




Investigating and Mitigating Ransomware (1).docx

-  My Files
-  My Files
-  Universidad Wiener

Document Details

Submission ID

trn:oid:::14912:376625437

Submission Date

Aug 29, 2024, 4:23 PM GMT+1

Download Date

Aug 29, 2024, 4:29 PM GMT+1

File Name

Investigating and Mitigating Ransomware (1).docx

File Size

1.2 MB

75 Pages

15,621 Words

96,946 Characters

73% detected as AI

The percentage indicates the combined amount of likely AI-generated text as well as likely AI-generated text that was also likely AI-paraphrased.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Detection Groups



1 AI-generated only 72%

Likely AI-generated text from a large-language model.



2 AI-generated text that was AI-paraphrased 1%

Likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?

The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.





School of Science and Technology

INVESTIGATION AND MITIGATION OF RANSOMWARE

SUPERVISED BY (SUPERVISOR'S NAME)

"Project Report submitted in partial fulfillment of the requirements of Nottingham Trent University for the degree of MSc IT Security".

YOUR NAME (STUDENT NUMBER)

AUGUST 2024

ABSTRACT

This dissertation delves into the realm of ransomware detection and mitigation, an evolving cyber threat that presents substantial risks to organizations globally. The study seeks to develop a comprehensive framework to improve the detection and prevention of ransomware attacks while minimizing their impact. Through an in-depth review of existing literature, the research identifies the strengths and limitations of current detection methods, including signature-based and behavior-based approaches. It proposes the integration of advanced technologies such as artificial intelligence and machine learning to enhance accuracy and adaptability. The study also examines the importance of prevention measures, such as software updates, multi-factor authentication, and user education programs, in reducing vulnerabilities. Additionally, it highlights the critical role of incident response planning, legal and compliance frameworks, and continuous research and adaptation in creating a resilient defense against ransomware. By providing an overview of ransomware mitigation strategies, this dissertation contributes to the understanding of how organizations can protect themselves against this growing threat. The findings emphasize the need for a multi-layered defense system, the significance of human factors in cybersecurity, and the benefits of international collaboration in combating ransomware. Suggestions for further studies include exploring emerging ransomware variants, the impact of new technologies, and the economic implications of ransom payments, offering a pathway for future research in this critical area. This research not only addresses current challenges in ransomware detection and mitigation, but also lays the groundwork for future advancements in cybersecurity practices, aiming to safeguard digital assets in an increasingly interconnected world.

ACKNOWLEDGEMENTS

I would like to express my gratitude to my supervisor for his guidance, support, and motivation which has helped me to grow academically and personally. I would also like to extend my heartfelt thanks to my friends, family, and most especially my wife for their unwavering support and understanding during this journey. Their encouragement has kept me motivated and I couldn't have accomplished this without them by my side.

Once again, thank you for the sacrifice and motivation during this period.

TABLE OF CONTENTS

| | |
|--|-----------|
| ABSTRACT | 2 |
| ACKNOWLEDGEMENTS | 3 |
| CHAPTER ONE: INTRODUCTION | 7 |
| 1.1 Background to the Study | 7 |
| 1.2 Problem Statement | 9 |
| 1.3 Aim and Objectives | 10 |
| 1.4 Significance of the Study | 11 |
| 1.5 PSEL Issues | 12 |
| 1.6 Structure of Dissertation | 13 |
| CHAPTER TWO: LITERATURE REVIEW | 15 |
| 2.1 Introduction | 15 |
| 2.2 Definition of Ransomware | 15 |
| 4.1 Overview of Colonial Pipeline Ransomware Attack | 18 |
| 2.5.1 Classification by Target | 23 |
| 2.5.2 Classification by Infection Vectors | 26 |
| 2.6 Ransomware infection path | 27 |
| 4.2 Detecting ransomware | 29 |
| 3.1 Introduction | 34 |
| 3.2 Research Design | 34 |
| 3.3 Data Collection Methods | 35 |
| 3.4 Inclusion and Exclusion Criteria | 37 |
| 3.5 Data Analysis Techniques | 38 |
| 3.6 Ethical Considerations | 39 |
| CHAPTER FOUR: ANALYSIS AND FINDINGS | 41 |
| 4.1 Introduction | 41 |
| 4.2 Attack Methodology: A Review of the Colonial Pipeline Ransomware Attack | 41 |
| 4.3 Evaluation of the effectiveness of current mitigation strategies against ransomware attacks | 45 |
| 4.4 Identifying gaps and limitations in the existing detection and mitigation frameworks | 49 |

| | |
|--|-----------|
| 4.5 Mitigation Techniques in Ransomware Attacks: Colonia Pipeline | 53 |
| 4.6 Proposed Detection and Mitigation Framework | 56 |
| 4.7 Summary | 64 |
| CHAPTER FIVE: SUMMARY CONCLUSION, RECOMMENDATION AND SUGGESTION FOR FURTHER STUDIES | 65 |

LIST OF TABLES

| | |
|---|----|
| Table 1: Inclusion and Exclusion Criteria | 37 |
| Table 2: Thematic analysis of the evaluation of the effectiveness of current mitigation strategies against ransomware attacks..... | 48 |
| Table 3: Thematic analysis to identify gaps and limitations in existing detection and mitigation frameworks for insider threats | 52 |

CHAPTER ONE: INTRODUCTION

1.1 Background to the Study

Methods of cyber extortion have existed since the 1980s. The PC Cyborg Trojan was the earliest ransomware example, dating back to 1989 (Tailor, Patel 2017). PC Cyborg masked folders and encrypted the names of all files on the C drive after restarting the target machine 90 times, making the system inoperable. Ransomware attacks were largely carried out in the 1990s and early 2000s by amateur hackers looking to acquire a reputation via cyber pranks and destruction (Srinivasan 2017). Around 2005, modern ransomware arose and rapidly became a viable commercial tactic for attackers (Wilner et al. 2019). To get greater ransoms, targets switched from people to businesses and organizations (et al. 2019). Transportation, healthcare, financial sectors, and government were specifically targeted (Alshaikh et al. 2020).

Ransomware has emerged as one of the most severe computer threats, and the number of threats confronting corporations, public sectors, industries, and IoT devices has grown dramatically in recent years (Yaqoob et al., 2017; Faghihi & Zulkernine, 2021). Even though ransomware has been around for over 30 years, its first impacts were low, impacting only a small number of people, and the recovery procedure was straightforward (Salvi & Kerkar, 2017). However, as IoT has matured, ransomware assaults have grown dramatically, peaking around 2012 (Humayun et al., 2021). In 2019, at least 966 government, educational, and healthcare organizations were hit by ransomware attacks, costing the US economy an estimated \$7.5 billion (Emsisoft Malware Lab, 2019). These attacks have sometimes endangered lives by interfering with emergency services or redirecting patients to other hospitals (Reilly, 2019). Ransomware attacks are estimated to inflict more than \$200 billion in damage by 2021 (Humayun et al., 2021). As a result of widely accessible ransomware toolkits and ransomware-as-a-service (RaaS)

that enable amateurs to launch ransomware assaults, the number of ransomware attacks has increased tremendously (Sharmeen et al. 2020).

Ransomware attacks may inflict considerable financial damage, lower productivity, interrupt routine business processes, and ruin people's or firms' reputations (Jain, Rani 2020). According to the findings of the global survey 'The State of Ransomware 2021' commissioned by Sophos, the average total cost to an organization to rectify the impacts of a ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, etc.) was US\$1.85 million, which is more than double the US\$761,106 cost reported in 2020 (ran, 2021). These assaults may potentially result in irreversible data or file loss. Paying the ransom does not ensure the release of the locked machine or data (for Cyber Security, 2018). The cost of recovering from an assault doubles on average for organizations that pay the ransom (Ltd. 2020). Ransomware attacks are estimated to cost the globe \$20 billion by the end of 2021, up from \$325 million in 2015 (Alshaikh et al. 2020). Since the COVID-19 epidemic, these assaults have been extremely damaging, beginning with hospitals, vaccine research facilities, and contact tracking applications (Pranggono, Arabo 2021). All of these figures indicate that we need to better understand the behaviour of ransomware and its variations to prevent and mitigate future attacks. Ransomware variations that avoid regular antivirus software and other detection measures continue to evolve as a result of their profitability. As a result, it is important to develop a new generation of effective countermeasures (Beaman et al. 2021).

Almost all firms have difficulty detecting ransomware (Thomas & Gallagher, 2018; Brewer, 2016). Attackers with access to storage devices encrypt system data and make systems inoperable (Brewer, 2016). Since its inception, ransomware attacks have grown in complexity and severity, with more recent versions encrypting user data employing a combination of symmetric and

asymmetric encryption (Davies et al., 2020). Such attacks have major consequences, such as businesses ceasing operations, consumers losing access to services, and reputations being harmed (Thomas et al., 2019). Security experts and ransomware developers are always engaged in an "arms race" to safeguard their digital infrastructure from such attacks.

1.2 Problem Statement

Ransomware has rapidly become one of the most significant cybersecurity threats, causing extensive financial and operational harm to individuals, businesses, and governments globally. Traditional cybersecurity measures have proven insufficient against the evolving sophistication of ransomware attacks, underscoring the urgent need for more advanced detection and mitigation strategies. The Cybersecurity and Infrastructure Security Agency (CISA, 2020) reports a troubling increase in ransomware incidents, leading to severe downtime, data loss, and considerable recovery costs. The disruption caused by these attacks, which often involve encrypting critical data and demanding ransom payments, poses significant risks to essential infrastructure and services, with profound economic and societal implications.

The sophistication of modern ransomware variants, which utilise advanced techniques such as obfuscation, polymorphism, and zero-day vulnerabilities, has increased the difficulty of detection and neutralisation. Attackers often employ social engineering and phishing campaigns, ensuring their malicious payloads evade conventional antivirus solutions (Kharraz et al., 2015). This increasing complexity necessitates innovative approaches to ransomware detection and mitigation. Furthermore, the legal and ethical challenges of responding to ransomware are substantial. The dilemma of whether to pay the ransom, often in violation of regulatory guidelines and ethical standards, is exacerbated by the pressure to resume operations quickly. The absence of

standardised protocols and the complex legal pattern further complicate effective ransomware management (Martin et al., 2018).

A review of the literature reveals several frameworks and methodologies proposed to address ransomware threats. Kapoor et al. (2021) introduced the Detection Avoidance Mitigation (DAM) framework, which offers a consolidated approach to detecting, avoiding, and mitigating ransomware. Similarly, Oz et al. (2022) emphasised the need for a comprehensive understanding of ransomware families and defence mechanisms, while Kang and Gu (2023) focused on contrasting static and dynamic analysis methods for threat detection. Despite these advancements, there remains a significant gap in research that fully integrates the technical, legal, and ethical dimensions of ransomware mitigation, highlighting the need for empirical studies to assess the real-world efficacy of current anti-ransomware tools and methodologies.

1.3 Aim and Objectives

This research aims to develop a comprehensive and measurable framework for mitigating ransomware attacks by proposing innovative detection and defence strategies, thereby filling existing knowledge gaps and providing actionable solutions for cybersecurity practitioners. Based on the aim of this dissertation, the specific objectives are to:

1. comprehensively assess existing ransomware literature within the next three months, focusing on the analysis of recent ransomware attacks, their patterns, delivery mechanisms, and attack procedures.
2. critically evaluate and measure the effectiveness of current detection techniques for ransomware in modern computing environments.
3. assess the effectiveness of current mitigation strategies against ransomware attacks, identifying specific strengths and weaknesses.

4. identify and recommend at least three potential new methods for mitigating ransomware, based on gaps identified in existing strategies.
5. propose a framework for detection and mitigation of ransomware attack based on the limitations of existing detection and mitigation methods.

1.4 Significance of the Study

The significance of this study lies in its potential to make a substantial contribution to the field of cybersecurity by enhancing the understanding and mitigation of ransomware attacks. The research addresses a critical and timely issue, given the escalating frequency and severity of ransomware incidents affecting various sectors globally. First and foremost, this study aims to provide a comprehensive assessment of the current state of ransomware. By systematically reviewing existing literature, it will offer an integrated perspective on ransomware trends, delivery methods, and the general processes involved in such attacks. This overall understanding is essential for identifying patterns and developing targeted strategies to combat ransomware.

Secondly, the study is significant in its practical implications for cybersecurity practices. By evaluating the effectiveness of different anti-ransomware tools and techniques, this research will provide valuable insights for cybersecurity professionals and organizations. The findings can inform the development and implementation of stronger defence mechanisms, enhancing organizational resilience against ransomware threats. Moreover, the research addresses the critical need for empirical evidence in ransomware mitigation. By conducting focused experiments and comparing the performance of various detection tools, the study will contribute to the evidence base on effective ransomware defences. This empirical approach helps bridge the gap between theoretical knowledge and practical application, ensuring that the recommendations are grounded in real-world scenarios.

Additionally, the study acknowledges the importance of ethical and legal considerations in ransomware response strategies. By exploring these dimensions, it aims to provide a balanced perspective that considers not only technical solutions but also the ethical and legal implications of different mitigation approaches. This overview is crucial for developing comprehensive and sustainable ransomware response strategies. Ultimately, the significance of this study extends to its potential impact on policy and practice. The insights gained from this research can inform policymakers, helping to shape regulations and guidelines that support effective ransomware mitigation. By contributing to a safer and more secure digital environment, this study addresses a pressing need in the field of cybersecurity.

1.5 PSEL Issues

Ransomware, a pervasive cybersecurity threat, presents numerous professional, social, ethical, and legal challenges that must be addressed to safeguard digital infrastructures effectively.

Professional issues: revolve around the integrity of cybersecurity practices, where adherence to rigorous methodologies is crucial for accurate detection and mitigation strategies. Researchers are obligated to follow established protocols, ensuring data is handled transparently and securely, while maintaining neutrality to minimise biases that could compromise the validity of their work (Hudson, 2020; Ghazinoory et al., 2014). The importance of proper licensing and privacy protection is emphasised, as the ethical management of sensitive data is paramount (Williams, 2018).

Social Issues: the social implications of ransomware research are significant, particularly concerning the protection of individuals' rights and societal norms. Researchers must ensure that their work aligns with community values and mitigates any potential negative impacts, prioritising inclusivity and justice in their studies (Elliott et al., 2018; Hudson, 2020).

Ethical Issue: ethical considerations, especially the principles of autonomy, beneficence, and justice, are critical when involving human participants. Informed consent and the fair distribution of research benefits are essential to maintaining ethical integrity (Beauchamp & Childress, 2019; Resnik, 2015).

Legal Issues: This complicates the pattern further, as strict adherence to intellectual property laws, data protection regulations such as the GDPR, and institutional ethical guidelines is crucial (Regulation (EU) 2016/679; U.S. Department of Health & Human Services). Researchers must obtain ethical approvals and ensure compliance with relevant legal frameworks to avoid potential legal consequences (Hudson, 2020)..

1.6 Structure of Dissertation

This dissertation is broken down into 5 chapters. This chapter which is the first chapter is the introduction of the dissertation which provides the background to the dissertation.

Chapter 2 provides a comprehensive overview of existing literature relevant to ransomware investigation and mitigation. It critically examines various perspectives and methodologies presented in previous research and identifies key themes and gaps in the literature. The review focuses on understanding how ransomware is delivered, the forensic procedures used in investigations, and the strategies employed for mitigation. By synthesizing and analyzing these studies, this chapter helps to contextualize the study within the broader field of cybersecurity.

Chapter 3 outlines the research design and methodology used in this dissertation. Given the qualitative nature of the study, this chapter details the selection of secondary data through an extensive literature review and explains the rationale behind choosing thematic analysis as the method for data analysis. It also discusses the inclusion and exclusion criteria applied to ensure the relevance and quality of the data. Additionally, the chapter

addresses ethical considerations related to the research, ensuring that the study adheres to the highest standards of academic integrity and ethical practice.

This chapter 4 presents the key findings from the thematic analysis conducted on the selected literature. The chapter is organized according to the themes identified during the analysis, with each theme being discussed about the research questions. The discussion integrates these findings with existing literature, highlighting how the results contribute to the current understanding of ransomware investigation and mitigation. The chapter also explores the implications of the findings for both theory and practice, offering insights that could inform future research and practical applications in cybersecurity.

chapter 5 of the dissertation summarizes the key findings and conclusions drawn from the research. It reflects on the research objectives and questions, discussing how they have been addressed through the study. Additionally, this chapter offers recommendations for future research and practical strategies for improving ransomware investigation and mitigation efforts. It also acknowledges the limitations of the study, suggesting areas where further investigation is needed to build on the findings presented in this dissertation. This chapter serves as a closing reflection on the research process and its contributions to the field of cybersecurity.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

Ransomware attacks have become a significant cybersecurity threat, posing severe risks to individuals, businesses, and governments (Kharraz et al., 2015). These malicious programs encrypt data or block access to computer systems while demanding payment from victims. Understanding ransomware requires exploring its fundamental mechanics, attack vectors, and potential defences. Research has focused on identifying ransomware through various methods, including network forensics, static and dynamic malware analysis, and the examination of artefacts like ransom notes and Bitcoin transactions (Gupta et al., 2017; Abrams et al., 2020).

Detection of ransomware is crucial to mitigate data loss and financial damage. Effective detection methods include signature-based techniques, which use known patterns to identify threats (Scaife et al., 2016); behaviour-based approaches, which monitor for suspicious activities mimicking ransomware behaviour (Pawar et al., 2020); and machine learning methods, such as anomaly detection and classification algorithms (Buczak & Guven, 2016).

The literature presents diverse perspectives on ransomware, reflecting varying definitions that encompass extortion, encryption, access denial, data theft, and exposure (Kharraz et al., 2018; Christin, 2017). These differing views underscore the complexity of addressing ransomware threats.

2.2 Definition of Ransomware

Ransomware, a type of malicious software, poses a significant threat by encrypting victims' data and demanding a ransom for decryption. This form of cyber extortion has become increasingly prevalent and sophisticated, as highlighted by various researchers. According to Yaqoob et al. (2017), ransomware attacks typically demand payment in Bitcoin, a claim

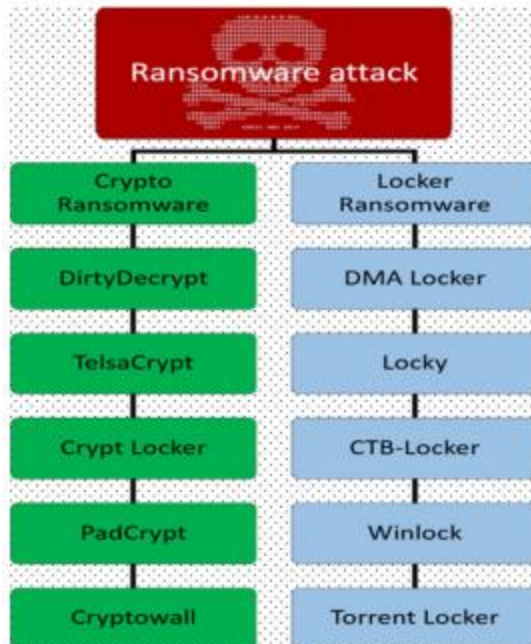
corroborated by Sophos (2019), which notes the growing prevalence and danger of these assaults to internet users. The broader category of malware, which includes viruses, worms, rootkits, botnets, and Trojan horses, also encompasses ransomware (Grégio et al., 2015). Ransomware specifically targets both individuals and organisations globally, with its primary function being to block access to an infected system until a ransom is paid (US-CERT, 2016). The more dangerous variant, crypto-ransomware, employs sophisticated encryption algorithms to lock users out of their data, often appending a new file extension to encrypted files (Dubey, 2016). Victims are typically informed of the attack through a notification that provides instructions on how to pay the ransom and retrieve their data (Trend Micro, n.d.). Although several types of ransomware exist, this paper will focus on crypto-ransomware, which, as Steinberg (2018) notes, is the most prevalent and destructive form.

The role of encryption is central to most definitions of ransomware. Ritter et al. (2017) describe ransomware as software that encrypts data and demands a ransom for decryption, with the primary objective being extortion through encryption. However, Christin (2017) expands this definition by including not only file encryption but also the restriction of access to entire computer systems, emphasising the psychological pressure exerted on victims to pay the ransom. These differing perspectives illustrate the dual nature of ransomware as both a threat to data encryption and a method of coercive denial of access. Social engineering techniques play a crucial role in ransomware attacks, as noted by Pawar et al. (2020), who highlight the deceptive strategies employed to trick users into triggering the malicious payload. This aspect underscores the manipulative nature of ransomware and its exploitation of human vulnerabilities. Kharraz et al. (2018) further discuss the difficulty in distinguishing ransomware from other forms of malware, such as wipers or spyware, which may exhibit similar behaviours but differ in intent.

The unique characteristic of ransomware, according to these scholars, is its explicit goal of extorting a ransom from the victim, making intent a key factor in its definition.

Reaves et al. (2016) argue for a more inclusive definition of ransomware that accounts for its evolving nature, particularly the potential for data theft or disclosure in addition to file encryption. This broader definition recognises the additional risks posed by modern ransomware variants, such as data exfiltration. The complexities and variations in ransomware definitions are further explored by Gröndahl et al. (2020), who identify inconsistencies across sources, leading to confusion and communication gaps in cybersecurity. This highlights the need for a consensus on the terminology and scope of ransomware to facilitate effective collaboration in the field. To refine the definition of ransomware, Morato et al. (2018) categorise the behaviour of different ransomware types, distinguishing between lock-screen ransomware, which merely prevents access to the computer, and encryption ransomware, which blocks access to data. Some ransomware variants, termed wipers, permanently deny access to files even after the ransom is paid (O'Brien, 2017). The rise of Ransomware-as-a-Service (RaaS), as noted by Petrasko (2017), has further increased the complexity, with platforms like Cerber and Atom allowing affiliates to launch attacks with minimal technical expertise. This development has likely contributed to the increased frequency of ransomware attacks, as observed by Thomas et al. (2019).

Figure 1: Taxonomy of Ransomware attack



Source: Humayun et al. (2021)

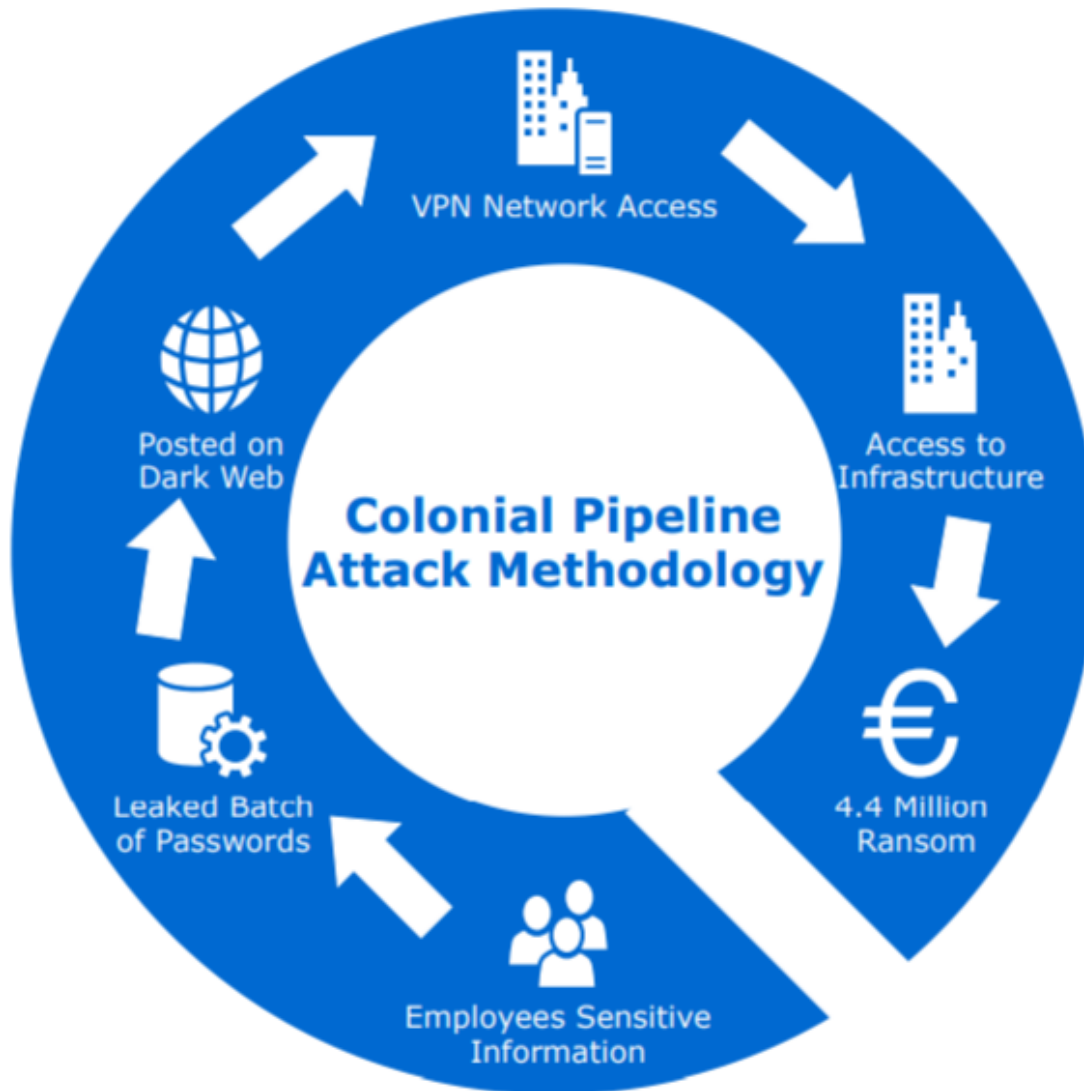
Over the last several years, ransomware has become more dangerous. According to the Federal Bureau of Investigation (FBI), in 2015, there was a rise in ransomware attacks on organisations that law enforcement saw (FBI, 2016). According to Check Point, in the second half of 2016, ransomware assaults accounted for 10.5% of all malware attacks globally (Check Point, 2017a, 2017b). Research indicates that ransomware increases businesses' risk (Schulze, 2017; O'Brien, 2017). Due to a lack of backups and ransomware detection technologies, an organisation may sometimes be left with no choice but to pay the ransom (Palmer, 2017).

4.3 Overview of Colonial Pipeline Ransomware Attack

In April 2021, Colonial Pipeline Co., the largest oil pipeline company in the United States, fell victim to a significant ransomware attack orchestrated by the hacking group DarkSide. The attack, which occurred on April 29, 2021, exploited vulnerabilities within the company's network, resulting in severe disruptions to the nation's fuel supply and prompting discussions on the

cybersecurity of critical infrastructure. The Colonial Pipeline System is responsible for transporting over 2.7 million barrels of fuel daily, making it a vital asset for the United States, particularly for the Eastern states, where the impact of the attack was most keenly felt (Medlock III, 2021). The attackers infiltrated Colonial Pipeline's network through an old, inactive account linked to a virtual private network (VPN) as can be seen in Fig. 2. This account did not have multi-factor authentication (MFA) enabled, allowing the hackers to gain unrestricted access to the entire network using only the compromised credentials (Turton and Mehrotra, 2021). The exact method by which the hackers obtained the account password remains unclear. Possibilities include human blackmail, the reuse of an old password, or even a successful password guess, but the lack of MFA was a critical failure that facilitated the breach (Beerman et al., 2023). Once inside, the attackers were able to deploy ransomware, encrypting crucial data and demanding a ransom payment to restore access.

Figure 2: Taxonomy of Ransomware attack

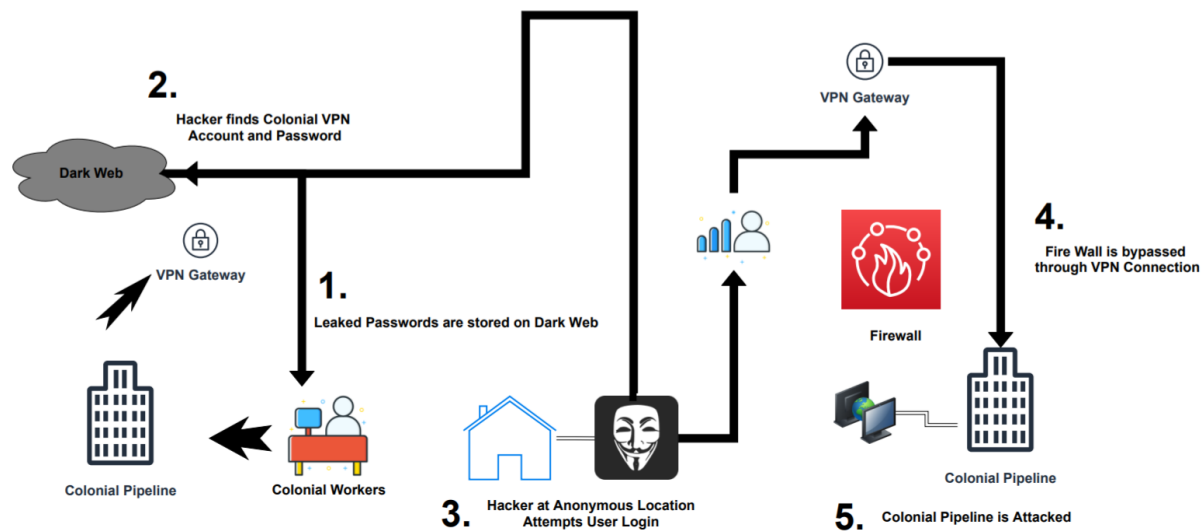


On May 7, 2021, about a week after the initial breach, Colonial Pipeline Co. received a ransom demand of \$4.4 million in cryptocurrency. This demand was communicated to an employee, who promptly reported the situation to his supervisors. The company made the controversial decision to pay the ransom, a choice that drew widespread criticism from cybersecurity experts. Despite the payment, the pipeline remained shut down for several days as the company worked to determine how the attack occurred and how to prevent future breaches (Beerman et al., 2023). The attack highlighted significant weaknesses in the cybersecurity measures of critical infrastructure. Despite

the rapid response, the shutdown of the Colonial Pipeline caused widespread fuel shortages along the East Coast, leading to panic buying and long queues at petrol stations. The disruption in fuel supply not only underscored the importance of the Colonial Pipeline to the U.S. economy but also demonstrated the broader risks posed by inadequate cybersecurity in essential services (Stephens, 2021).

Further investigation into the attack revealed that the compromised VPN account had no multi-factor authentication (MFA) enabled, a critical oversight that allowed the attackers unfettered access to the network. This breach brought to light the necessity for rigorous cybersecurity measures, particularly for systems classified as critical infrastructure. The absence of MFA, combined with the existence of an old, unused account linked to a critical system, underscores the need for constant vigilance and the implementation of robust security protocols (Beerman et al., 2023). In response to the attack, Colonial Pipeline implemented several security enhancements, including the installation of alarms within its network. These alarms are designed to notify the company if any unauthorized access occurs in the future, thereby preventing hackers from moving freely within the network. This measure, although reactive, represents a crucial step toward strengthening the security of the pipeline's operations (Beerman et al., 2023). Figure 3 illustrates the process of access to the Colonial Pipeline infrastructure and highlights the points at which security failures occurred.

Figure 3: Process of Access to Colonial Pipeline Infrastructure



Moreover, the attack spurred a broader discussion on the role of government in protecting critical infrastructure. The Colonial Pipeline, categorised as "Critical Infrastructure vulnerable to attack," demonstrated how such an asset's compromise could have far-reaching consequences, including economic disruptions and threats to national security. The incident has prompted calls for increased government involvement in cybersecurity, particularly through agencies like the Cybersecurity and Infrastructure Security Agency (CISA), which has proposed legislation to enhance its role in defending critical infrastructure. These proposals include making CISA's approach more team-oriented and establishing a Cyber Safety Review Board to document and review lessons learned from cybersecurity incidents (Smith and Monken, 2021).

The ransomware attack on Colonial Pipeline serves as a stark reminder of the vulnerabilities that exist within critical infrastructure and the urgent need for comprehensive cybersecurity measures. As demonstrated by the fuel shortages and economic disruption that followed the attack, the stakes are incredibly high. The lessons learned from this incident must inform future strategies to protect essential services from similar threats. Ensuring that all critical infrastructure systems are protected with up-to-date security

measures, including MFA, and conducting regular reviews of system access protocols are essential steps in mitigating the risk of future ransomware attacks (Voas et al., 2021). The importance of securing critical infrastructure cannot be overstated, especially as the digital and physical realms continue to converge. The Colonial Pipeline attack has shown that the consequences of neglecting cybersecurity in such vital systems can be severe, affecting not only the operations of the targeted company but also the wider economy and national security. As the world becomes increasingly reliant on digital infrastructure, the need for robust and proactive cybersecurity measures will only grow more critical. Future incidents must be prevented by learning from past mistakes and implementing the necessary changes to protect against the ever-evolving threat pattern (Parfomak and Jaikaran, 2021).

2.4 Taxonomy of Ransomware

Ransomware is classed in many ways. As shown in Figure 3, we categorise ransomware based on its target and infection technique in this research. In this part, we first present a summary of each categorization category before classifying the most significant ransomware families using our technique.

2.4.1 Classification by Target

Ransomware may be categorised according to its objectives into two orthogonal categories: target victim and target platform.

Ransomware Victims: Ransomware may target a wide range of victims. Analysing the characteristics of ransomware victims might give useful information for developing realistic defense methods. End-users and organisations are the two types of ransomware victims.

End-users: The main targets of the earliest ransomware families were end-users. Ransomware is particularly successful against end users because to a lack of security knowledge and technical help (Kevin Savage et al. 2015).

Cryptographic ransomware may encrypt people's data that are kept on personal devices (e.g., PCs, laptops, cellphones, and so on). In the meantime, locker variations may lock end-user devices and block access until a ransom is paid. Unsurprisingly, the quantity requested by end-users is substantially smaller than the amount demanded by organisational objectives (Kevin Savage et al. 2015). Furthermore, a single ransomware infection may infect thousands of end-user computers, making it lucrative (Atapour-Abarghouei et al. 2019).

Organisation: Initially, organisations were not the primary targets of ransomware. However, as ransomware developed over time, many other sorts of organisations, including governments, hospitals, businesses, and schools, were routinely attacked. In these assaults, hackers pre-select their targets and aim to create maximum disruption in the expectation of receiving a large ransom payment (Jercich 2020). Locker ransomware may lock computers utilised in the target, potentially halting the whole operation (WIRED 2018). Similarly, cryptographic ransomware may encrypt important data stored in an organization's system and render it unavailable until a large ransom is paid. Cybercriminals may also threaten to make public their target's info.

Ransomware Target Platforms: Another important consideration in understanding ransomware behaviour is the target platform. Ransomware attacks a wide range of platforms. It is usually tailored to a single platform and operating system since it often makes use of system-specific libraries/functions (i.e., system calls) to carry out its malicious acts (Kevin Savage et al. 2015). In this research, we will use the words platform and operating system interchangeably, and we will categorise ransomware target platforms into three groups: PCs/workstations, mobile devices, and IoT/CPS devices are all examples of IoT/CPS devices.

PCs/workstations: PCs and workstations are the most typical targets for ransomware. Because of their ubiquity among consumers, the bulk of ransomware attacks PCs and workstations running Windows. Furthermore, several ransomware families, such as KeRanger for macOS and LinuxEncoder for GNU/Linux platforms, target different operating systems. Screen locker ransomware attacks may be mitigated by reinstalling the operating system. However, because of the use of modern encryption methods, it is almost hard to decode and retrieve data from cryptographic ransomware (Tang et al. 2020; Taylor 2023). As a result, cryptographic ransomware families are the most common threats to PCs/workstations.

Mobile Devices: Because of their rising prominence in society, mobile devices such as smartphones are good targets for ransomware. In terms of mobile devices, ransomware targets the Android and iOS platforms, which share the largest worldwide mobile OS market. Apple has a tightly regulated environment in which apps are extensively reviewed before being made available to users. This is most likely why iOS users have not been impacted by malware. There have only been incidents of phony ransomware for iOS devices (BBC 2017b). On the contrary, ransomware poses a danger to Android consumers owing to the open ecosystem of the Android platform. In reality, the first locker ransomware for mobile devices, Android Defender, appeared in 2013, targeting Android platforms, and the first cryptographic ransomware, Simplocker, appeared the following year (Lipovsk et al. 2015). Although cryptographic ransomware is more dangerous than locker variations on PCs/workstations, the converse is true for mobile ransomware. The fundamental rationale is that the impact of locker ransomware on PCs/workstations can be prevented most of the time by removing the hard drive, however, the same method is difficult for mobile devices (Snow 2016).

IoT/CPS Devices: At present, IoT and CPS devices are not the primary targets of ransomware outbreaks. However, such devices are becoming more

common in a variety of deployment areas, including but not limited to smart homes, smart health, smart buildings, smart transportation, smart cities, smart manufacturing, and so on (Rondon et al. 2022). Indeed, Industrial IoT and CPS devices (e.g., PLCs, RTUs, RIOs, and so on) have already been powering industrial control systems in smart grids, water and gas pipelines, and nuclear and chemical facilities. Although ransomware for such systems is not widely used at the moment, attackers may target such settings more often in the future (Dickson 2016).

2.4.2 Classification by Infection Vectors

To infect their targets, ransomware writers utilise the same infection mechanisms as ordinary malware. Malicious e-mails, SMS or instant messaging (IMs), malicious programmes, drive-by-download, and vulnerabilities are the five types of ransomware infection tactics.

Malicious e-mails are the most typical ransomware infection vectors. Attackers send spam e-mails to victims with ransomware attachments (Sevtsov. 2017). Botnets may be used to spread such spam campaigns (Kurt et al. 2020). Ransomware may arrive with an attached malicious file, or the e-mail may include a malicious link that, when clicked, may install ransomware (drive-by download).

SMS Messages or IMs: SMS messages or instant messages are regularly utilised for mobile ransomware. In such cases, attackers send SMS messages or instant messaging to victims, instructing them to visit a rogue website and download ransomware onto their devices. Malicious Applications are employed by ransomware attackers who create and distribute mobile applications containing malware disguised as benign applications (Lipovsk et al. 2015).

Drive-by download: Drive-by download occurs when a person visits an infected website or clicks on malicious advertising (i.e., malvertisement), and

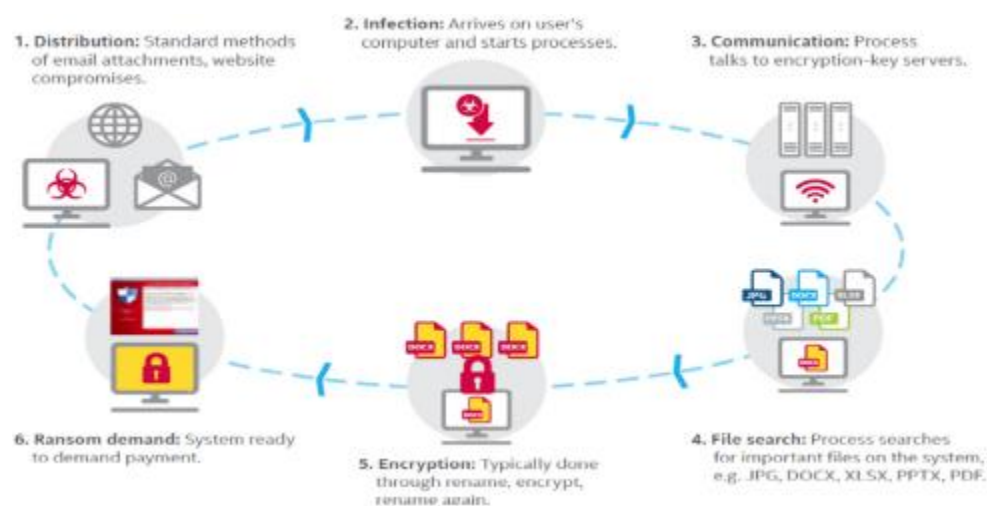
the malware is downloaded and installed without the user's awareness (Reuters Staff 2017).

Vulnerabilities: flaws in the victim platform, such as weaknesses in operating systems, browsers, or software, may be utilised as infection vectors by ransomware developers (BBC 2017a). Attackers may utilise exploit kits, or aid apps, to exploit known or zero-day vulnerabilities in target systems. Malvertisement and malicious links may be used by attackers to lead users to such kits.

2.6 Ransomware infection path

Wang and Wang (2015) claim that while exploiting a system's vulnerabilities, ransomware uses the same strategy as conventional malware. For instance, hacked websites or email attachments are used as attack vectors to infect a victim's machine. Many different organisations have put forth models that try to explain how ransomware behaves. According to several of them (Al-rimy, Maarof, and Shaid 2018), a ransomware assault may be classified into six different stages. The model shown in Figure 3 by McAfee (McAfee Labs 2016) is an illustration of such a concept.

Figure 4: McAfee 6 Phase Ransomware Model



(McAfee Labs, 2016)

Distribution: This stage involves delivering the malicious code to the victim's machine and packaging the ransomware. To make the distribution easier, a variety of exploitation tactics are used, including drive-by downloads, phishing assaults, spam mail campaigns, social engineering, and penetration (Davies, Macfarlane, and Buchanan 2020).

Infection: This stage focuses on how the ransomware operates and behaves at first. The malware investigates the operating environment at this phase and gathers data on the victim's device, including the platform type, OS version, and installed programmes (Prakash, Nafis, and Biswas 2017).

Communication: The ransomware pulls the encryption keys from the command and control (C&C) server at this stage. In order to provide the execution modules and encryption keys needed at a later stage of the infection, the attacker controls this remote computer. Not every ransomware performs this function since some variants already include the keys in their payload (Sgandurra et al. 2016). During this stage, some ransomware will attempt to switch to other computers on the network (Sophos, 2019).

File Search: The ransomware now begins searching for specific resources, such user files, resources, and accessibility features. Typically, file extensions are used to select files (Sultan et al., 2018).

Encryption: Depending on the family type, different ransomware hijacks and encrypts the targeted resources, with some (such as Petya) discarding the encryption key and others (such as Wannacry, NotPetya) communicating it back to the attacker through C&C server or ransom message. Hybrid key crypto-ransomware (HCR), which uses a variety of encryption algorithms to improve speed, makes up the majority of contemporary ransomware. During this stage, files may be moved, renamed, or corrupted, and the MBR may also be encrypted. If ransomware executes secretly, a computer reboot could

happen, which might be the first time a user notices the existence of ransomware (Davies, Macfarlane, and Buchanan 2020).

Ransom demand: After the encryption process is finished, the victim sees a message with payment instructions that demands a ransom. Although paying the ransom increases the likelihood of data recovery, it does not ensure that a decryption key will be sent (Richardson and North 2017).

4.2 Detecting ransomware

This analysis seeks to critically review and assess the efficacy of existing ransomware detection techniques, ranging from traditional signature-based methods to more sophisticated machine learning, network-based, and hybrid approaches. By evaluating these techniques within the context of contemporary cybersecurity challenges, this analysis aims to highlight the strengths, limitations, and potential areas for improvement in ransomware detection strategies.

1. Traditional Detection Techniques

Traditional ransomware detection techniques primarily rely on signature-based methods and heuristic analysis. Signature-based detection, as discussed by Bradley (2016) and Furnell & Emm (2017), involves identifying known ransomware strains based on predefined signatures or patterns. While effective against known threats, this approach struggles with new or modified variants. Jain & Rani (2020) highlight the limitations of signature-based detection in the context of evolving ransomware payloads, emphasizing the need for more adaptive methods. Singh et al. (2020) further critique traditional methods, arguing that while heuristic analysis can detect anomalies, it often results in higher false-positive rates due to its reliance on heuristic rules and behavioural patterns.

2. Machine Learning and Deep Learning Approaches

Recent advancements in machine learning (ML) and deep learning have significantly enhanced ransomware detection capabilities. Alamosa et al. (2021) and Hammadeh & Kavitha (2023) focus on the application of ML algorithms for detecting ransomware by analyzing network traffic and system behaviours. These approaches leverage supervised learning to improve accuracy over traditional methods by learning from large datasets of known threats. Zhao et al. (2021) and Wang et al. (2022) advance this further with deep learning frameworks, demonstrating that deep neural networks can achieve high detection rates for new ransomware variants by identifying complex patterns that are often missed by simpler models. These techniques address the shortcomings of traditional methods but require substantial computational resources and training data.

3. Network-Based Detection Methods

Network-based detection methods have gained prominence due to their ability to analyze traffic patterns and detect anomalous behaviours indicative of ransomware activities. Akbanov et al. (2019a) and Cabaj & Mazurczyk (2016) discuss how software-defined networking and traffic analysis can be utilized to identify ransomware communications and data exfiltration attempts. Homayoun et al. (2020) explore the use of frequent pattern mining in network traffic for threat hunting, which allows for the detection of unusual patterns associated with ransomware operations. These methods provide an additional layer of detection by monitoring network behaviour but may face challenges related to privacy concerns and the need for constant traffic analysis.

4. Hybrid Approaches

Hybrid detection methods combine multiple techniques to enhance detection accuracy and reduce false positives. Kang & Gu (2023a, 2023b) and Kapoor et al. (2021) advocate for combining signature-based, heuristic, and machine-learning approaches to leverage the strengths of each method. Wang et al.

(2023) also highlight the effectiveness of hybrid approaches by integrating traditional and advanced techniques to achieve a comprehensive detection system. These methods aim to balance the strengths of various techniques, providing strong protection against both known and novel ransomware threats. However, they can be complex to implement and may require significant computational resources.

5. Forensic and Post-Attack Analysis

Forensic analysis and post-attack strategies are crucial for understanding ransomware attacks and improving future detection. Boyton et al. (2020) and Davies et al. (2020) focus on forensic techniques to investigate ransomware activities, offering insights into attack vectors and encryption methods used by ransomware. Mercaldo et al. (2016) discuss the importance of analyzing ransomware characteristics to improve detection and prevention strategies. Post-attack analysis not only aids in recovery but also helps refine existing detection methods by incorporating lessons learned from actual attacks.

2.10 Ransomware Mitigation Techniques

Since the advent of ransomware, cyber-defenders have strived to create sophisticated security measures to counteract its various strains. However, the persistence of ransomware creators in exploiting new vulnerabilities, often capitalising on the general public's lack of cybersecurity awareness, has allowed ransomware to continue wreaking havoc. The primary focus of mitigation efforts has been on recovering encrypted data through reverse engineering or preventing the ransomware from completing the encryption process. Nonetheless, these strategies have often proven ineffective in practice, with most victims either paying the ransom or permanently losing their data (Kapoor et al., 2021). Despite these challenges, several promising mitigation techniques have emerged, offering potential pathways for the removal of ransomware and the recovery of affected devices.

One such approach involves software-defined networking (SDN) as proposed by Cabaj and Mazurczyk (2016), which was initially used to decrypt CryptoWall ransomware. This method, however, proved versatile against other variants as well. The approach centred on dynamic blacklisting of command and control (C&C) servers during the sample's execution. Without access to the C&C server, the infected system could not obtain the public key required for encryption. Although effective, this technique was limited by its inability to detect servers that had not been previously identified as C&C servers. Two SDN-based programmes, SDN1 and SDN2, were developed to enhance this mitigation strategy. SDN1 focused on analysing DNS responses to determine whether the domain was already listed in a database of unauthorised proxies, while SDN2 extended this functionality by restructuring the entire network architecture to block ransomware activity using the OpenFlow protocol.

Another significant mitigation strategy involves reverse engineering, as demonstrated by Zimba et al. (2018). This method aimed to uncover the operational mechanisms within various ransomware strains. By employing reverse engineering, the researchers identified features related to data destruction and recovery embedded in the ransomware's source code. The process included multiple scans, such as virus scans, obfuscation checks, and meta-data extraction, which enabled the discovery of distinct ransomware characteristics. Furthermore, they utilised sandboxing to observe the ransomware's behaviour in controlled environments. Interestingly, they found that attackers frequently failed to employ secure file deletion methods, allowing the researchers to recover data, particularly by leveraging timely offline backups of volume shadow copies (Hathaliya and Tanwar, 2020).

Baykara and Sekin (2018) introduced the Safe Zone application, which compresses all user files into a single file, effectively safeguarding them from external alterations. This application continuously updated the Safe Zone file, while a logging tool, File Watcher, monitored changes to parent folders and

activities within the Safe Zone. Additionally, the programme included a feature to check the integrity of the Safe Zone file. In the event of a ransomware attack, this system allowed users, even those with limited technical knowledge, to restore their systems to the most recent backup state securely.

2.11 Summary

Ransomware has evolved from a rudimentary form of malware to a sophisticated cybercrime that poses a significant threat to individuals and organizations worldwide. Its ability to rapidly mutate, coupled with the increasing sophistication of attack techniques, underscores the dynamic nature of this challenge. The proliferation of ransomware-as-a-service (RaaS) has further exacerbated the issue, making it accessible to a wider range of cybercriminals.

While various detection methods, including signature-based, heuristic-based, and machine learning approaches, have been developed, the polymorphic nature of ransomware and the emergence of new attack variants continue to pose challenges. Traditional detection methods often struggle to keep pace with the evolving threat pattern. Moreover, the scarcity of data during the early stages of an attack hampers the development of effective early warning systems.

Mitigation strategies have focused primarily on data recovery and prevention of encryption completion. However, the effectiveness of these approaches has been limited due to the rapid evolution of ransomware. While software-defined networking has shown promise in certain cases, a comprehensive and strong mitigation strategy is still under development.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

The Research Methodology chapter outlines the comprehensive approach and techniques employed to conduct the study on how ransomware is investigated and mitigated. This chapter aims to provide a detailed description of the research design, data collection methods, data analysis techniques, and ethical considerations. By ensuring that the research process is transparent, replicable, and rigorously conducted, this chapter underpins the entire research, making it strong and credible. The primary focus of this chapter is to delineate the qualitative approach, systematic literature review as a data collection method, and thematic analysis used to interpret the data.

3.2 Research Design

The research design chosen for this study is qualitative, which is particularly suitable for exploring complex phenomena like ransomware. Qualitative research allows for an in-depth understanding of the intricate and multifaceted nature of ransomware threats, their investigation, and mitigation strategies. According to Creswell (2013), qualitative research is ideal for capturing the richness of the experiences, perceptions, and practices of individuals and organizations dealing with ransomware incidents.

The research is structured as a literature review. A systematic literature review is a methodical and comprehensive approach to reviewing existing research to synthesize findings on a specific topic (Booth, Sutton, & Papaioannou, 2016). This design is appropriate as it enables the aggregation of existing knowledge, and identification of trends, patterns, and gaps in the current research on ransomware. By systematically identifying, evaluating, and synthesizing relevant studies, this design ensures a thorough understanding of the topic and provides a solid foundation for developing effective mitigation strategies.

3.3 Data Collection Methods

The data collection method for this study primarily involves secondary data collection, with a focus on a literature review. Secondary data, as defined by Babbie (2016), refers to data that has already been collected, processed, and published by other researchers, institutions, or organisations. In the context of this research on the detection and mitigation of ransomware, secondary data is sourced from reputable scientific publications, databases, and papers, ensuring the authenticity and reliability of the study. Notably, databases such as IEEE, ScienceDirect, and Google Scholar are utilised to access relevant literature (Al-Emran et al. 2018). This method is essential for obtaining reliable and relevant data that supports the ransomware investigation.

A literature review, as articulated by Fink (2014), is "a systematic, clear, and repeatable approach for finding, analysing, and synthesising the current corpus of completed and recorded work produced by researchers, scholars, and practitioners." This process allows researchers to place their study within the broader academic debate, facilitating an understanding of the ideas, concepts, procedures, and findings that have been explored by previous researchers (Hart, 1998). Engaging with the existing literature enables researchers to build upon prior knowledge, thereby contributing to the development of the field. Moreover, by critically evaluating various methodologies employed in previous studies, researchers can make informed decisions regarding the most appropriate methods for their research, as emphasised by Webster and Watson (2002).

This study's literature review focuses on the concept of ransomware, examining its origins, types, consequences, and strategies for detection and mitigation. The review involves a systematic process, beginning with the definition of research questions, which guide the literature search and ensure the review remains focused and relevant. A comprehensive search strategy is

developed, employing specific keywords and criteria to identify pertinent literature. The selected studies are evaluated based on their relevance to the research questions, methodological strength, and the significance of their findings (Ridley, 2012). The critical evaluation of these studies ensures the quality and reliability of the data. By synthesising the extracted data, this research provides a thorough overview of the current state of knowledge on ransomware detection and mitigation. Ultimately, relying on secondary data from reputable sources ensures that the study is both comprehensive and up-to-date, offering a solid foundation for subsequent analysis and interpretation.

3.4 Inclusion and Exclusion Criteria

Table 1: Inclusion and Exclusion Criteria

| | Description |
|------------------------------|--|
| Inclusion Criteria | Criteria for Selecting Literature and Data Sources |
| Relevance | Studies must be directly relevant to ransomware investigation and mitigation, including research on ransomware delivery methods, forensic procedures, mitigation strategies, and related topics. |
| Publication Date | Preference will be given to studies published within the last ten years that is between 2014 to 2024 to ensure the data reflects current trends and technologies in ransomware. |
| Peer-Reviewed Sources | Only peer-reviewed journal articles, conference papers, and reputable industry reports will be included to ensure the quality and credibility of the data. |
| Language | Only studies published in English will be included to ensure consistency in data analysis and interpretation. |
| Exclusion Criteria | Criteria for Excluding Literature and Data Sources |
| Irrelevance | Studies that do not directly address ransomware investigation or mitigation, or that focus on unrelated cybersecurity issues, will be excluded. |
| Outdated Research | Research published more than ten years ago will generally be excluded unless it provides |

| | |
|----------------------------------|---|
| | foundational or seminal insights that are still relevant today. |
| Non-Peer-Reviewed Sources | Sources that are not peer-reviewed, such as blog posts, opinion pieces, and non-academic articles, will be excluded to maintain the rigor and reliability of the study. |
| Non-English Publications | Studies published in languages other than English will be excluded due to language barriers and potential difficulties in accurate interpretation and analysis. |

3.5 Data Analysis Techniques

The data analysis technique utilized in this dissertation on the detection and mitigation of ransomware is thematic analysis. This qualitative method systematically identifies, analyses, and reports patterns or themes within data, making it particularly apt for synthesizing secondary data from literature reviews (Braun & Clarke, 2006). Thematic analysis begins with data extraction and familiarisation, wherein relevant research is selected based on specific inclusion and exclusion criteria. This process ensures that only high-quality studies are incorporated, with essential information such as study design and key findings systematically gathered (Kitchenham et al., 2009). Following this, the data undergoes coding and classification, where key concepts or variables are identified and coded, either manually or using specialised software (Thomas & Harden, 2008). The researcher then groups these codes into potential themes that address the research questions, forming broader patterns within the data. Finally, the data is interpreted and discussed within the context of the study's objectives, identifying trends, contradictions, or gaps in the literature, and offering explanations or hypotheses to account for

the observed phenomena (Thomas & Harden, 2008). This structured approach ensures that the findings are robust, rigorously analysed, and transparently reported.

3.6 Ethical Considerations

Although this study relies on secondary data, ethical considerations remain paramount. The researcher must ensure that all sources of data are properly credited to avoid plagiarism and respect the intellectual property rights of the original authors (Silverman, 2016).

1. **Proper Attribution:** The researcher will meticulously cite all sources of information and data used in the study. This includes academic articles, industry reports, and other relevant documents. Proper citation not only gives credit to the original authors but also enhances the credibility and reliability of the research.
2. **Intellectual Property Rights:** Respecting the intellectual property rights of the original authors involves using the data in a manner consistent with ethical research practices. This includes adhering to any usage restrictions and acknowledging the contributions of others.
3. **Sensitivity of Data:** The researcher must be mindful of the sensitivity of the data, especially when discussing ransomware incidents that may involve real individuals or organizations. Any identifiable information will be anonymized to protect the privacy and confidentiality of those involved.
4. **Ethical Approval:** While secondary data analysis generally does not require direct ethical approval, the researcher should still consider obtaining approval from the relevant institutional review board or ethics committee if the data includes sensitive or confidential information.

By adhering to these ethical considerations, the researcher ensures that the study is conducted with integrity and respect for the original data sources and contributors.

Summary

Chapter Three outlined the research methodology employed in this study, which focused on understanding and mitigating ransomware through a qualitative, systematic literature review approach. The qualitative research design, underpinned by the systematic review, has enabled a comprehensive exploration of the complex and multifaceted nature of ransomware, ensuring that the research is both rigorous and insightful. Secondary data collection, primarily through an extensive review of existing literature, has been instrumental in gathering reliable and relevant data from reputable sources. The inclusion and exclusion criteria established in this chapter have further ensured that only the most pertinent and high-quality studies were selected, enhancing the validity of the research findings. The data analysis was conducted using thematic analysis, a method well-suited for identifying and synthesizing patterns within the collected data. This structured approach has facilitated a deep understanding of the themes surrounding ransomware investigation and mitigation, providing a solid foundation for the study's conclusions. Ethical considerations have been thoroughly addressed, ensuring that all data sources were appropriately credited, intellectual property rights were respected, and sensitive information was handled with care.

CHAPTER FOUR: ANALYSIS AND FINDINGS

4.1 Introduction

This chapter aims to analyze the data gathered on the identification and prevention of ransomware in modern computer systems. Using thematic analysis, this chapter assesses the effectiveness of current detection techniques and strategies for prevention, while also investigating areas where the current frameworks fall short. The findings are carefully examined to gain insights into the changing nature of ransomware threats and to validate an improved framework. By systematically evaluating the collected data, this chapter attempts to provide a comprehensive understanding of the strengths and weaknesses of current approaches, ultimately making the way for better solutions to reduce the impact of ransomware attacks.

4.2 Attack Methodology: A Review of the Colonial Pipeline Ransomware Attack

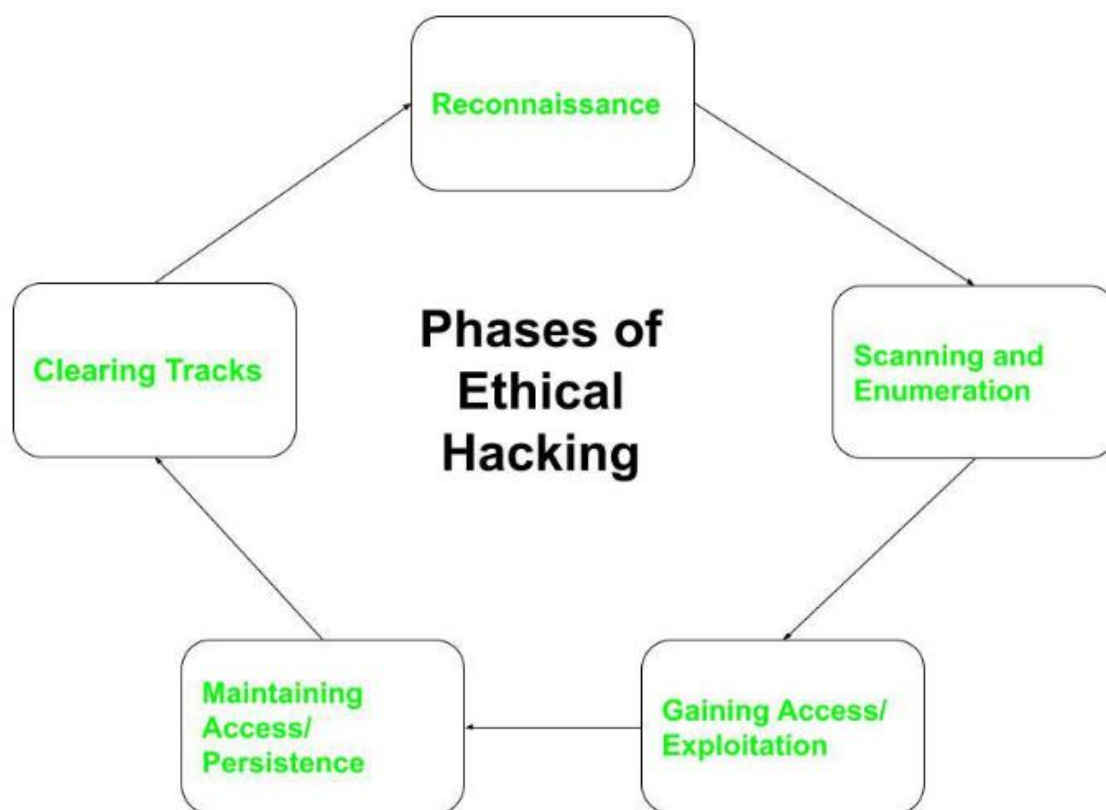
The Colonial Pipeline ransomware attack exemplifies a structured and systematic approach commonly employed by cybercriminals. This section provides an in-depth analysis of the attack methodology, beginning with the standard phases of a hacking operation, progressing through the specific techniques used by the DarkSide group, and concluding with the subsequent responses by Colonial Pipeline and the U.S. government. Understanding the chronological steps involved in such attacks is critical for developing effective detection and mitigation strategies.

Phases of the Attack

Hacking activities typically follow a structured sequence of steps that allow the attackers to gain access to a target system, maintain their presence, and ultimately achieve their objectives. According to Geeks For Geeks (2023), these phases include reconnaissance, scanning, gaining access, maintaining

access, and covering tracks. In the case of the Colonial Pipeline attack, the DarkSide hacker group most likely initiated the process with extensive reconnaissance. This phase involved gathering information about the security measures in place on the Colonial Pipeline network. For instance, they could have monitored the employee list on LinkedIn, identifying potential vulnerabilities such as employees who were about to leave the company (Geeks For Geeks, 2023).

Figure 5: Phases of ethical hacking



(Geeks For Geeks 2023)

Following reconnaissance, DarkSide likely moved on to scanning, where they would have identified open ports and potentially vulnerable accounts within the Colonial Pipeline's network. The next step involved gaining access, which was achieved by exploiting a VPN account that was no longer in active use

following the retirement of a company employee. Although the exact method by which DarkSide obtained the password remains unknown, theories suggest possibilities ranging from key-logging to involvement from a disgruntled employee. Ultimately, the password was discovered in a batch of leaked credentials on the dark web (CyberTalk, 2021; GovTech, 2021).

Exploitation through VPN Access

Once DarkSide obtained the password, they successfully infiltrated the Colonial Pipeline network through the compromised VPN account. The absence of two-factor authentication on this account allowed the attackers unrestricted access to the entire network. This oversight in security protocol highlights the critical importance of multi-layered authentication mechanisms, particularly for VPN services, which, while effective at blocking external access, become a significant vulnerability once breached (Uberti & Stupp, 2021).

After gaining entry, DarkSide had full control over the network infrastructure, enabling them to execute a chained attack. This involved systematically compromising various systems within the network. The earliest evidence of tampering was detected on April 29, though it is possible that access was gained earlier, allowing the group ample time to plan their subsequent actions. Notably, the hackers maintained their presence on the network undetected for a week, during which they were able to exfiltrate over 100 gigabytes of data (Uberti & Stupp, 2021).

The Ransom Demand and Colonial Pipeline's Response

On May 7, at approximately 5 a.m., DarkSide left a ransom note on one of Colonial Pipeline's computer screens, demanding payment of 4.4 million dollars to release their control over the network (Dudley & Golden, 2021). The hackers also threatened to leak the stolen data if their demands were not met. Faced with the potential loss of sensitive information and the crippling of their operations, Colonial Pipeline opted to pay the ransom. This decision

underscores the complex considerations that companies face when dealing with ransomware attacks, where the immediate recovery of operational capabilities often takes precedence over the long-term implications of capitulating to criminal demands (Martin & Weiner, 2021; Parfomak & Jaikaran, 2021).

Despite the payment, the full extent of the data theft and the specific methodologies used by DarkSide to cover their tracks remain unclear. The effectiveness of their attack is evident in the substantial ransom payment, the data breach, and the broader impact on Colonial Pipeline's operations and reputation. Moreover, the incident exposed significant vulnerabilities within the company's network, which could potentially be exploited by other hacker groups in the future. As a response, Colonial Pipeline reported that they had switched VPN services to mitigate the initial security flaw that was exploited (Fung & Sebastian, 2021).

The U.S. Government's Intervention

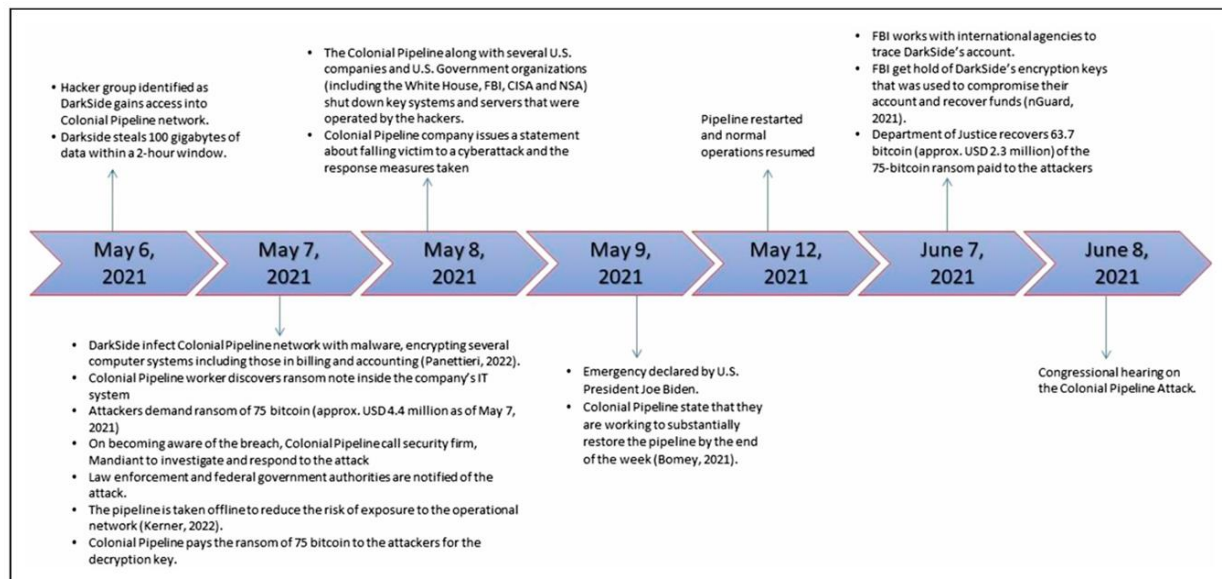
In the aftermath of the attack, the U.S. government took decisive action to mitigate the impact and pursue the perpetrators. The Department of Justice successfully seized \$2.3 million of the ransom payment from the DarkSide group. This operation was authorised by U.S. Magistrate Judge Laurel Beeler and executed by the Special Prosecutions Section and Asset Forfeiture Unit of the U.S. Attorney's Office for the Northern District of California. This seizure, while significant, represents only a portion of the overall ransom paid, and the fate of the remaining stolen funds and data remains uncertain (Office of Public Affairs, 2021).

Summary

The Colonial Pipeline ransomware attack serves as a stark reminder of the sophistication and persistence of modern cybercriminals. The methodology employed by DarkSide, from the initial reconnaissance to the final ransom

demand, illustrates the critical need for robust cybersecurity measures, particularly in industries that are vital to national infrastructure. The response from Colonial Pipeline, though expedient, raises important questions about the long-term consequences of paying ransoms and the effectiveness of existing cybersecurity protocols. As the nature of cyber threats continues to evolve, so too must the strategies for detecting and mitigating such attacks. The insights gained from the Colonial Pipeline incident should inform future efforts to protect critical systems from similar threats.

Figure 6: Colonia Pipeline Ransomware Attack Timeline



4.3 Evaluation of the effectiveness of current mitigation strategies against ransomware attacks

To evaluate the effectiveness of current mitigation strategies against ransomware attacks, several key themes emerge from the literature, focusing on detection, prevention, and response strategies.

Detection Techniques: Modern detection techniques play a critical role in identifying ransomware threats. Machine learning approaches have gained prominence for their ability to detect ransomware through pattern recognition

and behaviour analysis. For instance, Almousa et al. (2021) demonstrate the effectiveness of machine learning in analyzing network traffic to identify ransomware activity. Similarly, Ispahany et al. (2024) highlight the use of advanced machine-learning methods to enhance ransomware detection. Additionally, Zhao et al. (2021) propose a deep learning framework specifically designed for ransomware detection, showcasing the advancements in leveraging deep learning for improved accuracy. These techniques are essential in identifying ransomware before it can execute its payload, thereby reducing the potential impact.

Prevention Strategies: Prevention remains a cornerstone in mitigating ransomware attacks. Strategies such as regular software updates, user education, and proactive system defences are widely endorsed. Bradley (2016) emphasizes the importance of regular updates and security patches in preventing ransomware infections. Baykara and Sekin (2018) propose a "safe zone" system that creates isolated environments to contain potential ransomware threats. Furthermore, Wu et al. (2018) explore ransomware prevention strategies that include behavioural analysis and heuristic detection methods. These preventive measures are critical in reducing the likelihood of ransomware breaches by addressing vulnerabilities before they can be exploited.

Response and Mitigation: Effective response and mitigation strategies are crucial once a ransomware attack occurs. Research by Reilly (2019) focuses on sector-specific responses, such as those in the healthcare industry, highlighting tailored approaches to deal with ransomware incidents. Ganorkar and Kandasamy (2017) discuss defensive mechanisms that include real-time monitoring and incident response protocols. Additionally, Prakash et al. (2017) provide insights into incident response frameworks specifically for Locky ransomware, emphasizing the importance of a structured approach to

recovery. These response strategies are vital in minimizing damage and facilitating recovery after an attack.

Advanced Techniques and Future Directions: Emerging technologies and techniques continue to shape the pattern of ransomware mitigation. For example, the use of federated learning for ransomware detection, as discussed by Koike et al. (2024), represents an advanced approach to enhancing detection capabilities through collaborative learning across multiple entities. Similarly, the research by Singh et al. (2020) on ransomware analysis and defence indicates ongoing advancements in understanding and combating ransomware threats. These innovations suggest a trend towards more sophisticated and adaptive solutions that are crucial for staying ahead of evolving ransomware tactics.

Table 2: Thematic analysis of the evaluation of the effectiveness of current mitigation strategies against ransomware attacks

| Theme | Sub-theme | Key Points | Literature Citations |
|--------------------------------|-------------------------------------|---|---|
| Detection Techniques | Machine Learning | Utilizes pattern recognition and behaviour analysis to identify ransomware. Approaches include network traffic analysis and deep learning frameworks. | Almousa et al. (2021), Zhao et al. (2021), Ispahany et al. (2024) |
| Prevention Strategies | Regular Software Updates | Emphasizes the necessity of keeping software and systems updated to close vulnerabilities that could be exploited by ransomware. | Bradley (2016) |
| | User Education | Involves training users to recognize phishing attempts and other ransomware delivery methods to prevent infections. | Wu et al. (2018) |
| | Isolated Environments | Uses "safe zones" or sandbox environments to contain and mitigate ransomware threats before they affect the broader system. | Baykara and Sekin (2018) |
| Response and Mitigation | Incident Response Protocols | Includes real-time monitoring, structured response frameworks, and sector-specific approaches to manage and recover from ransomware attacks. | Reilly (2019), Ganorkar and Kandasamy (2017), Prakash et al. (2017) |
| | Real-Time Monitoring | Involves continuous surveillance of network activity to detect and respond to ransomware attacks swiftly. | Ganorkar and Kandasamy (2017) |
| Advanced Techniques | Federated Learning | Applies collaborative learning methods across multiple entities to enhance detection capabilities and adapt to new ransomware variants. | Koike et al. (2024) |
| | Behavioural and Heuristic Detection | Combines behavioural analysis with heuristic methods to identify ransomware based on its actions and characteristics. | Wu et al. (2018) |
| Emerging Trends | Ransomware Analysis | Ongoing research into new ransomware strains and defensive techniques to improve the overall effectiveness and adaptability of mitigation strategies. | Singh et al. (2020) |

4.4 Identifying gaps and limitations in the existing detection and mitigation frameworks.

To conduct a thematic analysis of the existing detection and mitigation frameworks for insider threats, it is important to identify recurring themes, gaps, and limitations as they are discussed in the literature. This analysis will focus on the following key themes:

1. Technological Frameworks and Their Shortcomings

Numerous studies have explored the technological approaches to insider threat detection and mitigation, highlighting the use of machine learning, behavioural analytics, and system monitoring tools (Hald & Pedersen, 2021; Probst et al., 2020; Schultz, 2021). However, these frameworks often face limitations in real-world applicability due to issues like false positives and the high cost of implementation (Greitzer et al., 2018; Park et al., 2021). While technological advancements have enhanced the capability to detect insider threats, they frequently struggle to balance accuracy with usability, leading to either over-alerting or under-detection (BaMaung et al., 2018). This suggests a gap in frameworks that can adapt to varying environments without sacrificing detection efficiency.

2. Human Factors and Organizational Culture

Human behaviour and organizational culture play crucial roles in insider threat scenarios, yet they remain underexplored in many frameworks (Nurse et al., 2019; Ponemon Institute, 2022). Studies suggest that most detection systems fail to adequately account for the nuances of employee behaviour or the influence of workplace culture (Shaw & Fischer, 2020). For example, employees under stress or those with grievances may exhibit behaviour that could be flagged as suspicious, leading to potential false positives (Costa et al., 2019). This indicates a significant gap in the integration of psychological

and sociological insights into detection frameworks, which could enhance the understanding of insider motivations and improve detection accuracy.

3. Policy and Governance Limitations

Another critical theme in the literature is the role of policy and governance in mitigating insider threats. Although many organizations have established policies, the enforcement and effectiveness of these policies are often inconsistent (Cappelli et al., 2016; Colwill, 2009). The literature points to a need for more strong governance frameworks that are not only well-defined but also flexible enough to adapt to changing threat pattern (Gheyas & Abdallah, 2016). Additionally, there is a noted lack of comprehensive policy frameworks that effectively integrate technical, human, and organizational aspects (Hunker & Probst, 2011). This gap underscores the need for a general approach that combines policy with other mitigation strategies.

4. Data Privacy and Ethical Considerations

The tension between effective insider threat detection and the preservation of data privacy is another significant theme. Many frameworks have been criticized for potentially infringing on employee privacy or creating ethical dilemmas (Greitzer & Hohimer, 2016; Gaikwad et al., 2021). The literature highlights a gap in frameworks that can achieve a balance between comprehensive monitoring and respect for individual privacy rights (Brackney & Anderson, 2004; Martin & Rice, 2011). This issue is particularly pressing given the increasing use of advanced monitoring tools that can deeply intrude into personal data, raising concerns about the ethical implications of such practices.

5. Insider Threat Awareness and Training

Despite the availability of sophisticated detection tools, the literature consistently emphasizes the importance of insider threat awareness and

training programs (Cole & Ring, 2006; Greitzer et al., 2010). However, there is a noted gap in the effectiveness of these programs, as many are not tailored to specific organizational contexts or do not evolve with emerging threats (Keeney et al., 2005; PWC, 2021). This suggests a need for more dynamic and continuous training initiatives that are aligned with both current and potential future threats, ensuring that employees are both aware of and able to respond to insider threat scenarios effectively.

Table 3: Thematic analysis to identify gaps and limitations in existing detection and mitigation frameworks for insider threats

| Theme | Description | Gaps/Limitations | Key Literature |
|---|--|--|--|
| Technological Frameworks | Focuses on the use of machine learning, behavioural analytics, and monitoring tools for detecting insider threats. | High false positive rates High implementation costs Limited real-world applicability Balance between accuracy and usability is lacking | Hald & Pedersen (2021); Probst et al. (2020); Schultz (2021); Greitzer et al. (2018) |
| Human Factors and Organizational Culture | Examines the role of employee behaviour and workplace culture in insider threat scenarios. | Insufficient integration of psychological and sociological insights Lack of understanding of employee motivations Potential for false positives | Nurse et al. (2019); Shaw & Fischer (2020); Costa et al. (2019) |
| Policy and Governance | Discusses the role of organizational policies and governance frameworks in mitigating insider threats. | Inconsistent enforcement of policies Lack of comprehensive and flexible governance frameworks Poor integration of technical and organizational aspects | Cappelli et al. (2016); Colwill (2009); Gheyas & Abdallah (2016) |
| Data Privacy and Ethical Considerations | Addresses the balance between effective threat detection and the preservation of employee privacy and ethical standards. | Potential infringement on employee privacy Ethical dilemmas due to invasive monitoring Lack of frameworks balancing monitoring and privacy rights | Greitzer & Hohimer (2016); Gaikwad et al. (2021); Brackney & Anderson (2004) |
| Insider Threat Awareness and Training | Focuses on the importance and effectiveness of awareness and training programs for mitigating insider threats. | Ineffective or outdated training programs Lack of contextualization for specific organizations Failure to evolve with emerging threats | Cole & Ring (2006); Greitzer et al. (2010); Keeney et al. (2005); PWC (2021) |

4.5 Mitigation Techniques in Ransomware Attacks: Colonia Pipeline

Understanding the effectiveness of mitigation techniques in preventing and responding to ransomware attacks is essential for any organisation. These attacks, which have been on the rise in recent years, pose significant risks to businesses and can severely disrupt operations if not adequately mitigated. Mitigation, as defined by Bullock et al. (2013), involves actions taken to reduce or eliminate risk to people and property from hazards and their effects. In the context of ransomware, effective mitigation strategies are critical to reducing the impact of an attack and ensuring that businesses can continue to operate efficiently. Early implementation of these strategies is particularly beneficial, as it can protect organisations from the increasingly sophisticated tactics used by attackers.

A key element of ransomware mitigation involves the proper installation and maintenance of computers and networks. Ensuring that these systems are correctly set up is a fundamental step in preventing attacks. For instance, maintaining up-to-date operating systems, application software, browsers, plug-ins, firmware, and anti-virus software is crucial. These updates should be tested thoroughly to avoid introducing new vulnerabilities into the system (Singh & Sittig, 2016). Additionally, network engineers should ensure that organisational firewalls are properly configured to prevent unauthorised access to resources. These basic security measures are the first line of defence against ransomware and can significantly reduce the likelihood of an attack.

Beyond these technical measures, it is also important for organisations to implement control access policies. These policies should restrict users' ability to create and remove files from computers, install and run software applications, and access only the systems and services required by their roles. The principle of "Least Privilege" is particularly relevant here, as it limits users' access rights to the minimum necessary for their jobs (Singh & Sittig, 2016).

For users who require administrative privileges, organisations can create two accounts: one with administrative rights for specific tasks and another with restricted access for everyday activities such as reading emails and browsing the Internet. These practices help minimise the potential damage from ransomware attacks by limiting the actions that users can perform on the network.

In addition to technical defences and access controls, security awareness training plays a vital role in ransomware mitigation. Training should be both informative and engaging, equipping users with the knowledge they need to recognise and respond to potential threats. This training is essential because even the most sophisticated technical defences can be undermined by human error. Pre-existing security awareness courses can be utilised, reducing the burden on the organisation to develop new content. During these sessions, IT staff should work closely with users to create realistic scenarios that prepare them for potential attacks (Singh & Sittig, 2016). For example, IT professionals can help users identify legitimate emails by creating and sending examples from the organisation's IT department. This builds trust between the IT team and users, enhancing the effectiveness of phishing detection efforts.

Moreover, conducting simulated phishing attacks and mock system recovery exercises can further increase users' ability to respond to real ransomware incidents. By periodically testing users with fake emails or links that mimic legitimate sources, organisations can assess their readiness and reinforce best practices (Singh & Sittig, 2016). These exercises are crucial for ensuring that users remain vigilant and can quickly identify and report suspicious activities. The inclusion of two-factor authentication across all user accounts adds an additional layer of security, making it more difficult for attackers to gain unauthorised access.

Monitoring systems for suspicious activities is another essential aspect of ransomware mitigation. A robust network and user activity monitoring system can detect early warning signs of an attack, such as receipt of emails from known fraudulent sources, executable email attachments, unexpected changes in key files, unknown processes encrypting files, or significant increases in network traffic on unexpected ports (Singh & Sittig, 2016). Continuous surveillance enables organisations to respond swiftly to potential threats, thereby minimising the impact of a ransomware attack. IT staff should regularly review the external environment for vulnerabilities and potential risks, ensuring that mitigation strategies remain effective over time.

In the event of a ransomware attack, users must know the appropriate steps to take to protect themselves and the organisation. If an attack occurs, affected users should immediately turn off their computers and report the incident to the IT support team. IT professionals should then disconnect the infected machines from the network and disable wireless network functionality to prevent the spread of the ransomware. In cases where the attack becomes widespread, both wireless and wired networks should be shut down to contain the damage (Singh & Sittig, 2016). These precautions are vital for an organisation's survival in the face of increasing security threats. Furthermore, organisations should collaborate with external security experts to continually assess and enhance their systems and security policies.

The Colonial Pipeline ransomware attack in May 2021 serves as a stark reminder of the importance of robust mitigation strategies. This attack, which disrupted fuel supplies across the eastern United States, highlighted several areas where improvements could have been made. If the Colonial Pipeline system had been better secured, particularly through the use of multi-factor authentication, the attackers might have been less likely to gain access to critical systems (Medlock III, 2021). Strong passwords, anti-malware

software, and vigilance against suspicious links are basic but effective methods that could have helped mitigate the damage (Monteith, 2016).

In response to the growing threat of ransomware, the United States government has taken steps to strengthen its defences. The Department of Justice (DoJ), for instance, has established a Ransomware and Digital Extortion Task Force. This initiative was introduced to combat the rising number of cyber-attacks targeting the nation's critical infrastructure, including the Colonial Pipeline attack (DeMarco, 2021). One significant measure undertaken by the DoJ was the issuance of a memorandum by Deputy Attorney General Lisa Monaco on 3 June 2021. This memorandum instructed federal prosecutors to treat ransomware cases with the same urgency and seriousness as terrorism cases, centralising the tracking and handling of these incidents (DeMarco, 2021). Such an approach underscores the critical importance of ransomware mitigation at both organisational and national levels.

4.6 Proposed Detection and Mitigation Framework

Based on the thematic analysis and identified gaps in the literature, the following is a proposed enhanced, comprehensive framework for the detection and mitigation of ransomware. This framework integrates multiple layers of defence, focusing on early detection, proactive prevention, user education, and standardized response mechanisms.

1. Multi-Layered Detection Mechanism

a. Signature-Based Detection:

- Continue to utilize signature-based detection for identifying known ransomware strains. This method remains effective for detecting previously cataloged threats with established signatures.

- **Integration:** Regular updates of signature databases should be complemented with behavioral analysis systems to cover the detection of new variants.

b. Behavior-Based Detection:

- Implement machine learning algorithms that analyze user and system behaviors to detect anomalies indicative of ransomware activity. This could include monitoring file encryption patterns, unusual file access requests, or suspicious process behaviors.
- **Hybrid Approach:** Combine behavioral detection with signature-based methods to reduce false positives. For instance, a detected anomaly would trigger a deeper signature analysis before action is taken.

c. Anomaly Detection Using AI:

- Employ AI-based models that learn from historical data and adapt to new threats in real-time. These models should be designed to evolve with emerging ransomware tactics, reducing the gap between detection and the appearance of new ransomware variants (Sgandurra et al., 2016).

2. Proactive Threat Intelligence Integration

a. Threat Intelligence Feeds:

- Integrate threat intelligence feeds that provide real-time data on emerging ransomware threats, IP blacklists, and known malicious domains.
- **Pre-Attack Detection:** Use this intelligence to identify potential attacks before they infiltrate the network, applying preemptive blocking of known malicious entities (Al-Rimy et al., 2018).

b. Honeypots and Deception Technology:

- Deploy honeypots designed to attract ransomware attacks, which can then be studied to develop more effective detection signatures and behavioral rules.
- **Information Sharing:** Data gathered from honeypots should be shared across platforms to update global threat intelligence networks (Griffin et al., 2019).

3. User Education and Awareness Programs

a. Phishing Simulation and Training:

- Implement regular phishing simulation exercises to educate users on recognizing and avoiding ransomware entry points, such as malicious email attachments or links.
- **Behavioral Metrics:** Track user responses to these simulations to identify high-risk individuals who may require additional training (Taylor et al., 2019).

b. Incident Response Protocols:

- Develop and train employees on specific protocols for responding to suspected ransomware attacks, including immediate steps to isolate infected systems and notify IT teams.
- **Automated Alerts:** Incorporate automated alerts that guide users through initial response steps in the event of a ransomware detection.

4. Standardization and Interoperability

a. Unified Defense Framework:

- Establish standardized protocols for ransomware detection and mitigation that can be adopted across different platforms and security tools, ensuring interoperability.
- **Industry Collaboration:** Encourage collaboration between security vendors to develop APIs and data exchange standards that allow different security systems to communicate and work together effectively (Kharraz et al., 2016).

b. Centralized Monitoring and Reporting:

- Implement a centralized monitoring system that consolidates data from various security tools, enabling a comprehensive view of the network's security posture.
- **Automated Correlation:** Use automated systems to correlate data from different sources, enhancing the detection of complex, multi-vector ransomware attacks (Kolodenker et al., 2017).

5. Post-Attack Mitigation and Recovery

a. Regular Backups and Redundancy:

- Maintain regular, encrypted backups of all critical data, with redundancy across multiple locations to ensure quick recovery in the event of a ransomware attack.
- **Immutable Backups:** Implement immutable backup solutions that prevent data from being altered or deleted by ransomware (Scaife et al., 2016).

b. Rapid Incident Response Teams:

- Develop specialized incident response teams trained to deal specifically with ransomware attacks. These teams should be

equipped with tools for quick containment, system restoration, and forensic analysis.

- **Forensic Analysis:** Post-incident, conduct a thorough forensic analysis to understand the attack vector and update detection mechanisms accordingly.

6. Legal and Compliance Considerations

a. Compliance with Industry Standards:

- Ensure that the framework aligns with industry-specific regulations and standards, such as GDPR for data protection or NIST guidelines for cybersecurity.
- **Regular Audits:** Conduct regular audits to ensure compliance and identify any weaknesses in the ransomware mitigation strategy (Taylor et al., 2019).

b. Legal Readiness:

- Prepare legal protocols for responding to ransomware demands, including when to engage law enforcement and how to handle ransom payments, if necessary.
- **Data Privacy Considerations:** Ensure that the legal response considers data privacy laws and the potential implications of data breaches caused by ransomware.

7. Continuous Improvement and Adaptation

a. Ongoing Research and Development:

- Invest in ongoing research to keep the framework updated with the latest ransomware trends and mitigation techniques.

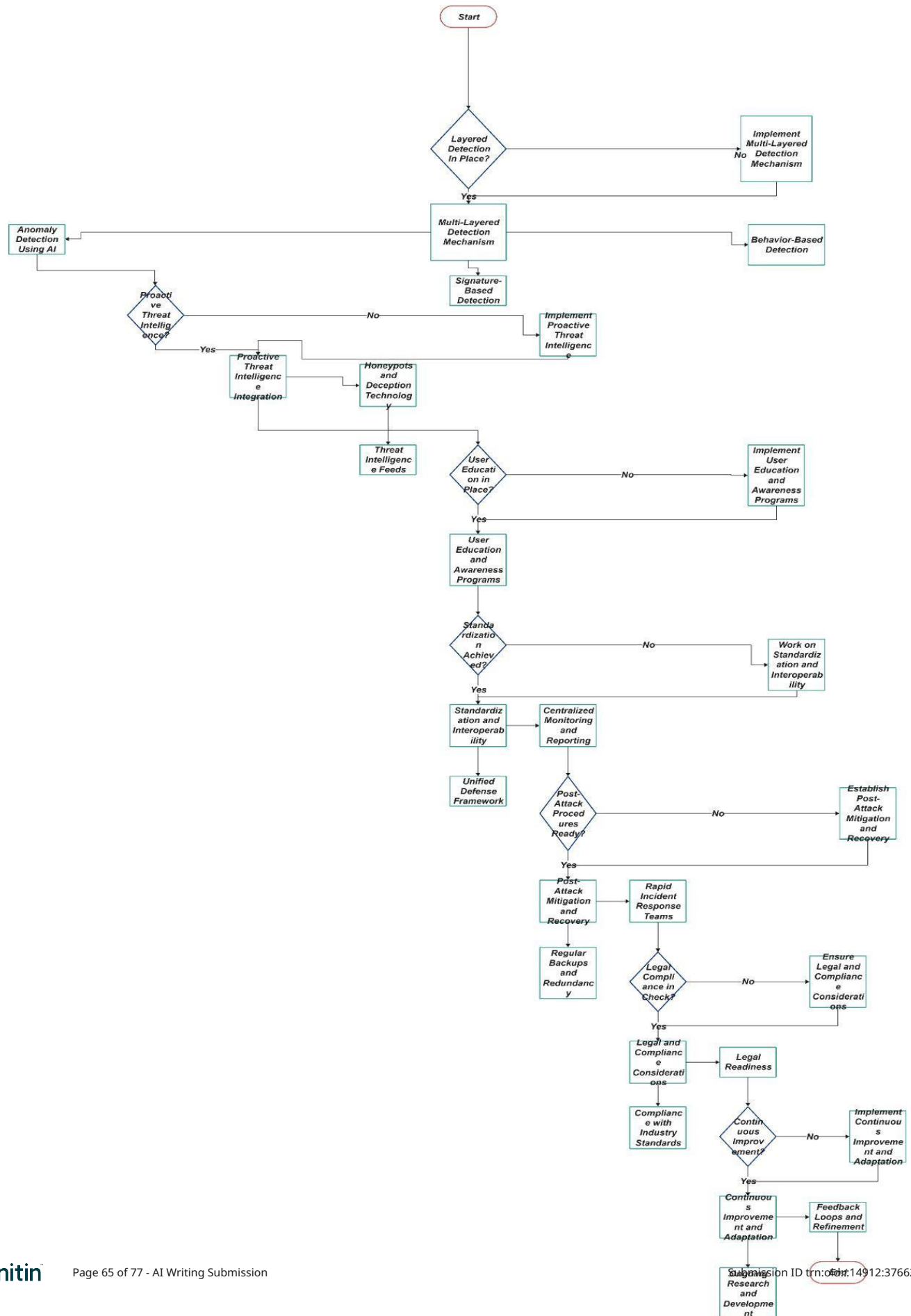
- **Community Engagement:** Engage with the broader cybersecurity community to share findings, tools, and strategies for combating ransomware (Griffin et al., 2019).

b. Feedback Loops and Refinement:

- Establish feedback loops from all layers of the framework, allowing continuous refinement based on real-world performance and emerging threats.
- **Periodic Review:** Regularly review and update the framework to address new challenges and incorporate technological advancements (Sgandurra et al., 2016).

"This comprehensive framework aims to provide strong protection against ransomware threats by addressing identified gaps and integrating multi-faceted strategies. It emphasizes the importance of early detection, proactive defense, user involvement, and continuous adaptation, offering a resilient approach to the ever-evolving ransomware pattern."

Proposed Ransomware Detection and Mitigation Framework's Flowchart



4.7 Summary

Chapter Four of the research focuses on the analysis and findings related to the detection and mitigation of ransomware, using the Colonial Pipeline ransomware attack as a case study. The chapter begins by outlining the attack methodology employed by the DarkSide group, highlighting the phases of the attack, including reconnaissance, exploitation through a compromised VPN, and the ransom demand. The analysis then evaluates the effectiveness of current ransomware detection and prevention techniques, emphasizing machine learning, software updates, and user education. Additionally, the chapter identifies gaps in existing frameworks, such as technological shortcomings, human factors, and policy limitations. The effectiveness of mitigation techniques is also discussed, with a focus on the importance of robust security measures, access controls, and user awareness training. Finally, the chapter concludes by highlighting the need for continuous improvement in ransomware defense strategies to address evolving threats.

CHAPTER FIVE: SUMMARY CONCLUSION, RECOMMENDATION AND SUGGESTION FOR FURTHER STUDIES

5.1 Introduction

This chapter provides the overall summary and the overall conclusion of the dissertation, thereby giving recommendations on how to detect and mitigate ransomware based on the findings of the dissertation, and then suggestions for future studies were also made.

5.2 Discussion of Findings

The Colonial Pipeline ransomware attack analysis offers critical insights into the broader pattern of ransomware detection and mitigation strategies. The findings align closely with the research objectives, revealing the strengths and weaknesses of current approaches while pointing towards potential areas for improvement.

Comprehensive Assessment of Existing Ransomware Literature

The Colonial Pipeline attack highlights the increasingly sophisticated nature of ransomware threats, as well as the evolving tactics used by cybercriminals. This case exemplifies the broader trends observed in recent ransomware literature, where attacks are characterized by meticulous planning, targeted exploitation, and swift execution. The use of a compromised VPN account without multi-factor authentication reflects a common vulnerability that has been identified across multiple ransomware incidents. The literature consistently highlights the need for robust, layered security measures to counteract such vulnerabilities.

Evaluation of Current Detection Techniques

The detection of ransomware remains a critical challenge in modern computing environments. The case of the Colonial Pipeline attack reveals gaps in real-

time detection capabilities, particularly in identifying and responding to the presence of attackers within a network before significant damage occurs. The literature reviewed highlights the effectiveness of machine learning and deep learning techniques in detecting anomalous behaviours indicative of ransomware. However, the Colonial Pipeline incident suggests that these techniques need to be integrated more effectively into organizational security frameworks to detect and neutralize threats before they can escalate.

Assessment of Mitigation Strategies

The mitigation strategies employed during the Colonial Pipeline attack highlight both strengths and weaknesses in current approaches. While the organization eventually regained control over its network, the initial response—paying the ransom—reflects the desperation that often accompanies such incidents. This decision also underscores the limitations of existing mitigation strategies, which may not be robust enough to prevent the need for such drastic measures. The literature suggests that while traditional strategies like software updates, user education, and access controls are essential, they are insufficient on their own to mitigate sophisticated attacks like the one on Colonial Pipeline. The attack demonstrates the importance of adopting advanced techniques, such as multi-factor authentication and continuous network monitoring, to enhance the resilience of systems against ransomware.

Identification of Gaps and Potential New Methods for Mitigation

The findings from the Colonial Pipeline attack highlight several critical gaps in current mitigation frameworks. First, the lack of comprehensive real-time detection mechanisms allowed the attackers to maintain undetected access to the network for an extended period. Additionally, the insufficient use of multi-factor authentication and robust password policies contributed to the attack's

success. These gaps suggest potential new methods for mitigating ransomware, including the development of more advanced authentication protocols, enhanced real-time monitoring systems, and more rigorous user training programs focused on identifying and responding to ransomware threats.

Proposal for a Framework for Detection and Mitigation

Based on the limitations identified in the Colonial Pipeline case and the broader literature, a comprehensive framework for the detection and mitigation of ransomware can be proposed. This framework should integrate multiple layers of defence, incorporating machine learning and deep learning techniques for early detection, coupled with robust authentication measures to prevent unauthorized access. Additionally, continuous user education and simulation exercises should be a core component of this framework, ensuring that all employees are equipped to recognize and respond to potential threats. Finally, the framework should include standardized response protocols that can be swiftly enacted in the event of an attack, minimizing damage and facilitating rapid recovery.

5.3 Conclusion

In the complex world of ransomware, where attackers' methods are evolving, and exploiting every possible vulnerability, it is more important than ever to have strong detection and mitigation strategies. The findings from this dissertation highlight a harsh reality: while there has been progress, current frameworks still have significant shortcomings that require urgent attention. The Colonial Pipeline attack highlights gaps in cybersecurity. Despite organizations having substantial resources and advanced tools, the attack succeeded due to simple oversights, such as the absence of multi-factor authentication on a VPN account. This incident shows how attackers can

exploit minor issues to launch devastating attacks, emphasizing the urgent need for more resilient and comprehensive defense mechanisms.

The current methods for detecting threats, while advanced, are not perfect. Signature-based techniques work well against known threats but struggle with new ransomware variants. Behavior-based detection, which uses machine learning, is a promising approach but needs more work to reduce false positives and become more reliable. The use of AI and deep learning is showing potential in adapting to new threats, but these technologies need to progress quickly to keep up with the increasingly sophisticated tactics of ransomware. The foundation of prevention strategies is crucial, but their implementation is often inconsistent. It is important to regularly update software, educate users, and proactively defend systems; however, many organizations struggle to maintain these practices at the necessary level of rigor. The idea of a "safe zone" for ransomware prevention is innovative, but it needs more widespread adoption and practical application to be truly effective.

The response to ransomware attacks highlights several areas needing improvement. The effectiveness of current incident response frameworks varies, and many organizations lack the preparedness to handle attacks swiftly and efficiently. It is essential to incorporate real-time monitoring, conduct regular simulations, and develop comprehensive recovery plans, which often fall short in practice. There is a critical need for specialized incident response teams and enhanced legal readiness, including clear protocols for dealing with ransom demands and data breaches. It has been identified that there is a critical gap in the integration between technological solutions and human factors. While many frameworks emphasize technological defenses, they often overlook the psychological and sociological aspects of ransomware threats. Understanding employee behavior, organizational culture, and the impact of

stress or grievances on security practices can significantly improve detection accuracy and response effectiveness.

In addition, policy and governance frameworks need to be strengthened. Effective enforcement of security policies, coupled with the flexibility to adapt to evolving threats, is essential. The tension between comprehensive monitoring and data privacy also requires careful balancing to avoid infringing on individual rights while ensuring robust protection against threats. In addressing these gaps, the proposed comprehensive framework offers a multidimensional approach to ransomware detection and mitigation. By integrating advanced detection techniques, proactive threat intelligence, user education, standardized protocols, and continuous improvement, this framework aims to provide a more resilient defense against ransomware attacks. It emphasizes the importance of a strategy that encompasses not only technological solutions but also organizational culture, policy enforcement, and legal considerations. Ultimately, the battle against ransomware is not one that can be won with isolated solutions or piecemeal improvements. It requires a concerted effort to address existing vulnerabilities, adapt to emerging threats, and continuously refine strategies in response to real-world challenges. The findings from this dissertation highlight the urgency of this ongoing battle and the need for a unified, comprehensive approach to safeguard against the ever-evolving threat of ransomware.

5.4 Recommendations

The following recommendations were made based on the findings of the study

Enhanced Multi-Layered Detection Systems: Organisations should adopt advanced machine learning and AI-based detection systems that combine signature-based and behavior-based methods. This hybrid approach improves detection accuracy by minimizing false positives and quickly adapting to new

ransomware variants. Also, regular updates to signature databases and behavioral analysis models are crucial. Keeping these resources current with the latest threat intelligence ensures timely identification of emerging ransomware threats.

Strengthened Proactive Prevention Measures: Maintain a rigorous schedule for updating and patching operating systems, software applications, and firmware. This reduces vulnerabilities that ransomware could exploit. Enforce MFA across all critical systems, particularly for remote access points like VPNs, to add layer of security against unauthorized access.

Comprehensive User Education Programs: Regularly conduct phishing simulation exercises and interactive training programs to keep employees aware of current threats and improve their ability to recognize and respond to potential ransomware attacks. Train employees on detailed incident response protocols, including steps to take in the event of a suspected ransomware attack. Ensure that these protocols are regularly updated and tested.

Robust Incident Response and Recovery Planning: Form specialized incident response teams trained specifically for handling ransomware attacks. Equip these teams with the necessary tools for containment, recovery, and forensic analysis. Implement regular, encrypted backups of critical data and ensure redundancy across multiple locations. Adopt immutable backup solutions to prevent alteration or deletion by ransomware.

Strengthening Legal and Compliance Frameworks: Ensure compliance with industry-specific regulations and cybersecurity standards, such as GDPR or NIST. Regularly audit policies to identify and address any gaps in compliance. Develop clear legal protocols for dealing with ransom demands, including engagement with law enforcement and considerations for handling ransom payments.

Ongoing Research and Adaptation: Support ongoing research into new ransomware threats and mitigation technologies. Engage with the cybersecurity community to stay informed about emerging trends and best practices. Create feedback loops from all aspects of the ransomware mitigation framework to continuously refine and improve strategies based on real-world performance and evolving threats.

5.5 Suggestions for Further Studies

1. **Exploration of Emerging Threats:** Conduct studies on the evolution of ransomware tactics and techniques, particularly focusing on new variants and their implications for current detection and mitigation strategies. Investigate how emerging technologies, such as quantum computing, might affect ransomware detection and mitigation. Explore potential advancements and adaptations needed to counteract these threats.
2. **Human Factors and Behavioural Analysis:** Research the impact of human behaviour and organizational culture on cybersecurity practices. Develop frameworks that integrate psychological and sociological insights to enhance the effectiveness of detection and prevention strategies. Study the long-term effectiveness of various user training programs and phishing simulations. Identify the most effective methods for improving user awareness and response to ransomware threats.
3. **Integration of AI and Machine Learning:** Further explore the application of AI and machine learning in anomaly detection for ransomware. Investigate the efficacy of different AI models and their ability to adapt to rapidly changing ransomware tactics. Examine the use of federated learning in threat intelligence sharing and its potential to enhance collective ransomware detection and mitigation efforts.

4. **Economic and Policy Implications:** Analyse the economic impact of ransom payments versus other mitigation strategies. Explore the long-term effects of paying ransoms on organizational security and financial stability. Investigate the effectiveness of current cybersecurity policies and governance frameworks in mitigating ransomware threats. Develop recommendations for creating more robust and adaptable policy structures.
5. **Global Perspectives and Collaboration:** Study the effectiveness of international cooperation and information sharing in combating ransomware. Identify best practices for cross-border collaboration and develop strategies to enhance global cybersecurity efforts. Examine how regional differences in cybersecurity threats and practices affect ransomware mitigation strategies. Develop region-specific recommendations for improving detection and response to ransomware attacks.

In the labyrinthine world of ransomware, where attackers constantly evolve their methods and exploit every conceivable vulnerability, the quest for robust detection and mitigation strategies is more crucial than ever. The findings from this dissertation underscore a stark reality: while progress has been made, current frameworks still exhibit significant shortcomings that demand urgent attention.

The Colonial Pipeline attack serves as a glaring illustration of these gaps. Despite the substantial resources and sophisticated tools at the disposal of modern organizations, the attack's success was facilitated by a combination of simple oversights—like the lack of multi-factor authentication on a VPN account—and the broader systemic vulnerabilities inherent in many cybersecurity approaches. This incident exemplifies how attackers can exploit even minor lapses to launch devastating attacks, highlighting the pressing need for more resilient and comprehensive defense mechanisms.

Current detection techniques, while advanced, are not without their flaws. Signature-based methods, though effective against known threats, fall short when faced with novel ransomware variants. Behaviour-based detection, powered by machine learning, offers a promising avenue but requires further refinement to minimize false positives and improve reliability. The integration of AI and deep learning shows promise in adapting to new threats, but these technologies must evolve rapidly to keep pace with increasingly sophisticated ransomware tactics.

Prevention strategies remain foundational, yet their implementation is often inconsistent. Regular software updates, user education, and proactive system defenses are crucial, but many organizations struggle to maintain these practices at the necessary level of rigor. The concept of a "safe zone" for ransomware prevention, while innovative, requires more widespread adoption and practical application to be truly effective.

The response to ransomware attacks also reveals significant areas for improvement. The effectiveness of current incident response frameworks varies, with many organizations lacking the necessary preparedness to handle attacks swiftly and efficiently. The incorporation of real-time monitoring, regular simulations, and comprehensive recovery plans is essential, but often falls short in practice. The need for specialized incident response teams and enhanced legal readiness, including clear protocols for dealing with ransom demands and data breaches, cannot be overstated.

One critical gap identified is the lack of integration between technological solutions and human factors. While many frameworks emphasize technological defenses, they often neglect the psychological and sociological aspects of ransomware threats. Understanding employee behavior, organizational culture, and the impact of stress or grievances on security practices can significantly enhance detection accuracy and response effectiveness.

Furthermore, policy and governance frameworks need strengthening. Effective enforcement of security policies, combined with flexibility to adapt to evolving threats, is essential. The tension between comprehensive monitoring and data privacy also requires careful balancing to avoid infringing on individual rights while ensuring robust protection against threats.

In addressing these gaps, the proposed comprehensive framework offers a multidimensional approach to ransomware detection and mitigation. By integrating advanced detection techniques, proactive threat intelligence, user education, standardized protocols, and continuous improvement, this framework aims to provide a more resilient defense against ransomware attacks. It emphasizes the importance of an all-round strategy that encompasses not only technological solutions but also organizational culture, policy enforcement, and legal considerations.

Ultimately, the battle against ransomware is not one that can be won with isolated solutions or piecemeal improvements. It requires a concerted effort to address existing vulnerabilities, adapt to emerging threats, and continuously refine strategies in response to real-world challenges. The findings from this dissertation highlight the urgency of this ongoing battle and the need for a unified, comprehensive approach to safeguard against the ever-evolving threat of ransomware.