Ransomware Rewired: The Evolution of Extortion in the Age of Encryption

Pavan Subhash Chandrabose Nara
Department of Computer Science
Southeast Missouri State University
Cape Girardeau, Missouri, USA

Suhair Amer
Department of Computer Science
Southeast Missouri State University
Cape Girardeau, Missouri, USA

ABSTRACT
This paper delves into the multifaceted nature of ransomware, a type of malware that restricts user access to their digital devices and/or data, demanding payment for its release. The study begins by tracing the evolution of ransomware from its rudimentary origins, exemplified by the AIDS Trojan in 1989, to the sophisticated cyber extortion schemes of the present day. It highlights the financial motivations behind ransomware attacks, distinguishing them from other forms of malware, and categorizes the various types of ransomwares, such as crypto malware, lockers, scareware, and doxware, each with its own modus operandi. The paper also analyzes the ethical quandaries that arise from ransomware attacks, examining the motivations and targets of cybercriminals, the varying responses of victimized entities, and the broader ethical implications of paying ransoms. Furthermore, it presents a study on the behavioral changes and risk perceptions of victims' post-attack, shedding light on the psychological and practical aftermath of ransomware incidents. The paper concludes by underscoring the escalating threat of ransomware, advocating for enhanced protective measures, and stressing the importance of legal and ethical frameworks to address this complex cybercrime.

Keywords
Ransomware, Cyber Ethics, Cyber Security, Malware, Data Encryption, Ransom Payment, Ethical Dilem- mas, Post-Attack Behavior, Risk Perception, Cybercrime, Data Recovery, Prevention Strategies.

1. INTRODUCTION
Since the rise of digital media there as been the rise of threats from threat actors, which are aiming to gain some form of data from the users. Sometimes it is information, sometimes it is their credentials, and sometimes they ask for ransom in exchange for their data [5]. Ransomware is not a specific one kind of threat, there might be a combination of threats. The usual thing is that threat actors gain access to the victim's data using any threat, it might be phishing or backdoor and will encrypt their data. Then demand some ransom to retrieve that data [8], [9].

Ransomware is a type of virus, or malware that locks users out of their computers and computing devices. It can also lock files and folders on a computer using private key encryption. The user or owner of the device will then be asked to pay a ransom in order to get access to their computer or files again. Normally the ransom is paid electronically, with Bitcoin being the primary electronic currency used in ransomware attacks. To put it simply, ransomware is like a digital shakedown. Imagine someone breaking into your house, locking all your valuables in a safe, and demanding a payment to give you the code.

In the digital world, ransomware does the same thing to your computer files. The first ransomware virus, AIDS Trojan was created in 1989 and used simple encryption to encrypt file names. Electronic currency was not known then, so ransoms were normally paid by having victims send prepaid cards in the mail. The first modern ransomware virus was created around 2005 and was spread as an attachment to a spam email. In 2009, an instance of ransomware locked down screens and was seen in Russian speaking countries [26].

In 2011 the shift was made from locking screens and encrypting files, to having a law enforcement agency claiming that the computer contains illegal files and is being used for malicious purposes [29]. Users were then informed that they had to pay a legal fine within a certain amount of time, or else they would be arrested. This is when ransomware started not just targeting Russian speaking countries and using prepaid forms of currency but was spreading across the world and demanding ransom to be paid using electronic payment methods [26].

Ransomware has been on the rise because of the accessibility of electronic-anonymous-payment methods to anyone with a computer and Internet connection. In fact, the FBI predicted that ransomware would become a one-billion-dollar crime in 2016 with an increase in attacks on businesses and corporations, like hospitals, schools, and even newspapers [4]. Although, malware comes in many different forms and is constantly evolving and we need to keep updating our antivirus software and use other security measures, one of the most serious threats is considered ransomware. Ransomware is much more complicated than a worm, keylogger, or an average Trojan Horse program, because it has financial demands.

If the user that is being attacked does not pay a fee to unlock and reclaim his/her personal data, he/she will lose the data indefinitely. Two prominent and more commonly known are:

- Locker ransomware which encrypts an entire hard drive and can shut the user out of the system entirely
- Crypto ransomware which will deliberately encrypt specific files like word documents, PDFs, and image files like PNGs or JPEG.

In general, Ransomware automatically corrupts and deletes files if money or information is not exchanged [26]. Ransomware comes in four distinct types: crypto malware, lockers, scareware, and doxware. Crypto malware is the most common form of ransomware. In this threat, the virus is spread to all computers connected to a specific network. Lockers infect a single computer's operating system and prevent the user from accessing files. Scareware appears like an antivirus software and states that there is a problem with the computer through multiple pop-ups. To make these alerts disappear, the user must pay a fee. Doxware, also known as leak ware, threatens to release personal information if a ransom is not paid [26]. Ransomware victims vary and their vulnerability to a ransomware attack depends on how attractive one's data is and how vulnerable one's security

is to criminal hackers.

It, also, depends on how fast the victim will respond to the ransom demand. No one can be completely immune to the effects of ransomware. In a fall 2016 ransomware study conducted by BitSight, educational institutions placed the number 1 target. Government agencies ranked as second and that the number of attacks on them tripled from fall 2015 to fall 2016. Healthcare organizations ranked third because hospitals would pay the ransom because patients' data is critical especially in life-or-death situations [23].

2. RELATED WORKS

Ransomware has evolved significantly since its early appearance in 1989 with the AIDS Trojan, which used simple encryption and physical mail for ransom payments [26]. Modern ransomware has grown more sophisticated, leveraging electronic currencies like Bitcoin and targeting a wider range of victims. The FBI predicted a substantial increase in ransomware attacks, estimating it would become a billion- dollar crime by 2016, affecting various organizations including hospitals and schools [4].

O'Gorman and McDonald [26] provide an overview of the growing menace of ransomware, detailing its mechanisms and early evolution. The effectiveness of ransomware is attributed to its complex nature compared to other malware, with its ability to encrypt and hold data hostage until a ransom is paid. Different variants of ransomware, including crypto malware, lockers, scareware, and doxware, each pose unique challenges. Martin [23] highlights the increasing targeting of institutions such as educational institutions, government agencies, and healthcare organizations, emphasizing the critical impact on sectors where data availability is crucial.

Fruhlinger [11][12] discusses specific ransomware attacks like WannaCry and NotPetya, illustrating the exploitation of vulnerabilities and the scale of damage inflicted. The CryptoLocker attack, as detailed by Jarvis [18], marked a significant escalation in ransomware attacks due to its widespread impact and the use of strong encryption. Mamedov, Sinitsyn, and Ivanov [22] analyze the Bad Rabbit ransomware, demonstrating the adaptability of ransomware in utilizing drive-by attacks to infiltrate corporate networks.

Kulkarni et. al [27] explore preventive measures and incident response strategies, particularly in the context of Locky ransomware. Rashid [29] discusses the Cyber ransomware's attack vector through Office 365, highlighting the exploitation of macros in document files. Krebs [19] and Matthews [24] provide real-world examples of ransomware attacks on organizations, such as Tribune Publishing and healthcare facilities, underscoring the disruptive impact on operations and services. Kruse et al. [1] examine the healthcare sector's vulnerability to ransomware, pointing out the systemic issues that contribute to its susceptibility.

Davis [5][8] documents several ransomware incidents in the healthcare industry, illustrating the repercussions of such attacks on patient care and data security. Lambeck [21] reports on an attack on a school district, indicating the widespread nature of ransomware threats across different sectors.

Ganorkar and Kandasamy [13] contribute to the under- standing of crypto-ransomware and strategies for defense. Graham [15] discusses the significant impact of the WannaCry attack on the UK's National Health Service. Empey [9] provides a guide on ransomware and protective measures. The FBI [10] offers resources on ransomware prevention and response. Kremez and Farral [20] delve into the ethical dilemmas associated with ransomware, particularly within the cybercriminal community.

Hassan [17] presents an ethical position statement on a ransomware attack on Medstar. Hammill [16] discusses the broader societal implications of ransomware. The Council of European Union [25] and the European Commission [3] address the regulatory and research ethics aspects of dual- use technologies, relevant to the misuse potential of ransomware research. Alper, Lenzini, and Sgandurra [14] explore deception-based protection strategies against ransomware. Simoiu et al. [2] present a study on user behavior and perceptions following ransomware attacks. Van Schaik et al. [28] analyzes risk perceptions and precautionary behaviors related to cybersecurity. Upadhyaya and Jain [31] provide a study into cyber ethics and cybercrime, focusing on the legal and ethical dimensions of ransomware.

3. EXPLAINING RANSOMWARE AND AVAILABLE PROTECTION

There are several methods to defend against ransomware attacks. Since a large portion of ransomware attacks originate from emails, it is important to verify the sender's authenticity before opening any attachments. It is also advised against enabling macros in downloaded documents from emails. Anti-malware software can provide a layer of defense against ransomware, and some programs are designed to remove ransomware from infected devices [4].

The process of a ransomware attack can be visualized in a few steps:

- *Infection:* Ransomware enters a system, often through a phishing email or malicious download.
- *Encryption:* It then locks up the user's files by encrypting them, changing the data so it's unreadable without a special key.
- *Demand:* Finally, it displays a message demanding a ransom payment, usually in cryptocurrency, for the decryption key.

Regularly updating systems with the latest security patches is crucial for protecting against ransomware and other types of virus attacks [30]. Another security measure is to immediately isolate any device suspected of being infected to prevent the malware from spreading across the network [30]. Furthermore, cultivating a security-aware culture within organizations can help mitigate risks associated with modern technology.

It is also essential for users to regularly back up their data on external devices or cloud storage, which allows for data restoration in the event of an attack [13]. Removing ransomware can be approached in several ways. Paying the ransom is the most straightforward method, although it is generally discouraged. Some ransomware, like the "WannaCry" virus, may offer the option to decrypt a limited number of files for free [15]. If computer access is still available, running an antivirus software in safe mode can help remove the ransomware [9].

Antivirus companies often recommend performing a full security scan to identify the specific type of ransomware and suggest copying encrypted files to an external drive to attempt decryption on an uninfected system. Companies like AVG pro-vide free tools for file decryption [30]. Ransomware operates by identifying and encrypting important files, rendering them inaccessible until a ransom is paid, typically in Bitcoin or other cryptocurrencies. Victims are notified of the infection and given instructions for payment to receive a decryption key.

However, paying the ransom does not always guarantee the recovery of data, as some victims may not receive the promised decryption keys. The FBI warns against paying ransoms, as it can encourage further criminal activity, and some victims have been asked to pay additional fees [10].

4. ETHICAL DILEMMAS

Ransomware attacks present several ethical dilemmas. For instance, cybercriminals often choose to target profitable companies or powerful government bodies. There is a perception among them that it is justifiable to steal from certain entities. However, there is disapproval within the cybercriminal com- munity when attacks target vulnerable populations or those deemed undeserving. These ethical dilemmas can be viewed through different ethical lenses. For example, a utilitarian perspective might weigh the needs of the many (access to healthcare, business continuity) against the harm caused by funding criminal enterprises. A deontological perspective, focused on moral duties, might argue that paying a ransom is inherently wrong, regardless of the consequences.

A notable example is the 2016 attack on Hollywood Presbyterian Medical Center, where the hospital was compelled to pay a $17,000 ransom to regain access to critical, life-saving equipment. This attack was widely condemned by other cybercriminals, with one expressing strong disapproval of targeting hospitals. Similarly, the WannaCry attack in 2017, which disrupted the UK's National Health Service, led to discussions among hackers about potentially banning ransomware due to the increased scrutiny and defensive measures it prompted. Some cyber-criminal groups, particularly in Russia, adhere to an ethical code that explicitly prohibits targeting hospitals, recognizing the potential for fatal consequences.

A complex ethical dilemma arises when comparing the responses of different healthcare providers to ransomware attacks. Hollywood Presbyterian Medical Center chose to pay a 40 Bitcoin ransom to quickly restore their systems and administrative functions. In contrast, Medstar Health opted not to pay the $19,000 ransom, instead shutting down their electronic records system, using paper records, and restoring data from backups, recovering nearly 90% of functionality within a week without paying the attackers. This situation prompts a debate on whether it is more ethical to pay the ransom to secure confidential patient data and ensure the continuity of critical services or to refuse to negotiate with cybercriminals. The core of the ethical dilemma lies in weighing the potential risks to patients' lives and the long-term consequences of either decision. While disrupting hospital services for ransom is undoubtedly a crime, the ethical consideration involves determining which course of action demonstrates greater responsibility and foresight.

Another ethical issue concerns companies facing ransomware attacks. Since ransomware is an illegal element of cyberspace, the decision to pay ransom can also be seen as problematic. Attackers exploit an organization or individual's sensitive information, and the ethical dilemma revolves around whether to pay the ransom to recover the data. Some argue that paying the ransom incentivizes further attacks, creating a lucrative environment for cybercriminals, who amassed around

$1 billion from ransomware in 2016 alone. Employee loyalty also introduces ethical considerations. Despite companies' investment in internal security, ransomware can still infiltrate their systems, sometimes with the help of insiders.

Furthermore, ransomware involves various ethical violations, including invasion of privacy, fraud, hacking, identity theft, piracy, trespass, and vandalism.

The debate around publishing research on potential vulnerabilities in anti-ransomware defenses also raises ethical questions about the potential for misuse. This concern is linked to the "dual use" nature of research, as defined in regulations like Council Regulation (EC) No 428/2009, where technologies can be used for both beneficial and malicious purposes. The European Commission has addressed the ethical implications of "Misuse of research", which could lead to the development of technologies for unethical purposes.

Some researchers, however, argue that disclosing potential weaknesses in anti-ransomware strategies can drive improvements and help cybersecurity professionals proactively enhance defenses. For example, researchers in discuss limitations in specific anti-ransomware approaches but emphasize that they do not disclose any code that could be misused and that they engage in dialogue with the authors of the analyzed applications.

5. POST-ATTACK

A study by Simoiu et al. [2] investigated the changes in user habits following a ransomware attack. The study revealed that 56% of respondents reported altering two or more habits, with the most common changes being more careful browsing (65%), purchasing antivirus software (44%), and updating antivirus software (31%).

Other changes included initiating data backups (26%), enabling automatic updates (24%), backing up data more regularly (22%), changing operating system configurations (20%), changing the operating system (10%), and changing the default browser (12%). Notably, none of the participants reported encrypting their hard drives following an attack. The study also found that the operating system used by victims significantly influenced victimization rates, with Windows users experiencing higher rates compared to non-Windows users. It is important to acknowledge the inherent difficulty in definitively determining whether participants' self-reported changes in habits accurately reflect their actual behavior [2].

The study by Simoiu et al. [2] yielded two key conclusions. Firstly, most victims attribute their ransomware experience, at least in part, to their own actions. Secondly, despite data backup being identified as the most effective strategy for mitigating the impact of ransomware, a minority of victims adopt this practice even after experiencing an attack, highlighting the need for increased awareness to promote this behavior [2].

In their research, Simoiu et al. [2] also explored how experiencing a ransomware attack influences risk perception. They assessed this through two questions:

- How likely do you think you are to experience a ransomware attack in the future?
- Suppose you were to experience a ransomware attack today and the only way of restoring access to the data on your computer was to pay the ransom (say $300). How likely is it that you'd pay the ransom?

Participants provided responses on a scale from 0 to 100, where 0 indicated no likelihood and 100 indicated certainty. The study found that victims reported a mean likelihood of 47 for future attacks, compared to a mean of 30 for non-victims, suggesting that victims perceive themselves to be at a higher risk of future attacks. Additionally, victims reported a lower likelihood of paying a ransom compared to non-victims.

The authors speculate that this lower likelihood of paying a ransom among victims may stem from a belief that they are now better equipped to handle future attacks. However, they emphasize the need for further research to fully understand the underlying reasons for these differences in risk perception and behavioral intentions [2].

It is widely recognized that risk perceptions, risk response, the adoption of precautionary security measures, online behavior, and awareness of one's vulnerability to security threats all play a significant role in shaping effective security practices [28].

6. TRENDS AND EMERGING THREATS

Ransomware has had a significant and growing impact on modern life, affecting individuals, businesses, healthcare systems, government and critical infrastructure. Some of the trends and emerging threats of ransomware include AI and machine learning, targeting IoT and OT (industrial systems), and supply chain attacks. Next are some examples.

Rele et al. [32] discuss how ransomware has emerged as a growing cybersecurity threat due to its capability to encrypt data and demand payment for its release. They explain that ransomware's adaptive and evolving nature often renders traditional detection methods ineffective. They proposed a novel approach to ransomware detection that leverages artificial intelligence (AI) and machine learning (ML). The proposed technique combines robust anomaly detection and classification algorithms with advanced feature extraction from system logs, network traffic, and file metadata. Their method employed autoencoders and isolation forests for anomaly detection, along with random forests and support vector machines for classification. After testing, their approach achieved high accuracy with minimal false-positive rates, significantly outperforming existing methods. The findings underscore the potential of AI and ML integration in cybersecurity, providing a strong foundation for proactive ransomware detection and mitigation [32].

Al-Hawawreh et al. [33] explain that due to the complexity and heterogeneity of Industrial Internet of Things (IIoT) system, which encompass diverse devices, both legacy and modern connectivity protocols, and distributed network architectures, these environments are increasingly attractive targets for sophisticated cyberattacks such as ransomware. Their paper explored ransomware threats and associated detection methods in IIoT environments from multiple perspectives, including recent attack trends, ransomware types, targeted operating systems, and platforms. They discuss the evolution and common architecture of IIoT systems, followed by an in-depth examination of ransomware development, its structural components, and evolving tactics. They also, presented a thorough review of recent research on detection models and highlight several critical challenges that remain unresolved. They concluded that there are urgent need for both offensive and defensive research efforts to safeguard IIoT systems against the growing threat of ransomware [33].

The study of Cartwright and Cartwright [34] examines the economics of ransomware attacks within production supply chains, emphasizing how interdependence among firms can be exploited by cybercriminals. They explain that Integrated supply chains create mutual dependencies, allowing attackers to maximize impact by targeting a single firm and effectively holding multiple firms hostage. In addition, overlapping or inconsistent security systems further expose vulnerabilities, where it may be optimal for attackers to compromise a smaller supplier to extort a larger producer central to the network. They developed a game-theoretic model of ransomware attacks on supply chains and solve for two types of Nash equilibria. To illustrate their findings, they analyzed a hub-and-spoke configuration and extend the analysis through simulations of more general network structures. The results show that the total ransom demand increases with the average path length of the network and being lowest in hub-and-spoke networks and highest in linear (chain-like) networks. Finally, they discuss several strategies for mitigating these risks [34].

7. CONCLUSION

Ransomware attacks represent a significant threat to both organizations and individuals, jeopardizing vital data stored on internet-connected devices. This malicious software locks users out of their devices, preventing access to data until a ransom is paid. Ransomware has been employed against a wide range of targets, including politicians, hospitals, po- lice departments, governments, lawmakers, businesses, and individuals. As technology advances, ransomware attacks are becoming increasingly sophisticated and destructive. Notable examples of ransomware include AIDS Trojan, GPCoder, CryZip, CryptoLocker, and SamSam.

Unfortunately, there are situations where traditional defense strategies may not be effective. In such cases, negotiating with attackers might be the only viable option to recover files in the short term. Although this approach raises ethical concerns, the potential value and critical nature of the compromised data may outweigh those concerns for some users, such as in the context of sensitive medical records. Negotiation typically involves either paying the ransom or attempting to bargain for a lower amount. The Hollywood Presbyterian Medical Center's response to a ransomware attack in 2016, where they negotiated the ransom down from $3.7 million to $17,000, illustrates this tactic.

The decision to comply with attackers' demands is influenced by several factors beyond the type and value of the encrypted files. These factors include the level of trust in the attackers, the credibility of their threat, and the financial cost of the ransom. Ideally, attackers would honor the agreement and provide the decryption key or restore access to the files or device.

However, there is minimal recourse against attackers who fail to cooperate, and the risk of being caught is negligible. Consequently, there is no assurance of a positive outcome. Time is a critical factor in victims' decisions; if seeking alternative solutions is more time-consuming than meeting the attackers' demands, negotiation becomes the preferred option. The central ethical dilemma concerning ransomware is whether to pay the ransom or refuse to comply. Regardless of the chosen course of action, it is imperative to educate all computer users about ransomware and how to protect themselves. Furthermore, there is an urgent need for the development and adaptation of laws to keep pace with the rapid advancement of technology. Laws must be enacted swiftly to defend against these malicious attacks and to educate the public.

To effectively combat ransomware, stronger legal frameworks are essential. This includes mandating clear data breach reporting procedures, establishing harsher penalties for attackers, and providing legal guidance on how organizations should respond to attacks. International cooperation is also vital, as ransomware often crosses borders.

8. REFERENCES

[1] T. Jacobson C. S. Kruse, B. Frederick and D. K. Monticone. Cyberse- curity in healthcare: A systematic review of modern threats and trends. Technical report, Texas State

University, San Marcos, August 2017.

[2] Joseph Bonneau Camelia Simoiu, Christopher Gates and Sharad Goel. "i was told to buy a software or lose my computer. i ignored it": A study of ransomware. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, Santa Clara, CA, USA, August 11–13 2019.

[3] European Commission. Guidance note - research involving dual-use items. Technical report, 2016.

[4] Mauro Conti, Tooska Dargahi, and Ali Dehghantanha. *Cyber Threat Intelligence: Challenges and Opportunities*, page 1–6. Springer Inter- national Publishing, Cham, Switzerland, 2018.

[5] J. Davis. Allscripts hit by ransomware, knocking some services offline, Jan 2018.

[6] J. Davis. Ransomware attack on fetal diagnostic lab breaches 40,800 patient records, Sept 2018.

[7] J. Davis. Ransomware attack on hancock health drives providers to pen and paper, Jan 2018.

[8] Jessica Davis. Ransomware, malware attack breaches 45,000 patient records. *Healthcare IT News*, July 2018. Accessed: 07 April 2025.

[9] C. Empey. The essential guide to ransomware and how to protect yourself, Feb 2018. Avast Blog, Avast Software S.r.o.

[10] FBI. Ransomware prevention and response for cisos, July 2016. US Department of Justice.

[11] J. Fruhlinger. What is wannacry ransomware, how does it infect, and who was responsible?, 2018. ProQuest.

[12] Josh Fruhlinger. Wannacry explained: A perfect ransomware storm. *CSO Online*, August 2022.

[13] S. Ganorkar and K. Kandasamy. Understanding and defending crypto- ransomware. *ARPN Journal of Engineering and Applied Sciences*, 12:3920–3925, 2017.

[14] Ziya Alper Genc¸, Gabriele Lenzini, and Daniele Sgandurra. On deception-based protection against cryptographic ransomware. In Roberto Perdisci, Cle´mentine Maurice, Giorgio Giacinto, and Magnus Almgren, editors, *Detection of Intrusions and Malware, and Vulnera- bility Assessment*, page 219–239, Cham, Switzerland, 2019. Springer International Publishing.

[15] C. Graham. Nhs cyber attack: Everything you need to know about 'biggest ransomware' offensive in history, May 2017. The Telegraph.

[16] A. Hammill. *The rise and wrath of ransomware and what it means for society*. Diss., Utica College, 2017.

[17] N. Hassan. Ransomware attack on medstar: Ethical position statement. *SEISENSE Journal of Management*, 1(4):29–31, 2018. Zenodo.

[18] Keith Jarvis. Cryptolocker ransomware, December 2013.

[19] B. Krebs. Cloud hosting provider dataresolution.net battling christmas eve ransomware attack, 2019.

[20] V. Kremez and T. Farral. How ransomware has become an 'ethical' dilemma in the eastern european underground, 2016.

[21] L. Lambeck. Bridgeport schools computer network hit by ransomware attack, Jan 2019.

[22] O. Mamedov, F. Sinitsyn, and A. Ivanov. Bad rabbit ransomware, October 2017.

[23] J. Martin. Who is a target for ransomware attacks?, July 2017.

[24] L. Matthews. Ransomware attack disrupts emergency services at ohio hospital, 2018.

[25] Council of European Union. Council regulation (eu) no 428/2009, 2009.

[26] Gavin O'Gorman and Geoff McDonald. Ransomware: A growing menace. Technical report, Symantec Security Response, 2012.

[27] T. Nafis P. Kulkarni and S. Biswas. Preventive measures and incident response for locky ransomware. *International Journal of Advanced Research in Computer Science*, 8(5), 2017. ProQuest.

[28] Joseph Onibokun Lynne Coventry Jurjen Jansen Paul Van Schaik, Debora Jeske and Petko Kusev. Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75:547–559, 2017.

[29] F. Rashid. Cerber ransomware targets enterprises via office 365, 2016. ProQuest.

[30] R. Richardson and M. North. Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1):10–21, 2017.

[31] R. Upadhyaya and A. Jain. Cyber ethics and cyber crime: a deep dwelved study into legality, ransomware, underground web and bitcoin wallet. In *2016 International Conference on Computing, Communication and Automation (ICCCA)*, page 143–148. IEEE, April 2016.

[32] Mayur Rele, John Samuel, Dipti Patil, Udaya Krishnan, Exploring Ransomware Detection Based on Artificial Intelligence and Machine Learning, Procedia Computer Science, Volume 252, 2025, Pages 548-556, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2025.01.014. (https://www.sciencedirect.com/science/article/pii/S1877050925000146)

[33] Muna Al-Hawawreh, Mamoun Alazab, Mohamed Amine Ferrag, M. Shamim Hossain, Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms, Journal of Network and Computer Applications, Volume 223, 2024, 103809, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2023.103809. (https://www.sciencedirect.com/science/article/pii/S10848045230022 8X)

[34] Anna Cartwright and Edward Cartwright. 2023. The Economics of Ransomware Attacks on Integrated Supply Chain Networks. Digital Threats 4, 4, Article 56 (December 2023), 14 pages. https://doi.org/10.1145/3579647