MATICS : Jurnal Ilmu Komputer dan Teknologi Informasi ISSN : 1978-161X(p); 2477-2550(e)
Volume 16, No. 2(2024), pp 76-83 DOI : 10.18860/mat.v16i2.28794
Received : August 5th 2024; **Accepted** : August 28th 2024 ; **Avalaible Online** : September 20th 2024

Mitigation of Malware Ransomware Virus

Aan Ansori, Fitri Damyati, Syifa Amara Dhestyani.

***Abstract*— This research aims to explore and analyze ransomware mitigation strategies, a type of malware that encrypts data and demands a ransom. A literature review was used to collect and analyze data from academic journals, industry reports, and technical publications. The analysis of the literature indicates that prevention strategies such as user education, routine data Backups, and software updates are effective in reducing the risk of attacks. Early detection technologies, including intrusion detection systems and behavior analysis, have proven capable of identifying attacks before significant damage occurs. A swift and coordinated response, involving the isolation of infected systems and forensic analysis, can minimize impact and recovery costs. The research concludes that ransomware mitigation requires a holistic approach encompassing prevention, early detection, and rapid response. The combination of these strategies is effective in reducing damage and recovery costs following a ransomware attack.**

***Index Terms*—**Mitigation, malware, and ransomware**.**

I. INTRODUCTION

Ransomware attacks have become an increasingly alarming threat to cybersecurity, especially when linked to attacks on several government websites in the Republic of Indonesia. These incidents highlight significant vulnerabilities in the government's digital infrastructure, where cybercriminals successfully infect and encrypt critical data, resulting in disruptions to crucial public services. For example, attacks on ministry and state agency websites disrupt daily operations and delay various administrative processes essential to the public. The damages incurred are not only financial but also harm the government's reputation and diminish public trust in national security systems. Moreover, the advanced techniques used by attackers, such as phishing emails and software vulnerability exploitation, demonstrate the need for a more proactive and integrated security system enhancement. In facing this ever-evolving threat, the Indonesian government needs to adopt a layered approach that includes prevention, early detection, and a swift and coordinated response to protect digital assets and ensure the continuity of public services.

Manuscript received August 5, 2024. This work was supported in part by UIN SMH Banten.

Aan Ansori is with the UIN SMH Banten, Indonesia (aan.ansori@uinbanten.ac.id)

Fitri Damyati is with the University Tirtayasa, Banten, Indonesia (fitri.damyati@untira.ac.id)

Syifa Amara Dhestyani is with the Telkom University, Bandung, Indonesia (syifaamdh@student.telkomuniversity.ac.id)

Ransomware attacks have also become a serious threat to internet users, especially for average users who often lack knowledge and preparedness against cyber threats. Ransomware encrypts users' data and demands a ransom for the restoration of access, causing significant financial and emotional damage. Many average users who fall victim to these attacks are reluctant to report them due to fear, shame, or a lack of understanding of the steps to take. This unawareness exacerbates the problem, as without reports, efforts to track, understand, and address the attacks become more difficult for cybersecurity authorities. As a result, average users often have to bear the losses themselves, losing important data such as personal documents, photos, and financial information. The lack of reporting also makes it difficult to measure the true scale of the ransomware threat and reduces the opportunities to provide appropriate education and assistance to the general public. Ransomware is one of the most significant and damaging forms of malware threats in today's cybersecurity landscape.[1] This type of malware works by encrypting data on the infected device, then demanding a ransom from the victim to obtain the decryption key. Ransomware incidents have increased drastically in recent years, targeting various sectors including government, healthcare, education, and business.

The history of ransomware can be traced back to the late 1980s when the first known attack, known as the 'AIDS Trojan,' appeared. [2] At that time, this ransomware, developed by early cybercriminals, was designed to encrypt user files and demand a ransom in the form of a postal check to obtain the decryption key. Although this attack was relatively simple compared to modern threats, it marked the beginning of a phenomenon that later evolved into a serious global threat. Over time, ransomware has undergone significant evolution in complexity and destructive power. Modern ransomware is now much more sophisticated and organized, with variants such as WannaCry, Petya, and CryptoLocker causing financial losses reaching billions of dollars worldwide. These attacks not only target individuals but also large organizations and critical infrastructure, highlighting the dangerous nature of this threat and underscoring the urgent need for effective mitigation strategies and robust defense systems.

The main challenge faced in mitigating ransomware is the rapid evolution of techniques used by attackers.[3] Ransomware has evolved from using simple techniques such as spam emails and malicious attachments to

complex multi-phase attacks that involve exploiting zero-day vulnerabilities and spreading through infected networks.[4]

Prevention is the first and most critical step in ransomware mitigation.[5] Effective prevention measures include educating and training users to recognize signs of phishing attacks, implementing strict data backup policies, and regularly updating and patching software and operating systems.[6] In addition to prevention, early detection is a key element in reducing the impact of ransomware attacks. Technologies such as intrusion detection systems (IDS), advanced firewalls, and endpoint detection and response (EDR) solutions can help detect suspicious activity before an attack causes significant damage.[7]

Response to ransomware incidents must be swift and coordinated to minimize impact and prevent further damage. The critical first step is isolating the infected systems to prevent further spread of the ransomware to other networks or devices. Once the system is isolated, forensic analysis should be conducted to determine the ransomware's point of entry, the attack methods used, and any patterns of spread that may have occurred. This process involves a thorough examination of system logs, infected files, and the techniques used by the perpetrators to exploit vulnerabilities.[8] Additionally, data recovery through reliable backups is a key step in restoring normal operations without having to meet ransom demands. Regularly performed backups stored in secure locations can be lifesavers in this situation, allowing organizations to recover important data and reduce reliance on ransom payments..[9] Integrating all these steps into a comprehensive response plan allows organizations to handle ransomware attacks more effectively, reduce financial and operational impact, and strengthen defenses against potential future attacks.

Ransomware incidents can provide valuable insights into the effectiveness of various mitigation strategies and weaknesses in cybersecurity systems. A notable example is the WannaCry attack in 2017, which exploited vulnerabilities in the Windows SMB protocol.[10] This attack caused widespread global damage, disrupting operations across various organizations from hospitals to private companies, and highlighted the importance of timely software updates. WannaCry demonstrated how ransomware can spread rapidly through unpatched networks, prompting many organizations to improve their policies on security patches and routine updates. A similar incident also occurred in Indonesia in 2024, when the National Data Center (PDN) experienced a ransomware attack that resulted in significant disruptions to public services.[11] This attack illustrates how vulnerable critical infrastructure is to cyber threats and how deficiencies in mitigation practices can exacerbate the impact. The incident at the PDN revealed the urgent need to enhance preventive measures, such as routine data backups and cybersecurity training for users, to protect data and ensure operational continuity. The experiences from both incidents underscore the importance of a proactive and coordinated approach in ransomware mitigation strategies.[12]

Evaluating the effectiveness of ransomware mitigation strategies requires a holistic and comprehensive approach, involving various aspects to ensure thorough protection. First, assessing the success of preventive measures is crucial for understanding how effective prevention efforts, such as user education, data backup policies, and software updates, are. This involves analyzing whether these measures can prevent attacks or reduce their likelihood. Additionally, the speed and efficiency of response to incidents are also critical elements in the evaluation. This includes the organization's ability to quickly detect attacks, isolate infected systems, and implement effective recovery strategies to minimize impact. Slow or inefficient responses can amplify damage and increase recovery costs. Furthermore, the evaluation should account for recovery costs and the long-term impact of attacks. This includes calculating costs associated with data recovery, system repairs, and operational losses due to service disruptions. Additionally, long-term impacts such as reputation damage and decreased customer trust should be analyzed to fully understand the consequences of ransomware attacks. This evaluation provides a comprehensive view of the effectiveness of mitigation strategies and helps organizations formulate improvement measures to enhance their readiness for future cyber threats. A comprehensive approach ensures that all aspects of mitigation, from prevention to recovery, are carefully considered to effectively reduce the risk and impact of ransomware attacks.

This research aims to provide an in-depth analysis of various ransomware mitigation strategies, identify best practices, and offer recommendations to enhance readiness and response to future ransomware threats.

II. METHODS

This research uses a literature review method to collect and analyze data related to ransomware mitigation strategies.[13] The literature review method was chosen because it allows researchers to access a variety of relevant information sources, including academic journals, industry reports, and technical publications.[14] These sources include articles published in leading cybersecurity journals, reports from cybersecurity companies such as Kaspersky Lab, Symantec, and Trend Micro, as well as technical documentation from organizations such as NIST, Europol, and the FBI, which provide guidance and recommendations for ransomware mitigation.

The data collection process begins with identifying relevant sources, followed by gathering information on various types of ransomware, implemented mitigation strategies, and analysis of notable ransomware incidents. The collected data is classified based on categories such as ransomware types, mitigation strategies, and case study outcomes.[15] Analysis is conducted qualitatively to identify trends, key findings, and best practices in ransomware mitigation. The

effectiveness of mitigation strategies is evaluated based on indicators such as the success rate of prevention, response speed, and recovery costs.

The results of the analysis are then compiled into a structured report, which includes an introduction, methods, results and discussion, as well as conclusions.[16] To provide in-depth and evidence-based insights into ransomware mitigation strategies and identify best practices that can be implemented to enhance cybersecurity across various organizations. By using the literature review method, this research aims to offer a comprehensive overview of effective measures for reducing the risk and impact of ransomware attacks.

III. RESULTS

This literature review research reveals several key findings regarding effective ransomware mitigation and evolving attack trends. One major finding is that ransomware continues to evolve at an alarming rate, with cybercriminals constantly updating their techniques and variants to evade detection. New variants of ransomware are often more sophisticated and harder to detect, making unpatched systems highly vulnerable to attacks.

The WannaCry ransomware attack incident in 2017, which exploited vulnerabilities in the Windows SMB protocol.[17] This attack caused widespread global damage by encrypting data on thousands of systems worldwide. In 2023, one bank in Indonesia was also suspected of being hit by a ransomware attack that mutated from LockBit, [18] and in 2024, the National Data Center (PDN) experienced a ransomware attack that resulted in significant disruptions to public services. [12] The experiences from these incidents highlight the importance of a proactive and coordinated approach in ransomware mitigation strategies. This necessitates a holistic and comprehensive evaluation of the effectiveness of ransomware mitigation strategies, involving various aspects to ensure thorough protection. Therefore, effective strategies and mitigations are required.

The most effective mitigation strategies involve a layered approach that combines prevention, early detection, and rapid response. For instance, ransomware prevention relies heavily on measures such as keeping operating systems and software up to date, using reliable antivirus and antimalware software, and educating users about cybersecurity risks and best practices. Early detection is also crucial, and this can be achieved by utilizing advanced network and system monitoring tools to detect suspicious activity before ransomware can cause significant damage.[19]

Mitigation steps in dealing with ransomware attacks are a series of actions and strategies designed to prevent, reduce, and handle the impact of ransomware attacks. Mitigation steps involve proactive and reactive approaches to manage the risks and consequences posed by ransomware attacks.[20]

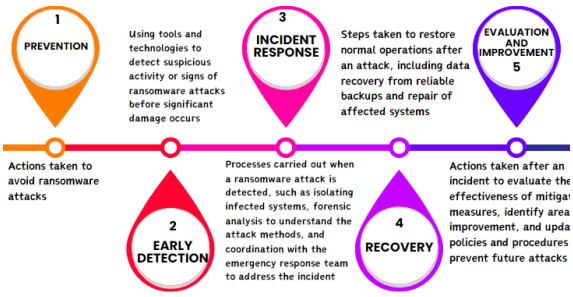

Fig. 1. Mitigation of ransomware attacks

These mitigation steps may include:

1. **Prevention**:
   To prevent ransomware attacks, key steps include educating users about threats and signs of an attack, implementing strict security policies such as using strong passwords and multi-factor authentication, and using up-to-date security software like antivirus and firewalls.[21] Additionally, it is important to regularly back up data and store it in a separate location, ensure timely system updates and patches, and set up email filters to block phishing emails. Active monitoring of systems and using detection systems can also help prevent ransomware attacks.
2. **Early Detection:**
   For early detection of ransomware attacks, actions include monitoring systems and networks for suspicious activity, using behavioral analysis to detect unusual patterns, implementing intrusion detection systems (IDS), conducting regular audits and reviewing activity logs, and utilizing specialized ransomware detection tools.[22]
3. **Incident Response:**
   Actions in response to ransomware incidents include isolating the infected systems to prevent further spread, conducting forensic analysis to understand the attack methods and entry points, coordinating with emergency response teams for incident handling, and notifying and involving relevant parties such as vendors and authorities if necessary.[23]
4. **Recovery:**
   Actions in responding to ransomware incidents include isolating the infected systems to prevent further spread, conducting forensic analysis to understand the attack methods and entry points, coordinating with emergency response teams for incident management, and notifying and involving relevant parties such as vendors and authorities if necessary.[24]
5. **Evaluation and Improvement:**
   Post-ransomware attack evaluation and improvement involve assessing the effectiveness of mitigation measures, identifying weaknesses in policies and procedures, and improving security processes and policies.[25] These steps also include retraining users and security teams and updating software to address vulnerabilities.

By implementing these mitigation measures, organizations can minimize the risk of ransomware attacks, expedite incident response, and reduce the potential impact and recovery costs.

Ransomware attack prevention strategies consist of a series of actions and policies designed to prevent ransomware infections on computer systems. This strategy includes educating users to recognize and avoid threats, implementing strict security policies, using up-to-date security software, performing routine updates to close vulnerabilities, and adopting best practices such as regular data backups and network segmentation to limit the spread of ransomware if an infection occurs. As illustrated in the following image;[26]

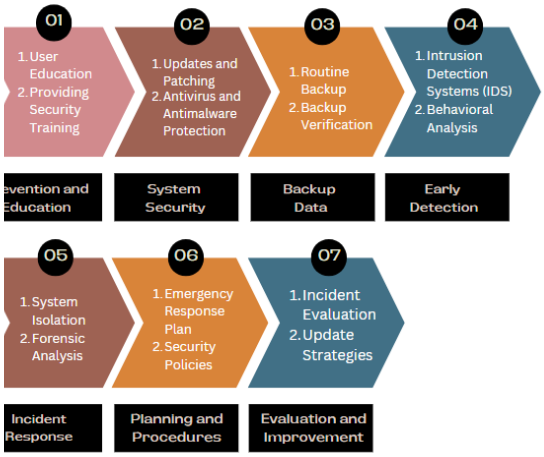

Fig. 2. Strategies for Preventing Ransomware Attacks

Prevention strategies for ransomware attacks and mitigation measures that can be taken to address ransomware threats:[2]

1. **Prevention and Education**
   a) User Education: Train employees and users about the risks of ransomware and how to recognize signs of an attack, such as phishing emails or suspicious attachments.
   b) Security Training: Provide regular training on good security practices, including how to handle suspicious emails and the importance of strong passwords.
2. **System Protection**
   a) Updates and Patching: Ensure that all software, operating systems, and applications are regularly updated to close vulnerabilities that could be exploited by ransomware.
   b) Antivirus and Antimalware Protection: Use up-to-date antivirus and antimalware software to detect and remove threats before they can cause damage.
3. **Backup Data**
   a) Perform regular data backups and store copies in a location separate from the main network. Ensure that backups are accessible and easily recoverable..
   b) Backup Verification: Regularly test and verify the integrity of backups to ensure data can be restored in the event of a ransomware attack.
4. **Early Detection**
   a) Intrusion Detection System (IDS): Implement an intrusion detection system to monitor network activity and identify potential threats.
   b) Behavioral Analysis: Use behavioral analysis tools to detect unusual activity patterns that may indicate a ransomware infection.
5. **Incident Response**
   a) System Isolation: Immediately isolate the infected system to prevent the ransomware from spreading to other devices.
   b) Forensic Analysis: Conduct forensic analysis to determine the point of entry and method of attack, as well as to understand the extent of the impact.
   c) Data Recovery: Restore data from trusted backups. Ensure that the data is free from ransomware before copying it to the main system.
6. **Planning and Procedures**
   a) Emergency Response Plan: Develop and test an emergency response plan that includes steps for dealing with ransomware attacks.
   b) Security Policies: Create and implement clear security policies for device usage, data access, and security responsibilities.
7. **Evaluation and Improvement**
   a) Incident Evaluation: After an attack, conduct an evaluation to assess the effectiveness of the mitigation strategies applied for improvement.
   b) Update Strategies: Adjust and enhance mitigation strategies based on findings from incident evaluations and the latest trends in ransomware threats.

The research findings show that regular data backups are one of the most effective mitigation strategies. Backups stored offline or in a secure location ensure that data can still be recovered without having to pay a ransom in the event of a ransomware attack. Additionally, implementing data encryption and using two-factor authentication (2FA) have also proven effective in protecting sensitive data from unauthorized access.

Intrusion Detection System (IDS) is a security tool that detects and reports suspicious activities on a computer network, helping organizations identify cyber threats before they cause significant damage.[27]

IDS is divided into two main types: Network-based IDS (NIDS), which monitors network traffic, and Host-based IDS (HIDS), which monitors activity on individual devices or servers.[28] IDS is effective in detecting threats that are not picked up by firewalls and provides early warnings.[29] However, IDS also has drawbacks such as a high number of false positives and a reactive nature, only detecting threats after suspicious activity has occurred.

Endpoint Detection and Response (EDR) is a cybersecurity approach designed to monitor and respond to threats on endpoints or end-user devices, such as computers, laptops, mobile devices, and servers.[30] EDR integrates various technologies to detect, investigate, respond to, and mitigate security threats that may compromise endpoint devices.[31]

EDR is a key component in modern cybersecurity that enhances detection and response to threats at endpoints, helping organizations tackle complex cyberattacks.[32] Although effective, EDR requires proper planning and expertise to maximize its benefits..

IV. DISCUSSION

Discussions on ransomware mitigation based on the results of literature review research show that ransomware continues to evolve into a more sophisticated and harder-to-detect threat. One of the main factors enabling this development is the rapid evolution of techniques and variants used by cybercriminals. They continuously update their methods to evade detection by existing security systems. New variants of ransomware often use more complex encryption techniques and exploit zero-day vulnerabilities, which do not yet have security patches from software providers.[33] Therefore, it is crucial for organizations to regularly update their software and operating systems.

The most effective mitigation strategies require a layered approach that combines prevention, early detection, and rapid response. Prevention includes measures such as using reliable antivirus and antimalware software, keeping operating systems and applications up to date, and educating users about cybersecurity risks and best practices. Early detection is crucial for identifying signs of ransomware infection before data is encrypted. Advanced network and system monitoring tools can help detect suspicious activity and enable a quick response before ransomware causes significant damage.

Regular data backups are one of the most crucial mitigation strategies. By having backups stored offline or in a secure location, organizations can restore their data without paying ransom in the event of a ransomware attack. Additionally, implementing data encryption and using two-factor authentication (2FA) have also proven effective in protecting sensitive data from unauthorized access.[34] This approach ensures that even if data is stolen, cybercriminals cannot read it without the correct decryption key.

Collaboration and information sharing between organizations are also important factors in strengthening defenses against ransomware. Initiatives like Information Sharing and Analysis Centers (ISACs) and public-private partnerships help accelerate the dissemination of information about the latest threats and security solutions.[35] Additional references from reports by Cisco, the FBI, and the Ponemon Institute reinforce the findings that a comprehensive and collaborative approach is essential to address the ever-evolving ransomware threat.[36] By adopting the recommended strategies, organizations can enhance their resilience against ransomware attacks and reduce the risk of significant losses.

Results of the SWOT (*Strengths, Weaknesses, Opportunities, Threats*) analysis for IDS; [37]

1) **Strengths**
   a) Network Anomaly Detection: IDS is highly effective in monitoring network traffic and detecting anomalies or unusual attack patterns, including those not detected by firewalls or other security devices.
   b) Early Warning: Provides early alerts to security teams before further attacks occur, allowing for rapid response.
   c) Ability to Detect Malicious Traffic: IDS can identify complex types of attacks.

2) Weaknesses
   a) High Number of False Positives: IDS often generates false alerts, which can disrupt security teams and lead to unnecessary vigilance.
   b) Reactive, Not Proactive: IDS typically detects attacks only after suspicious activity has occurred, not before an attack takes place.
   c) Lack of Automated Response: Cannot automatically respond to threats or attacks; IDS only provides alerts.[38]

3) Opportunities
   a) Integration with AI: Utilizing artificial intelligence (AI) and machine learning to enhance detection accuracy and reduce false positives.
   b) Development of Integrated Detection Systems: Integration with other security solutions such as EDR and SIEM (Security Information and Event Management) to create a more comprehensive defense system.
   c) Demand for Network Security Solutions: Increasing need for better cybersecurity creates opportunities to expand the use of IDS.

4) **Threats**
   a) Evolution of Cyber Attack Tactics: Evolving and increasingly sophisticated threats can make IDS less effective.
   b) Dependence on Expertise: Requires a trained security team to effectively monitor and respond to alerts.
   c) Complexity of Modern Network Management: More complex network infrastructure can make anomaly detection more challenging.

Results of the SWOT (*Strengths, Weaknesses, Opportunities, Threats*) for EDR: [39]

1) **Strengths**
   a) Real-Time Detection and Response: EDR can monitor and analyze endpoint activity in real time to detect and respond to threats more quickly.
   b) Isolation and Recovery Capabilities: Allows for the isolation of infected endpoints and automatic system recovery, minimizing further damage.
   c) In-Depth Forensic Data: Provides detailed forensic data and analysis that aid in incident investigation and the development of improved defense strategies.

2) Weaknesses
   a) Dependency on Endpoints**:** EDR only monitors endpoints and may not detect network traffic or attacks that are not visible to endpoint devices.
   b) Implementation Complexity**:** Requires complex configuration and management, including routine software updates.
   c) Resource Requirements**:** Needs significant resources for data storage and processing for

large-scale data analysis.

3) **Opportunities**
   a) AI and Machine Learning Development**:** Integration of AI can enhance threat detection capabilities proactively and automatically.
   b) Increasing Market Demand for Endpoint Security**:** With the rise in mobile device usage and remote work, the demand for stronger endpoint security solutions is increasing.
   c) Cross-Platform Integration**:** Opportunities to integrate EDR with other security platforms to provide more comprehensive visibility and response.
4) **Threats**
   a) Increasingly Sophisticated Endpoint Attacks**:** New threats like evolving malware or more difficult-to-detect fileless attacks can reduce the effectiveness of EDR.
   b) Dependency on Endpoint Presence**:** If endpoints are disconnected or offline, EDR cannot provide protection.
   c) Competition with Other Security Technologies**:** Other security solutions like XDR (Extended Detection and Response) offer broader detection capabilities, which can reduce reliance on EDR.

V. CONCLUSION

This research highlights the importance of ransomware mitigation as a crucial step in protecting data and systems from increasingly sophisticated cyber threats. Ransomware, with its ability to encrypt data and demand ransom, has become a major threat to individuals and organizations. Literature reviews indicate that ransomware continues to evolve, with cybercriminals using new techniques to avoid detection and maximize the impact of their attacks. Therefore, a layered approach that includes prevention, early detection, and rapid response is key to effectively addressing this threat.

By leveraging AI, IDS can be more effective in analyzing network traffic in real-time and identifying suspicious patterns that may indicate an attack. AI enables IDS to use machine learning algorithms to identify new and previously unknown threats and reduce the number of false positives by filtering truly suspicious activities from normal ones.

On the other hand, with the help of AI, EDR can automatically process and analyze data from various endpoints to detect unusual or suspicious behavior. AI also allows EDR to automate responses to incidents, such as automatically isolating infected systems, automatically updating to address discovered vulnerabilities, and speeding up system recovery.

Both IDS and EDR have their own strengths and weaknesses in addressing cyber threats. IDS focuses more on network anomaly detection, while EDR provides deeper monitoring and response at the endpoint level. Combining both, especially with AI integration, can offer more comprehensive protection against cyber threats.

Preventive strategies, such as updating systems and software, using reliable security software, and educating users about cybersecurity practices, are essential in preventing ransomware infections. Regular data backups and the use of two-factor authentication have also proven effective in minimizing the damage caused by ransomware attacks. Additionally, having a well-prepared incident response plan and a trained cybersecurity team enables organizations to respond quickly and efficiently restore operations after an attack.

Collaboration between organizations and sharing information about the latest threats and security solutions are also crucial factors in strengthening defenses against ransomware. Collaborative initiatives help speed up the dissemination of information and enable a more effective response to cyber attacks.

REFERENCES

[1] M. Ryan, *Ransomware Revolution: the rise of a prodigious cyber threat*, vol. 85. Springer, 2021.

[2] G. Nagar, “The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies,” *Val. Int. J. Digit. Libr.*, pp. 1282–1298, 2024.

[3] R. Richardson and M. M. North, “Ransomware: Evolution, mitigation and prevention,” *Int. Manag. Rev.*, vol. 13, no. 1, p. 10, 2017.

[4] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, “IoMT malware detection approaches: analysis and research challenges,” *IEEE access*, vol. 7, pp. 182459–182476, 2019.

[5] Z. Manjezi and R. A. Botha, “Preventing and Mitigating Ransomware: A Systematic Literature Review,” in *Information Security: 17th International Conference, ISSA 2018, Pretoria, South Africa, August 15–16, 2018, Revised Selected Papers 17*, 2019, pp. 149–162.

[6] O. Sarker, A. Jayatilaka, S. Haggag, C. Liu, and M. A. Babar, “A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness,” *J. Syst. Softw.*, vol. 208, p. 111899, 2024.

[7] D. Morato, E. Berrueta, E. Magaña, and M. Izal, “Ransomware early detection by the analysis of file sharing traffic,” *J. Netw. Comput. Appl.*, vol. 124, pp. 14–32, 2018.

[8] S. Maniath, P. Poornachandran, and V. G. Sujadevi, “Survey on prevention, mitigation and containment of ransomware attacks,” in *Security in Computing and Communications: 6th International Symposium, SSCC 2018, Bangalore, India, September 19–22, 2018, Revised Selected Papers 6*, 2019, pp. 39–52.

[9] J. Beattie and M. Shandrowski, “Cyber-compromised data recovery: The more likely disaster recovery use case,” *J. Bus. Contin. Emer. Plan.*, vol. 15, no. 2, pp. 114–126, 2021.

[10] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "Ransomware detection and mitigation using software-defined networking: The case of WannaCry," *Comput. Electr. Eng.*, vol. 76, pp. 111–121, 2019.

[11] R. D. Hapsari and K. G. Pambayun, "Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis," *J. Konstituen*, vol. 5, no. 1, pp. 1–17, 2023.

[12] F. I. Adristi and E. Ramadhani, "Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede," *Sel. Manaj. J. Mhs. Bisnis Manaj.*, vol. 2, no. 6, pp. 196–212, 2024.

[13] A. M. Maigida, S. M. Abdulhamid, M. Olalere, J. K. Alhassan, H. Chiroma, and E. G. Dada, "Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms," *J. Reliab. Intell. Environ.*, vol. 5, pp. 67–89, 2019.

[14] H. Kurniawan *et al.*, *TEKNIK PENULISAN KARYA ILMIAH: Cara membuat Karya Ilmiah yang baik dan benar*. PT. Sonpedia Publishing Indonesia, 2023.

[15] B. A. S. Al-Rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," *Comput. Secur.*, vol. 74, pp. 144–166, 2018.

[16] H. Kallio, A. Pietilä, M. Johnson, and M. Kangasniemi, "Systematic methodological review: developing a framework for a qualitative semi-structured interview guide," *J. Adv. Nurs.*, vol. 72, no. 12, pp. 2954–2965, 2016.

[17] S. Askarifar, N. A. A. Rahman, and H. Osman, "A review of latest wannacry ransomware: Actions and preventions," *J. Eng. Sci. Technol*, vol. 13, pp. 24–33, 2018.

[18] N. Tambunan *et al.*, "Berita utama tentang error service di Bank Syariah Indonesia (BSI)," *Community Dev. J. J. Pengabdi. Masy.*, vol. 4, no. 2, pp. 5096–5098, 2023.

[19] R. Brewer, "Ransomware attacks: detection, prevention and cure," *Netw. Secur.*, vol. 2016, no. 9, pp. 5–9, 2016.

[20] D. F. Sittig and H. Singh, "A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks," *Appl. Clin. Inform.*, vol. 7, no. 02, pp. 624–632, 2016.

[21] Y. Diogenes and E. Ozkaya, *Cybersecurity–Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals*. Packt Publishing Ltd, 2019.

[22] U. Urooj, B. A. S. Al-rimy, A. Zainal, F. A. Ghaleb, and M. A. Rassam, "Ransomware detection using the dynamic analysis and machine learning: A survey and research directions," *Appl. Sci.*, vol. 12, no. 1, p. 172, 2021.

[23] V. Szücs, G. Arányi, and Á. Dávid, "Introduction of the ARDS—anti-ransomware defense System model—based on the systematic review of worldwide ransomware attacks," *Appl. Sci.*, vol. 11, no. 13, p. 6070, 2021.

[24] N. R. Bodlapati, "Analysis of Best Practices for the Prevention of Ransomware Attacks," 2021.

[25] A. Mukhopadhyay and S. Jain, "A framework for cyber-risk insurance against ransomware: A mixed-method approach," *Int. J. Inf. Manage.*, vol. 74, p. 102724, 2024.

[26] S. R. Gudimetla, "Ransomware Prevention and Mitigation Strategies," *J. Innov. Technol.*, vol. 5, no. 1, 2022.

[27] R. G. Bace and P. Mell, "Intrusion detection systems," 2001.

[28] A. Efe and İ. N. Abacı, "Comparison of the host based intrusion detection systems and network based intrusion detection systems," *Celal Bayar University Journal of Science*, vol. 18, no. 1. Celal Bayar University, pp. 23–32, 2022.

[29] J. M. Kizza, "System intrusion detection and prevention," in *Guide to computer network security*, Springer, 2024, pp. 295–323.

[30] E. C. Thompson, *Cybersecurity incident response: How to contain, eradicate, and recover from incidents*. Apress, 2018.

[31] A. Mishra, *Modern Cybersecurity Strategies for Enterprises: Protect and Secure Your Enterprise Networks, Digital Business Assets, and Endpoint Security with Tested and Proven Methods (English Edition)*. BPB Publications, 2022.

[32] A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, "Endpoint detection & response: A malware identification solution," in *2021 International Conference on Cyber Warfare and Security (ICCWS)*, 2021, pp. 1–8.

[33] A. Waheed, B. Seegolam, M. F. Jowaheer, C. L. X. Sze, E. T. F. Hua, and S. R. Sindiramutty, "Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure," 2024.

[34] G. Ali, M. Ally Dida, and A. Elikana Sam, "Two-factor authentication scheme for mobile money: A review of threat models and countermeasures," *Futur. Internet*, vol. 12, no. 10, p. 160, 2020.

[35] M. Karpiuk and J. Kostrubiec, "Activities for Cybersecurity as a Mission of Information Sharing and Analysis Centres," *First Publ. 2022*

by, p. 39, 2022.

[36] F. Iqbal, M. Debbabi, B. C. M. Fung, F. Iqbal, M. Debbabi, and B. C. M. Fung, "Cybersecurity And Cybercrime Investigation," *Mach. Learn. Authorsh. Attrib. Cyber Forensics*, pp. 1–21, 2020.

[37] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, no. 1–2, pp. 18–28, 2009.

[38] S. Anwar *et al.*, "From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions," *Algorithms*, vol. 10, no. 2, p. 39, 2017.

[39] H. Kaur *et al.*, "Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review," in *E3S Web of Conferences*, 2024, vol. 556, p. 1006.