DOI: 10.53477/1842-9904-23-12

SOFT COMPUTING IN PREVENTING RANSOMWARE RELYING ON LARGER-SCALE DATA AND ANALYSIS

Attila Mate KOVACS*

Ransomware attacks continue to pose a significant threat to organizations and individuals worldwide. The attackers' ability to constantly evolve and adapt their tactics challenges traditional cybersecurity approaches to keep pace. Ransomware attacks targeting the healthcare industry accounted for 45% of all reported cyberattacks. The nature and scale of attacks and the increasing healthcare technology adoption will continue to pose ransomware attack risks. However, by collecting and analyzing large volumes of data and applying soft computing techniques, cybersecurity experts can improve their ability to detect and prevent ransomware attacks. As a result, soft computing offers options for detecting and preventing malware attacks. Using methods from the field of soft computing, such as fuzzy logic, neural networks, and genetic algorithms, makes it possible to conduct a thorough analysis of large data sets. These can yield insightful information that can help recognize and react to ransomware attacks. These techniques can also help to decrypt files that have been encrypted using ransomware.

Keywords: *soft computing; cybersecurity; ransomware; healthcare; detection; fuzzy logic; genetic algorithm; neural network.*

Introduction

In the last few years, we have witnessed increased concerns from the media, governments, and private sector players regarding the potential damage attributed to cyberattacks. Cyberattacks have continued to develop, taking different forms,

**** Attila Mate KOVACS is a PhD Candidate within Óbuda University Doctoral School on Safety and Security Sciences, Budapest, Hungary. E-mail: attilamate.kovacs@gmail.com***

such as installing spyware in personal computers, spreading worms or viruses, and attempting to destroy a country's critical infrastructures (Christiansen and Piekarz 2019). Computers and other digital devices worldwide are now more susceptible to attacks from different malware. Some of the most common attacks include denial-of-service (DOS), Trojan horses, viruses, worms, blended threats, backdoors, rootkits, email bombs, zombies, and ransomware.

However, ransomware has been the most prevalent malware in the healthcare industry over the past years. Ransomware holds the target data "hostage" for some ransom (Mookherjee et al. 2020). The main focus of ransomware attacks is data availability. Due to the significant impacts of ransomware, recent studies have focused on its growing intensity and threats. Projections now indicate that costs attributed to ransomware attacks will hit over $11.5 billion annually (Hassan 2019). Ransomware attacks will continue to grow up to 350% annually, making the attacks a significant source of threats to critical infrastructures such as healthcare systems. In response, the focus is shifting to the potential use of soft computing to fight ransomware attacks.

For the last three decades, the subject of soft computing has been the focus of substantial scientific investigation. As a result, various soft computing models have found applications in diverse fields, such as agriculture, biological engineering, and information security systems (Mishra, Satapathy, and Chatterjee 2022, 2). The diversity of soft computing models makes soft computing techniques a reliable strategy for solving complex problems. Significantly, over the last few decades, there has been a constant increase in the usage of soft computing to combat cyberattacks in the field of information security. The paper reviews the literature on large-scale ransomware attacks and the use of soft computing in the fight against cyberattacks.

Methodology

The paper adopts a qualitative case study approach to review, synthesize, and make study recommendations. Qualitative research methodology focuses on understanding a humanistic query as an idealistic approach (Pathak, Kalra, and Jena 2013). The authors reiterate that the qualitative method is reliable due to its basis on numeric and strategies that other researchers can use and propagate objectively. Conversely, the qualitative case study technique investigates and analyses single or collective cases to reflect the intricate nature of the research target (Hyett, Kenny, and Dickson-Swift 2014, 2). In this respect, a case is an object under study based on a particular or peculiar reason. In addition, the classification and selection of cases help to clarify the study topic and design the study strategy. As a result, there are three study cases and study design frameworks. The case study frameworks are the intrinsic case, the instrumental case, and the collective instrumental case (Rubin and Babbie. 2016).

The objective of the intrinsic case, as opposed to understanding the function of a case, is to gain insight into the particulars of a single item. (Hyett, Kenny, and Dickson-Swift 2014, 2). An instrumental case is employed to elucidate an issue under study or refine a particular theory. Such a case study is adopted to promote a better comprehension of an object of interest. A collective case study, on the other hand, is an instrumental study that makes use of numerous nested cases. This paper adopts a collective qualitative case study focusing on the objects of ransomware and software computing. The qualitative approach was chosen owing to the numerous benefits associated with the methodology. Because the researcher had access to the most recent, high-quality data, qualitative research technique offers a thorough grasp of a studied subject or area (Pathak, Kalra, and Jena 2013, 46).

Hypothesis

The paper is intended to test the following hypothesis: "If soft computing models can imitate human brains, can soft computing help fight against the threats of ransomware"? Besides, the paper hypothesizes that combining vast data samples and soft computing techniques can enhance ransomware detection and prevention. Consequently, the paper collects and assesses large data samples based on ransomware attacks while using soft computing literature to test the hypothesis. When large ransomware data samples and soft computing strategies are combined, the result can enhance overall cybersecurity, leading to effective detection, quicker reaction times, and less downtime.

Moreover, gathering large data samples on ransomware attacks can make it possible to develop more efficient machine-learning models, resulting in increased detection skills. By combining these strategies, businesses can strengthen their defence against ransomware attacks, minimizing the damage caused by successful attacks and reducing future assaults. According to the paper, preventing ransomware attacks will require a combination of the accumulation and analysis of large data samples and the application of soft computing techniques.

Literature Review

Initially, scholars and practitioners believed that ransomware originated in Russia. However, Information Resources Management Association (2021) outlines the explosion of cyberattacks in the past 12 years that demystified the myth (see Figure no. 1 for timeline). A review of historical cases of attacks proved that ransomware existed in other parts of the world, including North America and Asia.

Besenyő et al. (2021, 2-3, 24) has analyzed terrorism targeting healthcare facilities and workers since the 9/11 attacks. Their study highlights the vulnerability

of healthcare systems to various threats. This research underscores the importance of enhancing security measures within the healthcare sector, including detecting and preventing attacks. By examining the multiple challenges healthcare facilities face in dealing with terrorism and other threats, this study provides valuable context for understanding the broader implications of attacks and the need for effective countermeasures.

The history of malware can date back to 1970s, when the first malicious programs gained popularity in entertainment (Abaimov and Martellini 2022). Since then, malware has evolved, with the first ransomware detected in 1989 introduced as "AIDS Trojan". The Trojan tricked PC users leading them to encrypt and hide files on a computer drive, which required the owner to pay some ransom for decrypting the files (Kumar et al. 2021, 380). The explosion of the attacks remains the subject of great scrutiny in cybercrime. Research indicates that if unchecked, ransomware will implode and reach levels that could create devastating impacts. As a result, there has been increasing interest in and use of various soft computing techniques (Dawn et al. 2020, 924).

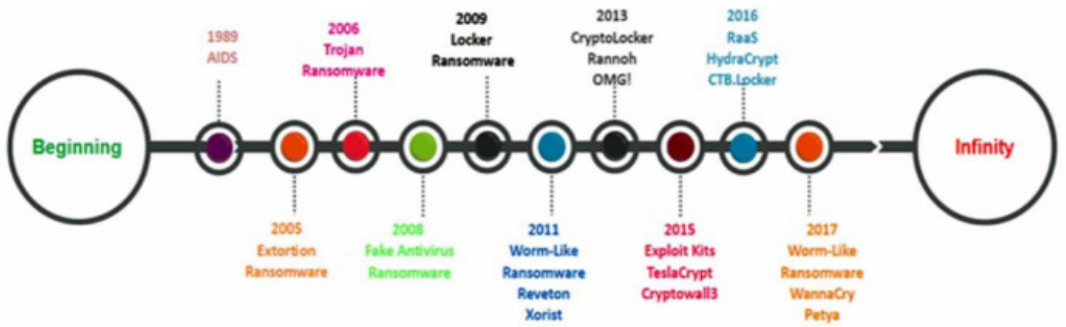

Figure no. 1: The Ransomware Timeline
(Source: Information Resources Management Association 2021)

Researchers believe that traditional methods in the fight against ransomware must be improved (Information Resources Management Association 2021, 1087) to better understand its impacts and advance better prevention and control strategies.

To situate ransomware in the context of malware, it can also be described as a fundamental explanation that ransomware is a malicious malware that conceals files on a target computer or network and demands payment for the decryption key required to release the contents (Abaimov and Martellini 2022). The attackers typically require payment in a cryptocurrency such as Bitcoin, making it difficult to trace the money and the attackers themselves. Ransomware has increased in the scale of attacks, affecting different countries and sectors (see Appendix 1).

Researchers classify ransomware attacks into several categories. According to Fields (2018), ransomware attacks comprise five main categories based on target platforms. Ransomware can take different forms and infect either a personal computer, mobile device, cloud storage, servers, and smart TV sets (Hassan 2019). Regardless of the ransomware category, the authors note that its attacks continue to produce adverse consequences for individuals and organizations. However, ransomware attacks on organizations are typically large-scale and specialized in targeting specific organizations to achieve certain goals.

There are various ways in which ransomware attacks can take place. Fields (2018) states that ransomware attacks can occur through email attachments, malicious links, and software vulnerabilities. In addition, some ransomware appears in lock screen attacks, such as CovidLock, which rely on the user's input to execute a code (Modlin, Amber and Gregory, Andrew and Odebode, Iyanuoluwa and Hodson, Douglas and Grimaila, Michael. 2021, 33). After the virus installs on a device, it typically begins encrypting data and presenting a message to the user demanding money in return for the decryption key (Kovács 2022, 98, 100). Once this process is complete, the malware will typically remove itself.

1. Incidences of Ransomware Attacks

Review cyberattacks indicate that ransomware attacks remain challenging for many organizations and sectors. Alqahtani and Sheldon (2022) note that ransomware attacks affect critical cyber-physical systems and continue to attack many users. In an empirical study involving 50 organizations in the UK and North America, Yuryna Connolly et al. (2020, 2) found that private sectors have faced severe effects of crypto-ransomware attacks. Also, the authors noted that the organization's size was not a factor in ransomware attacks. Ransomware attacks are becoming increasingly common and are a significant threat to sectors that provide critical services. These sectors include healthcare, finance, energy, transportation, and government agencies. These industries are particularly vulnerable because they handle sensitive data and provide essential services that are crucial to the functioning of society.

The healthcare industry is disproportionately affected by ransomware attacks, despite the fact that they affect all enterprises. In the healthcare sector, ransomware attacks continue to be the most common type of cybercrime that is recorded (Mookherjee et al. 2020, 581). During the course of eight years starting from early 2010, the number of ransomware attacks in the healthcare sector has increased by more than 125 percent (Abraham, Chatterjee, and Sims 2019, 547-48). Ransomware is a malicious malware that conceals files on a target computer or network, while demanding for payment to gain access to a decryption key needed to unlock the files. As the healthcare sector expands and transitions digitally, it becomes more

vulnerable, accounting for at least 45% of all cyberattacks (Thamer and Alubady 2021, 213-215). During the COVID-19 pandemic, the US Department of Health Services reports that at least four states fell victim to ransomware, while another 400 hospitals were reportedly on the target list (Dullea, Budke, and Enko 2020, 534). One of the renowned ransomware attacks targeting numerous healthcare systems is the WannaCry, which affected Britain's National Health Services (NHS) (Fields 2018, 85). The WannaCry attack paralyzed operations in over 80 hospitals for four days, leading to delays in clinical appointments and scheduled surgeries (Tully et al. 2020, 229). The other notable ransomware attacks in the healthcare sector are the 2016 Hollywood Presbyterian Hospital in California, which held the hospital's data hostage for ten days until it paid a ransom of $17,000 in bitcoin (Gagneja 2017,1-5). Hospitals are now the primary target for ransomware attacks due to the increasing storage of patient information in digital systems and security holes in hospital information technology systems (see Appendix 2).

Ransomware attacks in the healthcare industry come in different mechanisms. Table no. 1 indicates that cyberattacks targeting the healthcare industry come in nine forms (Alvarez 2017). Notwithstanding the forms of attacks, the incidences of ransomware targeting hospitals rose in 2015 (Nikki et al. 2018, 1, 21-22). A review of reported cases of ransomware indicates that its impacts spread worldwide, with the US being the most affected country (see Appendix 1). Most ransomware attacks affect developed countries, where digital medical information is more valuable to cybercriminals. Similarly, in developed countries, ransomware attacks affect critical national sectors such as transport, healthcare, government agencies, commercial facilities, and energy (Moallem 2020).

Table no. 1: Common Mechanisms of Attacks in Healthcare

Mechanism of Attack	Frequency of Attack
Injected unexpected items	47%
Manipulate data structures	19%
Manipulate system resources	9%
Employ probabilistic techniques	6%
Indicator	6%
Abuse existing functionality	4%
Collect and analyze information	4%
Engage in deceptive interactions	3%
Subvert access control	2%

Attacks within healthcare severely affect individuals and organizations, causing data loss, financial harm, and reputational damage (Fields 2018; The DoD Cyber Exchange 2020). For instance, in 2016 alone, over 73 million ransomware attacks were detected within the healthcare industry (Slayton 2018, 287-288, 293). Of the reported events, nearly 1,500 attacks occurred, and a record of 300 serious incidences. With projections indicating that ransomware attacks may quadruple by 2023, there is a need for preventive strategies. Maintaining up-to-date software, using strong passwords, and exercising caution while reading emails or clicking on links from unfamiliar sources are crucial to avoid ransomware attacks. It is essential to perform frequent data backups to protect against data loss in case of an attack (Singh and Sittig 2016). Government agencies, cybersecurity institutions such as the Cybersecurity and Infrastructure Security Agency (CISA), and private sector recommends strategies such as planning, joint partnerships, preparation, and information sharing (King 2022). However, the evolution in soft computing might provide a timely strategy to avert the impacts of ransomware attacks.

2. Soft Computing

Slayton (2018, 295) outlines that ransomware attacks stood at over 70 million in 2016. Given that the ransomware attacks could rise to numbers that might be complex to manage, research point to the ineffectiveness of conventional approaches (Information Resources Management Association 2021, 1087). The authors attribute the ineffectiveness of conventional methods to the widening cyberspace and increasing numbers of malware. Effective intelligent systems based on challenges under focus and combining appropriate soft computing techniques can be adapted to solve problems. Soft computing is critical in designing intelligent systems that can predict and help solve threats attributed to complex problems.

Soft computing continues to gain relevance in the fight against ransomware. Ransomware attacks continue to rise worldwide, devastatingly impacting critical infrastructures. However, the advanced artificial intelligence (AI) in soft computing has led to advances that can be employed to solve complex ransomware challenges (Shin and Xu 2017, 1). Soft computing is a subfield of Artificial Intelligence (AI) that focuses on creating intelligent algorithms and methods to cope with uncertainty, imprecision, and partial truth in data. AI in soft computing is gaining application in the fight against malware in computing systems and other digital devices.

Research shows that soft computing applications can be applied to detect and prevent ransomware in Android devices. For example, Zhang et al. (2021) found TC-Droid, an automatic threat detection framework for Android, to be effective in malware detection. Similarly, Grini, Shalaginov, and Franke (2018, 337-338) outline the importance of soft computing in overcoming the complexities of modern

ransomware. This paper outlines the importance of soft computing in addressing the complexities of modern ransomware. It demonstrates the effectiveness of using static features extracted from PE32 files and applying Bayesian networks for large-scale malware detection. Using static features extracted from PE32 to study large-scale malware detection, the authors found Bayes Network compelling. In a comprehensive study by Filiz et al. (2021), the authors tested 78 antimalware tools against a sample of 61 ransomware variants. Their findings revealed that the tested tools had minimal impact in effectively combating these ransomware threats. As a result, the authors recommended the adoption of soft computing techniques as more effective alternatives in dealing with ransomware attacks. This study supports the hypothesis that soft computing can enhance ransomware detection and prevention, offering a more robust approach compared to traditional antimalware tools.

Furthermore, Dutta et al. (2021) consent that the best way to combat malware is to use reverse engineering and machine learning. Mohammad (2020) suggests pursuing artificial intelligence in the fight against ransomware in addition to preventive strategies. Sharma et al. (2019, 323-324, 337-338) acknowledge that the complexity of ransomware threats and the data scale requires suitable countermeasures such as fuzzy logic. Similarly, Dovom et al. (2019,2) note that fuzzy logic and fast fuzzy pattern trees provide robust and powerful malware detection. These studies recommend soft computing techniques such as machine learning and artificial intelligence over traditional strategies. Thus, the future in the fight against ransomware might be the application of soft computing strategies. Understanding soft computing techniques is critical in their application against ransomware threats.

Since ransomware is a computer program, soft computing techniques provide a way of analyzing, detecting, and preventing attacks. Soft computing aims to imitate the human brain's capacity to reason and solve issues while operating in an unpredictable and imprecise environment, unlike conventional computer approaches, which depend on specific rules and deterministic models (Shin and Xu 2017). The following are the three primary components of soft computing:

− Fuzzy logic: a mathematical framework that addresses questions of ambiguity and imprecision in data (Dovom et al. 2019,3). Fuzzy logic makes it possible to represent and manipulate nebulous or ambiguous ideas, such as "warm" or "tall," which are complex to describe using typical binary logic;

− Neural or artificial neural networks: computer systems designed to replicate the structure and function of the human brain (Gupta 2021). The networks can learn from data, spot patterns, and make predictions based on information that may be noisy or inadequate;

− Evolutionary computation: refers to a group of optimization algorithms modeled after the processes that occur during biological evolution (Khoda et al. 2021). These algorithms use several strategies to find optimum solutions in spaces

with large dimensions and complicated structures, such as mutation, crossover, and selection.

Research continues to gain momentum in intrusion detection within computer and network security (Sathesh 2019, 72). Techniques from the realm of soft computing are increasingly finding applications in various domains, including control systems, image processing, data mining, pattern recognition, and decision-making systems (Abbasi et al. 2022). Researchers are now proposing different models to detect and prevent malware in Internet of Things (IoT) devices (Khoda et al. 2021). Soft computing models and theories developed to fight ransomware include fuzzy set theory, novel loss function, and particle swarm optimization. These strategies are incredibly effective when working with real-world situations that are complex to solve using typical computer approaches. Soft computing techniques have several applications in cybersecurity (Shin and Xu 2017). Some of the soft computing applications in cybersecurity are:

− Intrusion detection: soft computing strategies such as fuzzy logic and neural networks facilitate detecting network intrusions by analyzing traffic and identifying suspicious activities (Gupta 2021);

− Malware detection: soft computing techniques such as genetic algorithms help detect new and unknown malware by analyzing the behavior of programs and identifying patterns that indicate malicious activity (Lee, Lee, and Yim 2023, 15);

− Spam filtering: soft computing techniques such as neural networks and fuzzy logic apply in filtering spam emails by analyzing the content and identifying patterns that indicate spam (Ahmed et al. 2022, 4);

− Password cracking: soft computing techniques such as genetic algorithms are critical in cracking passwords by generating and testing many possible passwords until it finds the correct one (Shin and Xu 2017);

− Network security: soft computing techniques continue to find applications in optimizing network security by identifying vulnerabilities and developing strategies for mitigating the risk of attacks (Shin and Xu 2017);

− Overall, soft computing techniques have proven helpful in enhancing cybersecurity by providing practical solutions to cybersecurity challenges.

3. Soft Computing in Ransomware Protection

Techniques that make use of soft computing have the potential to play a key role in strengthening the security of healthcare information technology systems (Tully et al. 2020, 230). Healthcare IT security is critical due to the sensitive nature of patient data, including personal information and medical records. Soft computing can improve healthcare IT and security in more ways than one.

Soft computing plays a critical role in anomaly detection. The principles of soft computing help construct intelligent systems capable of recognizing user behavior

patterns and detecting abnormalities that suggest a ransomware attack (Shin and Xu 2017). Soft computing intelligent systems may assist in preventing the ransomware from carrying out its intended function and encrypting the victim's data. In addition, soft computing help analyze the danger of a ransomware attack and uncover weaknesses in the victim's system (Yuryna, Connolly et al. 2020, 7). Furthermore, soft computing approaches may also help avoid ransomware attacks by identifying malicious software or abnormalities, evaluating risk, and building reaction plans (Yuryna Connolly et al. 2020, 17).

Victims can lower the danger of ransomware attacks and keep their data from being encrypted and held for ransom if they combine these approaches with other cybersecurity measures. Moreover, soft computing plays a significant role in intrusion detection. According to Sharma et al. (2019, 336-337), neural networks and fuzzy logic in soft computing find applications in detecting network intrusions by monitoring network traffic and recognizing patterns that suggest suspicious behavior, which can prevent access to medical records. Risk assessment may aid the victim in developing effective security methods and allocating resources. In case a ransomware attack occurs, response plans, such as backup and recovery plans, incident response plans, and communication plans, may be developed using soft computing approaches. Incident response plans can assist the victim in responding swiftly and efficiently to a ransomware attack, reducing the damage and swift recovery of the impacted systems.

Similarly, soft computing methods are beneficial in analyzing the risk of cyberattacks and finding vulnerabilities in healthcare IT systems. Risk assessment is essential to vulnerability analysis against cybersecurity threats attributed to ransomware. Vulnerability analysis in healthcare is critical in developing successful security measures and the proper allocation of resources. Research also points to the effectiveness of soft computing strategies in malware detection (Dovom et al. 2019, 7). Soft computing methods such as genetic algorithms help discover new and unknown malware by monitoring the behavior of programs and detecting patterns that signal harmful activity. It also aids in behavior monitoring through behavioral analysis. Thus, the latter is critical in the protection of patients' data against malicious software.

Finally, soft computing strategies help develop effective access control. Soft computing techniques improve access control mechanisms by developing intelligent systems that recognize user behavior patterns and detect anomalies that indicate unauthorized access. Access control helps prevent data breaches, ensuring only authorized people can access patient information. In general, the security of healthcare information technology systems might be significantly enhanced with the application of soft computing techniques.

Large Sample Data Collection is Essential in Cybersecurity for Several Reasons:

− Improving accuracy: large sample data collection allows for more accurate analysis and prediction of cybersecurity threats (Aurangzeb et al. 2022). A more extensive data set helps identify patterns and trends that may slip through with a smaller sample size;

− Identifying new threats: large sample data collection can help identify new, emerging, less visible threats (Aurangzeb et al. 2022). By analyzing a large volume of data, cybersecurity experts can detect patterns that indicate the presence of new types of malware or cyberattacks;

− Enhancing machine learning: machine learning algorithms require large data sets to be trained effectively (Aurangzeb et al. 2022). With more data, the algorithms can effectively and accurately detect cybersecurity threats;

− Supporting incident response: large sample data collection can provide valuable insights into how cyberattacks occur and how they can be prevented or mitigated (Aurangzeb et al. 2022). New insights are invaluable in developing incident response plans that are more effective against cyberattacks;

− Enabling threat intelligence sharing: large sample data collection can support sharing threat intelligence information between organizations (Aurangzeb et al. 2022).

Organizations can better prepare and defend against cyberattacks by sharing information on cybersecurity threats. Hence, Aurangzeb et al. (2022) reiterate that extensive sample data collection is essential in cybersecurity. It allows for more accurate analysis, identification of new threats, enhanced machine learning, improved incident response, and better threat intelligence sharing. Thus, cybersecurity experts can stay ahead of evolving threats and protect organizations from cyberattacks.

4. Summary – Potential Application

Soft computing techniques have the potential to contribute to preventing ransomware attacks in the following ways:

− Malware detection: soft computing techniques such as genetic algorithms and neural networks can detect new and unknown malware by analyzing programs behavior and identifying patterns that indicate malicious activity. Detection is critical in preventing ransomware's spread and protecting the victim's data.

− Anomaly detection: soft computing techniques find use in intelligent systems that can recognize user behavior patterns and anomalies that indicate a ransomware attack. Intelligent systems can help prevent ransomware from executing and encrypting the victim's data.

− Risk assessment: soft computing techniques are critical in assessing the risk of a ransomware attack and identifying vulnerabilities in the victim's system. Risk assessment helps in developing effective security strategies and appropriate resource allocation.

− Response planning: soft computing techniques help respond to ransomware attacks through backup and recovery plans, incident response plans, and communication plans. Response plans are critical in minimizing the damage and restoring the affected systems as soon as possible.

Conclusion

There is a growing adoption of technology across all sectors of national economies worldwide. While technology adoption increases workplace efficiency, they are prone to attacks. Cybersecurity has emerged as one of the greatest challenges facing governments and private sectors worldwide. The critical infrastructure such as the healthcare sector, is becoming the main target of cyberthreats such as ransomware attacks owing to the sensitive information in such sectors. Attacks on critical infrastructure can cripple essential services such as healthcare services, water provision, and electricity supply. Such attacks can be catastrophic to the society and may pose a threat to the national security. However, using large data samples, it is now possible to collect data on ransomware attacks and employ soft computing techniques such as fuzzy logic to detect and assess risks, and develop response plans to prevent ransomware attacks and its impacts.

BIBLIOGRAPHY:

Abaimov, Stanislav, and M. Martellini. 2022. *Machine Learning for Cyber Agents: Attack and Defence*. Cham, Switzerland: Springer.

Abbasi, Muhammad Shabbir, Harith Al-Sahaf, Masood Mansoori, and Ian Welch. 2022. "Behavior-Based Ransomware Classification: A Particle Swarm Optimisation Wrapper-Based Approach for Feature Selection."*Applied Soft Computing* 121 (March): 108744. https://doi.org/10.1016/j.asoc.2022.108744.

Abraham, Chon, Dave Chatterjee, and Ronald R. Sims. 2019. "Muddling Through Cybersecurity: Insights from the U.S. Healthcare Industry." *Business Horizons* 62 (4): 539–48. https .

Ahmed, Naeem, Rashid Amin, Hamza Aldabbas, Deepika Koundal, Bader Alouffi, and Tariq Shah. 2022. "Machine Learning Techniques for Spam Detection in Email and IoT Platforms: Analysis and Research Challenges." Edited by Wenjia Li. *Security and Communication Networks* 2022 (February): 1–19. https://doi.org/10.1155/2022/1862888.

Alqahtani, Abdullah, and Frederick T. Sheldon. 2022. "A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook." *Sensors* 22 (5): 1837. https://doi.org/10.3390/s22051837.

Alvarez, Michelle. 2017. "Security Trends in the Healthcare Industry: Data Theft and Ransomware Plague Healthcare Organizations." *IBM Security*. Somers, New York: IBM. ibm.com.

Aurangzeb, Sana, Haris Anwar, Muhammad Asif Naeem, and Muhammad Aleem. 2022. "BigRC-EML: Big-Data Based Ransomware Classification Using Ensemble Machine Learning." *Cluster Computing* 25 (March): 3405–22. https://doi.org/10.1007/s10586-022-03569-4.

Besenyő, János, Márton, Krisztina, & Shaffer, Ryan (2021). Hospital Attacks Since 9/11: An Analysis of Terrorism Targeting Healthcare Facilities and Workers. Studies in Conflict & Terrorism 2021, Studies in Conflict & Terrorism, 1-24. https://doi.org/10.1080/1057610X.2021.1937821.

Christiansen, Bryan, and Agnieszka Piekarz. 2019. *Global Cyber Security Labor Shortage and International Business Risk*. Hershey, Pennsylvania: IGI Global.

Dawn, Subhojit, Valentina Emilia Balas, Anna Esposito, and Sadhan Gope. 2020. *Intelligent Techniques and Applications in Science and Technology: Proceedings of the First International Conference on Innovations in Modern Science and Technology*. Cham, Switzerland: Springer International Publishing.

Dovom, Ensieh Modiri, Amin Azmoodeh, Ali Dehghantanha, David Ellis Newton, Reza M. Parizi, and Hadis Karimipour. 2019. "Fuzzy Pattern Tree for Edge Malware Detection and Categorization in IoT." *Journal of Systems Architecture* 97 (August): 1–7. https://doi.org/10.1016/j.sysarc.2019.01.017.

Dullea, Erik, Chris Budke, and Pete Enko. 2020. "Cybersecurity Update: Recent Ransomware Attacks against Healthcare Providers." *Missouri Medicine* 117 (6): 533–34. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7721413/.

Dutta, Nitul, Nilesh Jadav, Sudeep Tanwar, Hiren Kumar Deva Sarma, and Emil Pricop. 2021. "Introduction to Malware Analysis." *Studies in Computational Intelligence*, October, 129–41. https://doi.org/10.1007/978-981-16-6597-4_7.

Fields, Ziska. 2018. *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*. Hershey, Pennsylvania: IGI Global.

Filiz, Burak, Budi Arief, Orcun Cetin, and Julio Hernandez-Castro. 2021. "On the Effectiveness of Ransomware Decryption Tools." *Computers & Security* 111 (December): 102469. https://doi.org/10.1016/j.cose.2021.102469.

Gagneja, Kanwalinderjit K. 2017. "Knowing the Ransomware and Building Defense against It - Specific to Healthcare Institutes." *2017 Third International Conference on Mobile and Secure Services (MobiSecServ)*, February 1–5. https://doi.org/10.1109/MOBISECSERV.2017.7886569

Grini, Lars Strande, Andrii Shalaginov, and Katrin Franke. 2018. "Study of Soft Computing Methods for Large-Scale Multinomial Malware Types and Families Detection." *Recent Developments and the New Direction in Soft-Computing Foundations and Applications*, 337–50. https://doi.org/10.1007/978-3-030-47124-8.

Gupta, Brij B., ed. 2021. *Advances in Malware and Data-Driven Network Security*. IGI Global.

Hackett, Robert, 2016: "How One Health Care Organization Dodged the Ransomware Bullet." Fortune, May 7, 2016. https://fortune.com/2016/05/07/health-care-ransomware/.

Hariri-Ardebili, Mohammad Amin, Fernando Salazar, Farhad Pourkamali-Anaraki, Guido Mazzà, and Juan Mata. 2023. "Soft Computing and Machine Learning in Dam Engineering." *Water* 15 (5): 917. https://doi.org/10.3390/w15050917.

Hassan, Nihad A. 2019. *Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks*. New York, NY: Apress.

Hyett, Nerida, Amanda Kenny, and Virginia Dickson-Swift. 2014. "Methodology or Method? A Critical Review of Qualitative Case Study Reports." *International Journal of Qualitative Studies on Health and Well-Being* 9 (1): 23606. https://doi.org/10.3402/qhw.v9.23606.

Information Resources Management Association. 2021. *Research Anthology on Artificial Intelligence Applications in Security*. Hershey, Pennsylvania: IGI Global.

Khoda, Mahbub E., Joarder Kamruzzaman, Iqbal Gondal, Tasadduq Imam, and Ashfaqur Rahman. 2021. "Malware Detection in Edge Devices with Fuzzy Oversampling and Dynamic Class Weighting." *Applied Soft Computing* 112 (November): 107783. https://doi.org/10.1016/j.asoc.2021.107783.

King, Steve. 2022. Losing the Cybersecurity War, CRC Press. Kovács, A. M. 2022. "Ransomware: A Comprehensive Study of the Exponentially Increasing Cybersecurity Threat." *Insights into Regional Development* 4 (2): 96–104. https://doi.org/10.9770/IRD.2022.4.2(8).

Kumar, Raghvendra, Nguyen Ho Quang, Vijender Kumar Solanki, Manuel Cardona, and Prasant Kumar Pattnaik. 2021. *Research in Intelligent and Computing in Engineering*. Cham, Switzerland: Springer Nature.

Lee, Kyungroul, Jaehyuk Lee, and Kangbin Yim. 2023. "Classification and Analysis of Malicious Code Detection Techniques Based on the APT Attack." *Applied Sciences* 13 (5): 2023, 13, 2894. https://doi.org/10.3390/app13052894.

Mishra, Debesh, Suchismita Satapathy, and Prasenjit Chatterjee. 2022. *Soft Computing and Optimization Techniques for Sustainable Agriculture*. India: Walter de Gruyter GmbH & Co KG.

Moallem, Abbas. 2020. HCI for Cybersecurity, Privacy and Trust, 1st edn, Springer Nature. Modlin, Amber and Gregory, Andrew and Odebode, Iyanuoluwa and Hodson, Douglas and Grimaila, Michael. (2021). CovidLock Attack Simulation. https://doi.org/10.1007/978-3-030-69984-0_3. In: Arabnia, Hamid R. 2021. *Advances in Parallel and Distributed Processing, and Applications: Advances in Parallel & Distributed Processing, and Applications: Proceedings from PDPTA'20, CSC'20, MSV'20, and GCC'20*. Cham, Switzerland: Springer Nature. 25-34. https://doi.org/10.1007/978-3-030-69984-0

Mohammad, Adel Hamdan. 2020. "Ransomware Evolution, Growth and Recommendation for Detection." *Modern Applied Science* 14 (3): 68–74. https://doi.org/10.5539/mas.v14n3p68.

Mookherjee, Somnath, Lauren A. Beste, Jared W. Klein, and Jennifer Wright. 2020. *Photography in Clinical Medicine*. Cham, Switzerland: Springer.

Nikki, Spence, Bhardwaj Niharika, Paul David, and Coustasse Alberto. 2018. "Ransomware in Healthcare Facilities: A Harbinger of the Future?" *Perspectives in Health Information Management; Chicago*, 1–22.

Pathak, Vibha, Sanjay Kalra, and Bijayini Jena. 2013. "Qualitative Research." *Perspectives in Clinical Research* 4 (3): 192. https://doi.org/10.4103/2229-3485.115389.

Rubin, Allen, and E. R. Babbie. 2016. *Essential Research Methods for Social Work*. 4th ed. Boston, MA: Cengage Learning.

Sathesh, A. 2019. "Enhanced Soft Computing Approaches for Intrusion Detection Schemes in Social Media Networks." *Journal of Soft Computing Paradigm* 2019 (2): 69–79. https://doi.org/10.36548/jscp.2019.2.002.

Sharma, Arushi, Ekta Gandotra, Divya Bansal, and Deepak Gupta. 2019. "Malware Capability Assessment Using Fuzzy Logic." *Cybernetics and Systems* 50 (4): 323–38. https://doi.org/10.1080/01969722.2018.1552906.

Shin, Yung C., and Chengying Xu. 2017. *Intelligent Systems: Modeling, Optimization, and Control*. New York, NY: CRC Press.

Singh, Hardeep and Sittig, Dean. 2016. 'A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks', Applied Clinical Informatics, vol. 07, no. 02, pp. 624–632. Slayton, Thomas B. 2018. "Ransomware: The Virus Attacking the Healthcare Industry." *Journal of Legal Medicine* 38 (2): 287–311. https://doi.org/10.1080/01947648.2018.1473186.

Thamer, Noor, and Raaid Alubady. 2021. "A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research." *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*, April, 210–16. https://doi.org/10.1109/bicits51482.2021.9509877.

The DoD Cyber Exchange. 2020. "Cybersecurity Awareness Month – DoD Cyber Exchange." Public.cyber.mil. 2020. https://public.cyber.mil/cybersecurity-awareness-month/.

Tully, Jeff, Jordan Selzer, James P. Phillips, Patrick O'Connor, and Christian Dameff. 2020. "Healthcare Challenges in the Era of Cybersecurity." *Health Security* 18 (3): 228–31. https://doi.org/10.1089/hs.2019.0123.

Winton, Richard. 2016. "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating." Los Angeles Times, February 18, 2016. https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

Yuryna Connolly, Lena, David S. Wall, Michael Lang, and Bruce Oddson. 2020. "An Empirical Study of Ransomware Attacks on Organizations: An Assessment of Severity and Salient Factors Affecting Vulnerability." *Journal of Cybersecurity* 6 (1): 1–18. https://doi.org/10.1093/cybsec/tyaa023.

Zetter, Kim, 2016. "Why Hospitals Are the Perfect Targets for Ransomware." March 30, 2016, Wired, . https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets.

Zhang, Nan, Yu-an Tan, Chen Yang, and Yuanzhang Li. 2021. "Deep Learning Feature Exploration for Android Malware Detection." *Applied Soft Computing* 102 (January): 107069. https://doi.org/10.1016/j.asoc.2020.107069.

Appendix 1:
Critical Infrastructure Cyber-Attack Incidents' International Sample, 2011-2012

Year	Industry Type	Attack Description	Country	Attack Details
2011	Water and Wastewater Systems	Greenfield Wastewater Treatment Plant intentionally shut down critical systems	United States	SCADA/control systems were intentionally shut down, preventing current wastewater operations from continuing; the tampering of the original security systems and their displayed conditions existed until the start of the backup security systems.
2011	Healthcare and Public Health	Hacker froze operations at pharmaceutical company	United States	Jason Cornish, a former IT employee of Shionogi, Inc. , gained unauthorized access to the computer network. Cornish used a Shiongi user account to access a company server.
2011	Transportation Systems	Computer Glitch Causes Ride Shutdown	United States	The computer systems on the Skywheel ride were not communicating with each other resulting in an error message that stopped the wheel from spinning. The ride was shut down for 17 hours. Passengers were unloaded safely.
2011	Energy	Circuit card shuts down nuclear plant	United States	The Watts Bar Nuclear Plant's Unit 1 reactor shut down. A malfunction in a circuit card on a newly installed computer system that assists the operation of the plant's turbine. The malfunction caused the turbine to trip causing the reactor to shut down.
2011	Transportation Systems	Control system failure causes bridge delays	Guyana	Problems with the bridge control system while opening and closing the bridge resulted in delays for motorists. The bridge typically closes for 90 minutes each day, but the control system problem caused a two-hour delay.
2011	Transportation Systems	Computer glitch causes delayed and canceled flights	United States	The computer glitch resulted in 36 canceled flights and about 100 delayed flights.
2011	Transportation Systems	Computer glitch causes BART train service shutdown	United States	The Bay Area Rapid Transit (BART) system was shut down for about 4 hours due to a computer glitch.
2011	Transportation Systems	Malware a Factor in Spanair Plane Crash	Spain	A Trojan infected computer may not have detected three technical issues that caused the plane to crash shortly after take-off. The crash resulted in the death of 154 passengers. Eighteen passengers survived.
2011	Water and Wastewater Systems	Water Utility Hack Destroys Pump	United States	The control system of the city water utility in Springfield, Illinois was hacked. Hackers gained remote access to the control system causing the system to turn on and off repeatedly leading to the burnout of a water pump.
2012	Water and Wastewater Systems	Wastewater Treatment District Hacked	United States	The former chief financial officer of the Key Largo Wastewater Treatment Distict, Salvatore Zappulla, has been arrested and charged with hacking the district's computer system.
2012	Water and Wastewater Systems	Computer Malfunction Blamed for Major Sewage Spill	United States	A major sewage spill occurred sending 2 million gallons of raw sewage into the Tijuana River. A programmable logic controller failed shutting down pumps and controls.
2012	Critical Infrastructure	Auto Manufacturer Hacked	United States	A computer virus was detected on the network of an automanufacturer. Unknown attackers stole employees' IDs and encrypted passwords after planting a computer virus on the company's computer systems.
2012	Petroleum	Iranian Oil Terminal offline after malware attack	Iran	Iran has been forced to disconnect key oil facilities after suffering a malware attack. The computer virus is believed to have hit the internal computer systems at Iran's oil ministry and its national oil company.
2012	Transportation Systems	Computer Glitch Stops Trains	Philippines	A computer glitch cause the Light Rail Transit Line 2 to stop. The line was down for 30 minutes.
2012	Transportation Systems	Cascade of Computer Crashes Causes Metro System Shutdown	United States	A computer problem caused the shut down of the Montreal metro system for about an hour. The problem started when a computer failure caused a shutdown on the orange line.
2012	Petroleum	Computer Virus Targets Saudi Arabian Oil Company	Saudi Arabia	Saudi Arabia's national oil company, Aramco, said that a cyber attack damaged approximately, 30,000 computers. The attack was aimed at stopping oil and gas production in Saudi Arabia. The company shut down its main internal network for more than a week.
2012	Energy	Computer Glitch Leads to Shutdown of Nuclear Reactor	United States	One of the two nuclear reactors at the Susquehanna Nuclear Powerplant was shut down because a computer system that controls the reactor's water level was not functioning properly.
2012	Petroleum	Shamoon virus knocks out computers at Qatari gas firm RasGas	Qatar	RasGas, the second largest producer of liquified natural gas in the world, was attacked by the Shamoon virus about 2 weeks after a similar attack on Saudi Aramco.

Appendix 2:
Sample of Ransomware Attacks Reported in the Healthcare Sector, 2015-2017

Primary CI Sector targeted	Year	Organization	Location	Modus operandi information	Duration (days, unless specified)	Ransom
Healthcare and Public Health	2015	Christopher Rural Health	USA		2	hundreds of dollars
Healthcare and Public Health	2015	The Arc of Winnebago, Boone and Ogle Counties	USA	CryptoWall	3	$1,400
Healthcare and Public Health	2016	Titus Regional Medical Center	USA		10	
Healthcare and Public Health	2016	Hollywood Presbyterian Medical Center	USA		10	$17,000
Healthcare and Public Health	2016	Lukas Hospital in Germany	Germany		weeks	
Healthcare and Public Health	2016	Klinikum Arnsberg hospital	Germany		1	
Healthcare and Public Health	2016	Los Angeles County Health Department	USA			
Healthcare and Public Health	2016	The Ottawa Hospital	Canada			
Healthcare and Public Health	2016	Henderson Methodist Hospital	USA	Locky	3	$1,600
Healthcare and Public Health	2016	Prime Healthcare Services	USA		days	$17,000
Healthcare and Public Health	2016	MedStar Health Baltimore	USA	Samsam	5	$1,250 - $18,500
Healthcare and Public Health	2016	DeKalb Health Auburn	USA		1-2 weeks	
Healthcare and Public Health	2016	Kansas Heart Hospital	USA		6	
Healthcare and Public Health	2016	Urgent Care Clinic of Oxford	USA			
Healthcare and Public Health	2016	University Gastroenterology	USA			
Healthcare and Public Health	2016	Marin General Healthcare District and Prima Medical Group	USA		1-2 weeks + permanent data loss	
Healthcare and Public Health	2016	New Jersey Spine Center	USA			
Healthcare and Public Health	2016	Keck Medicine	USA			
Healthcare and Public Health	2016	Rainbow Children's Clinic	USA		Unspecified some data never recovered	
Healthcare and Public Health	2016	Appalachian Regional Healthcare	USA		3 weeks	
Healthcare and Public Health	2016	Saint Francis Health System	USA			$14,400
Healthcare and Public Health	2016	Northern Lincolnshire & Goole NHS Foundation Trust	United Kingdom			
Healthcare and Public Health	2016	ARCare	USA		31 hours	about $1,500
Healthcare and Public Health	2017	Erie County Medical Center	USA		5 weeks	$44,000
Healthcare and Public Health	2017	National Health Service (NHS) UK	United Kingdom	WannaCry	3 days	
Healthcare and Public Health	2017	NHS Lanarkshire board hospitals	Scotland	BitPaymer	4	
Healthcare and Public Health	2017	Emory Healthcare	USA		year(s)	about $2,700
Healthcare and Public Health	2018	Hancock Health	USA	Samsam	4 days	$45,000-55,000
Healthcare and Public Health	2018	Adams Memorial Hospital, Indiana	USA			
Healthcare and Public Health	2018	Allscripts Healthcare Solutions, Inc.	USA	Samsam		
Healthcare and Public Health	2018	MN Associates in Psychiatry and Psychology	USA	TripleM		about $27000
Healthcare and Public Health	2018	Blue Springs Family Care	USA			
Healthcare and Public Health	2018	LabCorp	USA	Samsam	1 week	
Healthcare and Public Health	2018	Thundermist Health Center	USA			

Appendix tables' sources, also included in Bibliography:

https://fortune.com/2016/05/07/health-care-ransomware/ (Hackett, 2016)

https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html (Winton, 2016)

https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/ (Zetter, 2016)