. Integr. Socioecon. Dev. iCoMET 2018 - Proc., vol. 2018-January, no. February, pp. 1–7 (2018). https://doi.org/10.1109/ICOMET.2018.8346329
17. Jegede, A., Fadele, A., Onoja, M., Aimufua, G., Mazadu, I.J.: Trends and future directions in automated ransomware detection. J. Comput. Soc. Informatics **1**(2), 17–41 (2022). https://doi.org/10.33736/jcsi.4932.2022
18. Khan, F., Ncube, C., Ramasamy, L.K., Kadry, S., Nam, Y.: A digital DNA sequencing engine for ransomware detection using machine learning. IEEE Access **8**, 119710–119719 (2020). https://doi.org/10.1109/ACCESS.2020.3003785
19. Naidu, P.S., Kharat, R.: Security in Computing and Communications, vol. 625 (2016). https://doi.org/10.1007/978-981-10-2738-3
20. Turner, A.B., McCombie, S., Uhlmann, A.J.: Discerning payment patterns in Bitcoin from ransomware attacks. J. Money Laund. Control **23**(3), 545–589 (2020). https://doi.org/10.1108/JMLC-02-2020-0012
21. Alhawi, O.M.K., Baldwin, J., Dehghantanha, A.: Leveraging machine learning techniques for windows ransomware network traffic detection. In: Advances in Information Security, vol. 70, Springer New York LLC, pp. 93–106 (2018). https://doi.org/10.1007/978-3-319-73951-9_5

22. Humayun, M., Jhanjhi, N.Z., Alsayat, A., Ponnusamy, V.: Internet of things and ransomware: evolution, mitigation and prevention. Egypt. Informatics J. **22**(1), 105–117 (2021). https://doi.org/10.1016/j.eij.2020.05.003
23. Sajjan, R.S., Ghorpade, V.R.: Ransomware attacks: Radical menace for cloud computing. In: Proc. 2017 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2017, vol. 2018-January, no. May 2005, pp. 1640–1646 (2018). https://doi.org/10.1109/WiSPNET.2017.8300039
24. Azzedin, F., Suwad, H., Rahman, M.M.: An asset-based approach to mitigate zero-day ransomware attacks. Comput. Mater. Contin. **73**(2), 3003–3020 (2022). https://doi.org/10.32604/cmc.2022.028646
25. Yeboah-ofori, A.: Mitigating Cybercrimes in An Evolving Organizational Landscape (2022)
26. Aslan, O., Samet, R.: A comprehensive review on malware detection approaches. IEEE Access **8**, 6249–6271 (2020). https://doi.org/10.1109/ACCESS.2019.2963724
27. Akhtar, M.S., Feng, T.: Malware analysis and detection using machine learning algorithms. Symmetry **14**(11) (2022). https://doi.org/10.3390/sym14112304
28. S. Sundaram, IEEE Computational Intelligence Society, and Institute of Electrical and Electronics Engineers, Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence (SSCI 2018) : 18–21 November 2018, Bengaluru
29. Naeem, M.R., et al.: A malware detection scheme via smart memory forensics for windows devices. Mob. Inf. Syst. 2022, 2022, doi: https://doi.org/10.1155/2022/9156514
30. Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., Davidson, I.E.: Ransomware detection, avoidance, and mitigation scheme: a review and future directions. Sustain. **14**(1), 1–24 (2022). https://doi.org/10.3390/su14010008
31. Al-rimy, B.A.S., Maarof, M.A., Shaid, S.Z.M.: Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. Comput. Secur.. Secur. **74**, 144–166 (2018). https://doi.org/10.1016/j.cose.2018.01.001
32. Maurya, A.K., Kumar, N., Agrawal, A., Khan, R.A.: Ransomware evolution, target and safety measures. Int. J. Comput. Sci. Eng.Comput. Sci. Eng. **6**(1), 80–85 (2018). https://doi.org/10.26438/ijcse/v6i1.8085
33. Maimó, L.F., Celdrán, A.H., Perales Gómez, Á.L., García Clemente, F.J., Weimer, J., Lee, I.: Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. Sensors **19**(5), 1–31 (2019). https://doi.org/10.3390/s19051114
34. Yazdinejad, A., Bohlooli, A., Jamshidi, K.: Performance improvement and hardware implementation of Open Flow switch using FPGA. In: 2019 IEEE 5th Conf. Knowl. Based Eng. Innov. KBEI 2019, no. February, pp. 515–520 (2019). doi: https://doi.org/10.1109/KBEI.2019.8734914
35. Subedi, K.P., Budhathoki, D.R., Dasgupta, D.: Forensic analysis of ransomware families using static and dynamic analysis. In: Proc. - 2018 IEEE Symp. Secur. Priv. Work. SPW 2018, pp. 180–185 (2018). https://doi.org/10.1109/SPW.2018.00033
36. Beaman, C., Barkworth, A., Akande, T.D., Hakak, S., Khan, M.K.: Ransomware: Recent advances, analysis, challenges and future research directions. Comput. Secur. **111**, December 2021. https://doi.org/10.1016/j.cose.2021.102490
37. I. PES Institute of Technology (Bangalore, IEEE Communications Society, IEEE Photonics Society. Bangalore Chapter, IEEE Robotics and Automation Society. Bangalore Chapter, and Institute of Electrical and Electronics Engineers, 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 19–22 Sept. 2018
38. Alqahtani, A., Gazzan, M., Sheldon, F.T.: A proposed Crypto-Ransomware Early Detection (CRED) model using an integrated deep learning and vector space model approach. In: 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2020, pp. 0275–0279. https://doi.org/10.1109/CCWC47524.2020.9031182