5-2023

A SYSTEMATIC LITERATURE REVIEW OF RANSOMWARE ATTACKS IN HEALTHCARE

Jasler Klien Adlaon

A SYSTEMATIC LITERATURE REVIEW OF RANSOMWARE ATTACKS IN HEALTHCARE

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology

by

Jasler Klien Adlaon

May 2023

A SYSTEMATIC LITERATURE REVIEW OF RANSOMWARE ATTACKS IN HEALTHCARE

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Jasler Klien Adlaon

May 2023

Approved by:

Dr. Benjamin Berrcera, , Committee Chair

Dr. Conrad Shayo, Committee Member, Chair of Department of Information and Decision Sciences

ABSTRACT

This culminating experience project conducted a Systematic Literature Review of ransomware in the healthcare industry. Due to COVID-19, there has been an increase in ransomware attacks that took healthcare by surprise. Although ransomware is a common attack, the current healthcare infrastructure and security mechanisms could not suppress these attacks. This project identifies peer-viewed literature to answer these research questions: “What current ransomware attacks are used in healthcare systems? “What ransomware attacks are likely to appear in the future?” and “What solutions or methods have been used to prepare, prevent, and recover from these attacks?” The purpose of this research is to identify a possible increasing trend of seeing ransomware in the future and to see what technologies are used to combat these attacks. The findings focus on three solutions, artificial intelligence (AI), machine learning (ML), and blockchain as there can be many solutions that could have been included. Because the healthcare industry has many different types of systems involved, limitations of the research are solutions suggested being other studies may not work with other studies. For future study, indicating a specific type of healthcare organization may be recommended and will have better result.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE:

INTRODUCTION

Background of Study

Ransomware, in a global aspect, is responsible for the extortion of billions of dollars from American citizens and companies annually (Porath, 2023). This threat not only skyrocketed during COVID-19 but continues to increase over the years. While ransomware has been a common issue across many organizations, healthcare industries have specifically experienced an increase in these attacks. Another study indicates an increase in internet users in 2020 is ten percent higher than data collected in 2019 (Awaludin et al., 2023). Several research studies have documented various causes and reasons for this increase with the following observations. A study observed ransomware attacks have made medical staff and employees' resort to traditional pen and paper methods to monitor patient status (ELGawish et al., 2022). Various cybersecurity approaches have appeared due to COVID-19 and traditional approaches where it's focused on "static control of security equipment or work in reaction to an attack" no longer are effective with the rapid increase of attacks (Kadel et al., 2022). Current methods of healthcare systems are associated with connection to the Internet which allows telecare, telemedicine, remote diagnosis, and even telework to exist (Alabdulatif et al., 2022).

Another study explains the coverage of ransomware attacks within healthcare systems as "there are no systematic documentation of the extent and

effects of ransomware attacks," indicating that the technology and knowledge of healthcare systems are still subpar in comparison to ransomware attackers (Neprash et al., 2022). Two major reasons, as shown by various studies, are the introduction of telecommuting work (also known as remote work) and the lack of implications of proper remote security. To further elaborate, a study conducted in 2022 concluded the amount volume of malware to have an average of 419 threats per minute, which is a 12% increase in the second quarter of 2020 (Kadel et al., 2022). Moreover, the 2020 Remote Workforce Cybersecurity Report reported a two-thirds increase in breach reports with the healthcare industries shift to telework.

Because there many research studies shown about ransomware and the effects it has to organizations, particularly healthcare industries, an exploratory analysis published in 2022 about electronic health records and cybersecurity breaches show the dangers of current ransomware methods (Yeo & Banfield, 2022). Healthcare data breaches are considered to have the highest cost of data breaches compared to any other type of industry when adding costs to incident response, lost business, and notification costs (Yeo & Banfield, 2022). The study by Yeo & Banfield (2022), also found that COVID-19 has increased the amount of electronic health records going into healthcare systems which human capabilities with the current knowledge of their systems could not handle, which, in this study, explains the lack of subject matter experts (SME) about security are causes of these incidents occurring. Though this problem is only one of many

causes of the increase of ransomware attacks in healthcare systems, research by other scholars have found additional causes.

As ransomware attacks became more commonly seen in healthcare, its technology and methods have become increasingly more sophisticated in recent years (Porath, 2023). With the evolution of ransomware technology, characteristics and detections have become more difficult to detect and cybercriminals are leveraging this due to the rapid changes that are occurring in healthcare (Porath, 2023). Attempting to find mitigation for this when there are many services, research, applications, vendors, etc., is difficult to say when healthcare systems have different ways it processes and stores its data, different standard protocols it follows, and different solutions it uses in comparison to another system (Gopinath & Olmsted, 2022). With much ongoing research and observations of ransomware, there is no concrete evidence of its evolution and capabilities in the future. This culminating experience project will critically examine existing research studies about ransomware attacks in healthcare in hopes to answer these questions:

1. What current ransomware attacks are used in healthcare systems?
2. What ransomware attacks are likely to appear in the future?
3. What solutions or methods have been used to prepare, prevent, and recover from these types of attacks?

Organization

This project is organized as follows: Chapter two will provide a literature review to give background of the topics discussed. Chapter three will introduce the methodology of a systematic review to analyze ransomware in healthcare. Chapter four will dive into the given solutions of mitigation, detection, and preparation methods. Chapter five will provide a conclusion and summarization.

CHAPTER TWO

LITERATURE REVIEW

Chapter Two will discuss the literature utilized in this culminating project. The literature spotlights knowledge gaps for discussion and terminologies seen in later chapters. This will provide background of researchers' observations that correlate to the research questions posed in Chapter One.

Ransomware

The current state that ransomware technology and methodology has grown sophisticated enough to where the limits and impact within healthcare systems are unknown. One research study, driven to answer the occurrence of ransomware, has created a data source called Tracking Healthcare Ransomware Events and Traits (THREAT) to analyze ransomware events from news outlet, trade publications, forums on the dark web, corporate cybersecurity breaches, etc. (Neprash et al., 2022). Furthermore, the collection and data gathered within THREAT supplemented the group to statistically calculate the number of health care delivery organizations which resulted in an increased trend of ransomware attacks from 2016-2021.

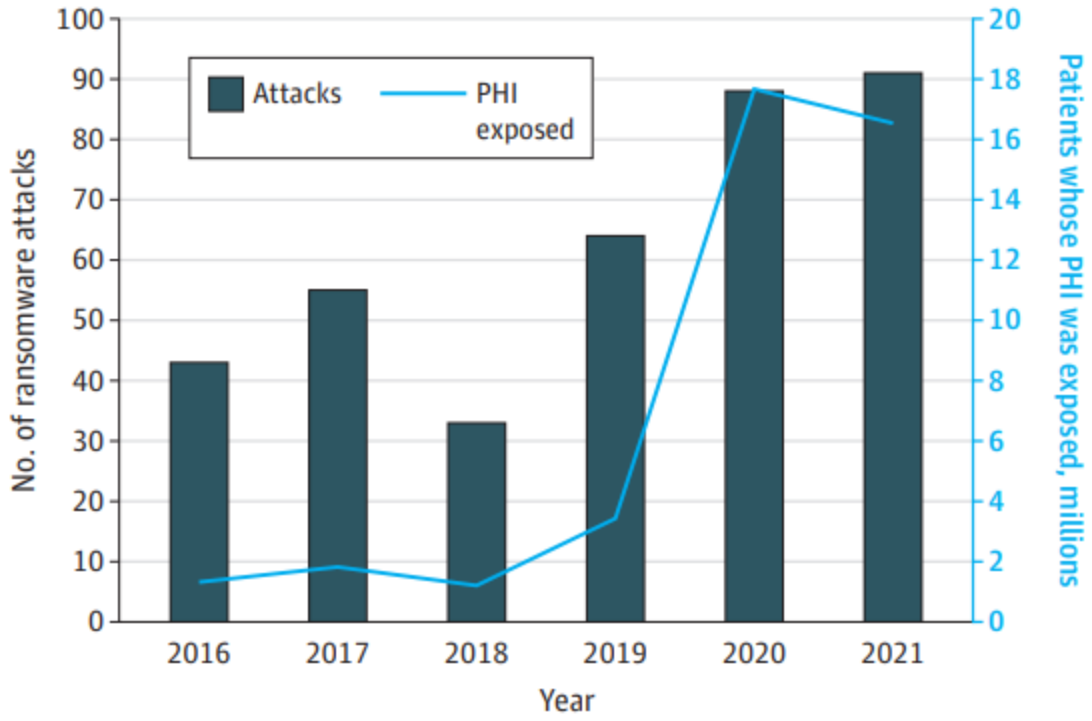

Figure 1. Number of Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Service Delivery Organizations, 2016-2021

Though the THREAT database provided solid evidence of an increasing trend of ransomware attacks, the research only searched the frequency of the occurrence but not detailed the types of ransomware attacks used and detailed information of which healthcare systems were primary targets. Neprash et.al (2022) that stated their statistical report may likely underestimate the data due to underreporting and other information that were not tracked in THREAT may have potentially helped the research out even further.

Ransomware Types

There have been commonly known forms of ransomware, however, introduction to new and more dangerous iterations are soon to be determined. Relevant to the scope of the research, three ransomware types will be highlighted: Crypto Ransomware, Locker Ransomware, and Doxware

Crypto Ransomware (Cryptoware). Crypto ransomware, also known as Cryptoware, is the newer iteration of ransomware where it has enabled criminals to encrypt the victim's files. Unencrypting these files was functionally impossible, according to law enforcement's perspective, due to the ransomware attaching itself to what was called "unstructured data" within the computer (Porath, 2023). Such "unstructured data" were PDFs, photos, Word and Excel files, and other individualized data and files. Another study conducted by Thamer and Alubady, observed that this type of ransomware did not completely target the hard disk, but complemented Porath's statement of "unstructured data." (Thamer & Alubady, 2021). There are two common types of encryption methods used in Cryptoware, symmetric and asymmetric encryption which both involve the use of encryption keys to decrypt its data. Common names that are used to address Cryptoware are CryptoLocker, TeslaCrypt, and CryptoWall (Kumar et al., 2021). Moreover, this type of ransomware is just one of the three types that are commonly seen in healthcare systems.

Locker Ransomware. Locker Ransomware is another iteration of Ransomware which involved the use of WinLocker and Master Boot applications to execute the attack. This type of ransomware shuts down the victim's computer so that the original user cannot access it anymore (Thamer & Alubady, 2021). In addition, the blocked victim could not access using the computer, its interface, and files that were in it (Porath, 2023). Furthermore, locker ransomware did not alter or access the files, instead it merely added a new lock to a computer, so initial users were denied access. Because it did not target accessing files, victims usually paid ransomware to recover their contents, until experts figured out a way to bypass the new lock it created. Though this type of ransomware still exists today, more sophisticated, and problematic versions of ransomware are deployed (Porath, 2023). Despite locker ransomware is not as advanced as doxware or even Cryptoware, experiences of this type can be used.

Doxware. An emerging type of ransomware where 81% ransomware attacks during the second quarter of 2021 were Doxware (Porath, 2023). Furthermore, this ransomware attack is more of the hazardous type as it can proliferate and share personal information online (Bertia et.al., 2022). Doxware, sharing similar characteristics as Cryptoware and locker ransomware, is a reason why cybercriminals have increasingly used this type of ransomware attacks. Attacking personal information in addition to encrypting and locking out a user has created a weakness in which victims feel like they do not have a choice but pay the

ransom. However, possibilities of new iterations of this ransomware may arise soon, cyber specialists and other researchers have diligently come up with various solutions to combat the attacks.

Artificial Intelligence (AI)

The emergence of Artificial Intelligence or AI helps develop better security posture within healthcare systems. Problems arise due to the vast number of attacks happening in a rapid succession rendering human efforts ineffective and time consuming. AI implementation solving these types of attacks allows healthcare organization opportunities to identify and recover from threats (Kadel et. al., 2022). Kadel et.al. (2022) observes that AI can help with cybersecurity and defense in such that AI capabilities may interconnect with other technologies such as machine learning and blockchain. A specific example to healthcare explained by the study, is AI helping with online virtual health assistance to help patients with commons needs such as schedule appointments, understanding billing process, and other administrative processes. Though the traditional security controls done by humans still are recommended, the hesitancy of the use and trust of autonomous response systems are still in question.

Machine Learning

Traditional healthcare systems were mainly managed by administrators and the swift to machine learning lessens the burden of those tasks. Due to more sophisticated attacks used more commonly, Intrusion Detection Systems (IDS)

were able to keep up using abnormal network behaviors over machine learning methods (Kumar et. al., 2022). Elgawish et. al. conducted a study to measure the capabilities of machine learning and deep learning techniques and the accuracy of detecting ransomware payload. However, due to the restriction of inaccessible information such as HIPAA or DUA related information, the study is limited to published dataset. The deployment of machine learning has also reached applications and services used in healthcare systems. For example, antivirus applications moved off from the traditional signature-based detection and started implementing machine learning detection to provide improved security measures.

Blockchain

Deployment of blockchain efforts in healthcare systems have been growing due to the importance of more sophisticated attacks with the lack of advanced security controls. Kumar et.al conducted a research study to create a framework for a more advanced blockchain solution to secure data transmission in IoT-enabled healthcare system called BDSDT, also known as Blockchain-orchestrated Deep learning approach for Secure Data Transmission. The purpose use of this research study is to bring awareness of many solutions for preventing attacks and securing healthcare data. Preserving privacy in healthcare systems is a priority as patient data is a valuable target for cybercriminals to attack. Blockchain prevents this by facilitating trust and data privacy (Alkadi et.al., 2020). With blockchain, data transmission is considered secure and trustworthy in IoT-enabled healthcare systems (Kumar et.al., 2022).

Additionally, using the BDSDT framework, current findings show that this framework outperforms competing strategies in both blockchain and non-blockchain settings. Using Kumar's et. al. research provides a brief overview of the importance of blockchain technology and its role to securing healthcare systems.

CHAPTER THREE:

METHODOLOGY

Chapter Three will discuss the methodology that is used to gather data as well as how the data was selected. To answer the research questions in Chapter One, the Preferred Reporting Items for Systematic reviews and Meta-Analyses, also abbreviated as PRISMA, 2020 statement was used. Page et.al. has updated the previous version of PRISMA, which was published in 2009, to include more valuable information, updated reporting guidelines, revised flow diagrams, and more (Page et al., 2021). The PRISMA 2020 statement was chosen to be the primary methodology for this research due to its design for evaluating a multitude of similar studies and collaborating them into a single research study. As a result, this chapter will demonstrate the full conduct of the systematic review.

Selection of Primary Studies

Selected primary studies were based on deriving specific keywords to various search facilities and search engines. The keywords were selected based on the research results needed to support the given research questions. For the search to begin Boolean operators and search strings were created to restrict the searches being seen. In this study, Boolean operators used were AND and OR with the search string of:

(ransomware OR ransom ware OR ransom-ware OR "ransom malware") AND (healthcare OR health care OR health-care) AND (artificial intelligence OR "machine learning" OR blockchain)

With this search string, it searches all variations of spelling of ransomware and healthcare while at least including one of the three other keywords, artificial intelligence, machine learning, or blockchain. This search string was used in the following platforms:

- Google Scholar
- IEEE Xplore Digital Library
- Business Source Premier
- Web Of Science
- Ebsco Host

Each of the platforms were searched with the following metrics: the title, keywords and abstract. The searches were conducted 17 March 2023 with the search range between the years 2019 to early January 2023. These results were conducted with inclusion/exclusion criteria specific to answering the research questions mentioned in Chapter 1. Using the criteria a set of results were ran through the snowballing process described by Wohlin (Wohlin, 2014). However,

discussion of the details of the inclusion and exclusion criteria will be shown in the next section.

Inclusion and Exclusion Criteria

Studies that are selected in this SLR went through an inclusion and exclusion criteria to make sure all studies reported with empirical data, showcase ransomware and healthcare related information and current and future solutions dealing with ransomware attacks. They must be peer-reviewed and written in English. If there were a recent version of a study, their most recent and updated version will be selected. Because Google Scholar was used as a platform for searching studies, selected studies were verified to make sure that they were credible and heavily looked against the inclusion and exclusion criteria. Table 1 below details the specific inclusion and exclusion criteria in the primary selection process.

Table 1. Inclusion and Exclusion Criteria for Primary Studies

Criteria for Inclusion	Criteria for Exclusion
The paper must be a peer-reviewed product published in a conference proceeding or journal.	Papers written in other languages.
The paper must contain information related to ransomware, healthcare, and at least one of the following: artificial intelligence, machine learning, and blockchain technologies.	Blogs, books, and other quick read-related documents
The paper must present empirical data related to the topic.	

Selection Results

There was a total of 1539 studies from the initial keyword searches on the selected platforms. It was reduced to 1292 after removing duplicate studies. Studies were run through the inclusion and exclusion criteria yielding the number of papers to 48 based on the title and abstract. These 48 papers were then read in full with the inclusion and exclusion criteria being reapplied, of which 26 papers remained. Forward and backward snowballing identified an addition 2 and 2 papers respectively, giving a final total for the number of papers to be included in this SLR.

Quality Assessment

A quality assessment was tested against the studies that were in the primary studies selection process. Due to this assessment, it allowed the

selection to be more accurate based on the relevance of the targeted research questions, but also ruled out any signs of bias and other factors that may have caused the selection of certain studies to be included in.

Stage 1: **Healthcare.** The paper must be focused on healthcare that is well-commented to a specific problem.

Stage 2: **Ransomware.** The paper must address the ransomware issue with support of the target focus of a healthcare area.

Stage 3: **Context.** Enough context must be provided to address research objectives and findings. This will allow for an accurate reading to be interpreted of that research.

Stage 4: **Machine Learning, Blockchain, Artificial Intelligence application.** There must be at least one of the following details mentioned above to see how the technology is applied to a specific problem which will assist RQ1 & background of RQ2.

Stage 5: **Security context.** The paper must provide an explanation for the security problem, to assist in answering RQ3.

Stage 6: **Machine Learning, Blockchain, Artificial Intelligence performance.** Assess and analyze the performance of the technologies used in the environment to identify which areas of healthcare are covered and which are not.

Stage 7: **Data acquisition**. Details about how the data was acquired, measured, and reported must be given to determine accuracy.

This quality assessment checklist was applied to all primary studies identified. Based on the checklist, 6 studies did not meet one or more of the checklist items and therefore were removed from the SLR, as shown in Table 2.

Table 2: Excluded Studies.

Checklist for the Criteria Stages	Excluded Studies
Stage 1: Healthcare	
Stage 2: Ransomware	
Stage 3: Context	
Stage 4: Machine Learning, Blockchain, AI	[25] [26]
Stage 5: Security Context	[13]
Stage 6: Machine Learning, Blockchain, AI Performance	
Stage 7: Data Acquisition	[6] [9] [10]

Data Extraction

All studies that have passed the quality assessment underwent assessment in their data quality. Each study was categorized and illustrated on a spreadsheet. The categorized given to the data were as follows:

Context data: Purposeful information of the study

Qualitative data: Findings and conclusions provided by the authors.

Quantitative data: Applications to the study that involved their data set, experimentation, and research.

Figure 2. shows stages of the number of papers that were selected and how it concluded the attrition rate of papers from the initial keyword searches on each platform down to the final selection of the selected primary studies.

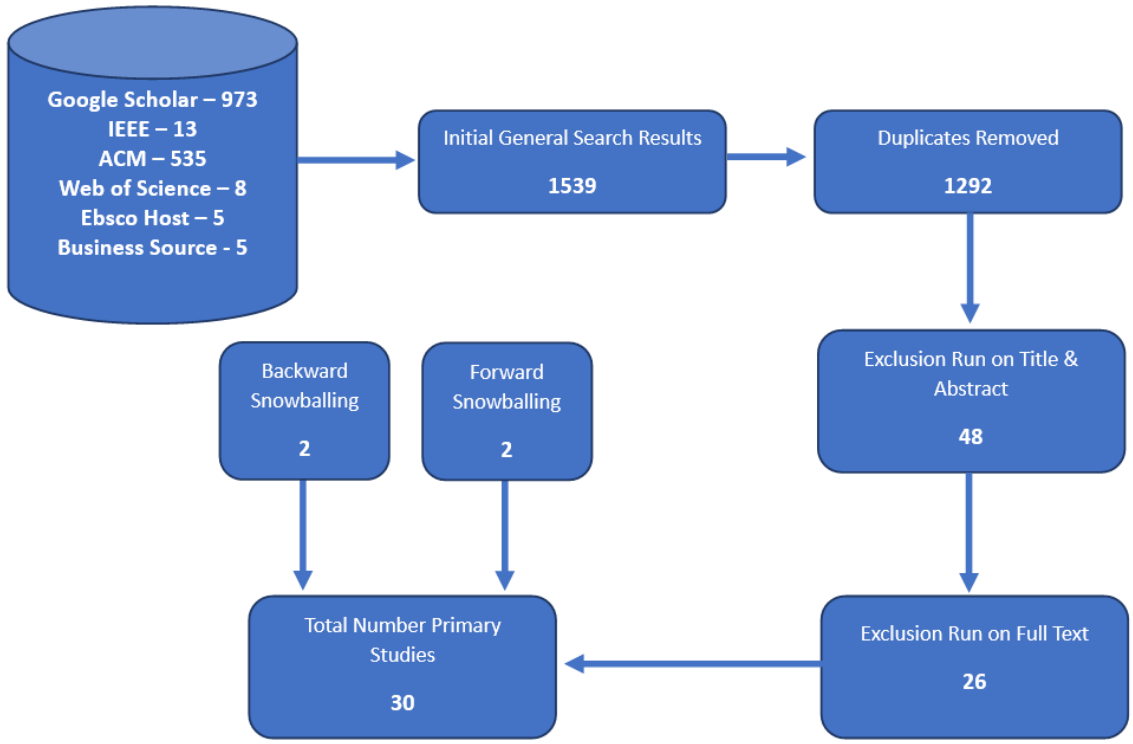

Figure 2. Attrition of Papers Through Processing

Publications Over Time

Although the “Selection of Primary Studies” briefly mentions the date range used in this SLR, further details of the selected timeframe will be done here. Ransomware within healthcare was not a new threat to begin with, but the impact of COVID-19 gave rise to an increase in it. The timeframe selection was done over a five-year gap starting from 2023 to 2019. Though there could be more studies done later in the year, the selection is relevant in understanding the current technologies used. Figure 3 is a chart showing the number of primary studies published in this five-year period.

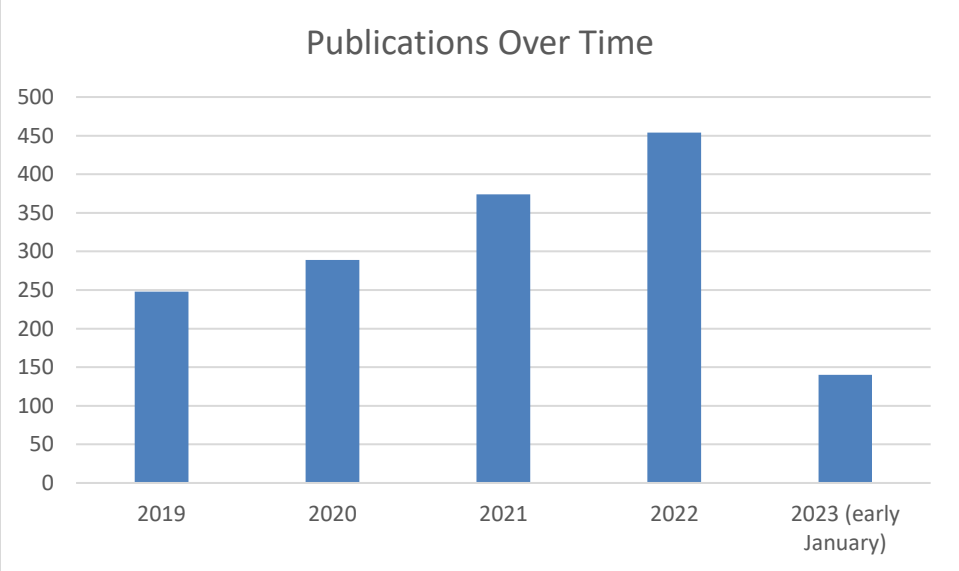

Figure 3. Number of Primary Studies Published Over Time.

As seen in the chart above, there is an increasing trend of publications that deal with ransomware attacks in healthcare. By the end of 2023 there will be a likelihood that the overall publications of 2022 will be surpassed.

Significant Keyword Counts

Another analysis was performed to summarize the common themes amongst the selected primary studies. Each study was searched by using keywords within the research questions such as: “prevent,” “solution,” “mitigation,” etc. with the some of the quality assessment stages such as: “healthcare,” “ransomware,” “blockchain,” “AI,” etc. to find what themes were likely to appear. Table 3 shows the number of times these specific words appeared in all the primary studies.

Table 3. Total Count of the Specific Keywords Shown in Each Primary Study.

Keywords	Count
system	3174
healthcare	2986
ransomware	1759
blockchain	1442
technology	657
solution	528
AI	190
machine learning	184
mitigation	142
prevent	139

As shown in the table above, excluding the keyword “system,” “healthcare,” “ransomware,” and “blockchain” were shown as a common theme. This indicates that all primary studies are relevant to ransomware in healthcare as well as implementation of blockchain technology.

CHAPTER FOUR

FINDINGS

This chapter will cover the findings that were found through the SLR process conducted in Chapter 3. Each primary study was thoroughly analyzed to understand each study's contribution towards answering the research questions for this study. Furthermore, the studies included in this SLR were categorized, summarized, and grouped for the understanding of their relevance towards this study.

Main Findings and Their Themes

Table 4 highlights all the included primary studies that passed the quality assessment and criteria in Chapter 3. Each of the primary studies were then put on this table to visually organize their key qualitative and quantitative data. Each study were then categorized based on the type of security application or technology that they focused on.

Table 4. Main Findings and Themes of the Primary Studies

Primary Study	Key Qualitative & Quantitative Data Reported	Types of Security Applications
[S1]	In-depth take of current cybersecurity architecture in healthcare. Analyzes and synthesizes existing reviews to identify challenges, limitations, threats, attacks that belong to the healthcare environment.	IoT, Big Data, Blockchain, AI
[S2]	Comprehensive examination of ransomware evolution and traditional ransomware detection. Highlights recent detection techniques and addresses the need of ML solution.	ML
[S3]	Classifies blockchain, machine learning, and SDN technology solutions used within healthcare. Provides scientific benefits to researchers in IT, health institutions, and security companies.	Blockchain, ML, & SDN
[S4]	Analyzes healthcare threats and their impacts and security measures with their limitations [S1].	IoT
[S5]	Healthcare 4.0 has integrated many new technologies that provided benefits to healthcare quality. Various new technologies such as implantable medical devices (IMDs), body are networks (BANs), implantable and wearable medical devices (IWMDs), have both improved care but immobilized new threats.	IoT
[S7]	Development of an AI-powered hybrid approach to overcome challenges in detecting ransomware. AIRaD (AI-based Ransomware Detection) uses behavioral chaining to detect multiple ransomware families in which is used to reverse engineer to extract features to create profiles.	AI
[S8]	Creating an Application Programming Interface (API)-based ransomware detection approach in combination with machine learning. Analysis using this combination yielded a 99.18% detection accuracy for Windows-based platforms.	ML
[S11]	Proposed a new ransomware countermeasure called Blockchain-enabled Security Framework to detect and defend the ransomware attacks for Smart Healthcare (BSFR-SH). BSFR-SH can create backups, data collection and signature generation, ransomware detection and analysis, and data recovery.	Blockchain

Table 4. (continued)

Primary Study	Key Qualitative & Quantitative Data Reported	Types of Security Applications
[S12]	Detailed study of IPFS and Blockchain's architecture for suggested secure healthcare storage solution. Combination of IPFS and Blockchain provides a cost-effective solution as scalability, energy consumption, and resource management are taken into consideration.	Blockchain
[S14]	Proposed recommendation model for health data storage that uses repositories to ensure patient preferences and storage decisions quickly. Machine Learning is used to map features and characteristics for each repository.	ML
[S15]	AI technology enhances performance of many conventional security systems with the expanding growth of complex cyber threats. Demonstrates the use cases of AI technology in all organization, but for this case, healthcare related information is noted.	AI
[S16]	New security framework responding to new technologies' security concerns. Prototype used covers capability system, secure transactional layer, service management layer, and mHealth application.	Blockchain
[S17]	An integrated clinical environments (ICE) improvement study to achieve an automatic, intelligent, and real-time system to detect, classify, and mitigate ransomware. Network Function Virtualization (NFV) and Software Defined Networking (SDN) were used to for additional precision.	ML
[S18]	Proof of concept for ransomware detection using machine learning models. Decision tree, random forest, KNN, SVM, SGBoost, and Logistic Regression were used as machine learning models for the discussion in which resulted in a 98.21% accuracy.	ML
[S19]	Proposal for a risk transference-based system architecture in which it moves sensitive data outside into data stores with security protocols. Threat model demonstrates the different vectors of where attackers will potentially attack.	Risk Transference

Table 4. (continued)

Primary Study	Key Qualitative & Quantitative Data Reported	Types of Security Applications
[S20]	Case study of Build-In ResilieNcy Analysis (BINA) model used to build a cyber resiliency context within healthcare. Focuses of demonstrating NIST SP 800 series document within context of healthcare.	Cyber Resiliency
[S21]	Use of the Bayesian grey filter-based convolution neural network (BGF-CNN) to enhance accuracy and reduce time complexity and overhead with the addition of using PSO and GWO optimization techniques. Proposed a blockchain-based cyber-physical system using a deep neural network (BGF Blockchain) in which cyberspace is related to blockchain technology and physical is related to medical facilities and patients.	Blockchain
[S22]	Case study showing AI and blockchain-based secure architecture for analyzing malware and network attacks on wearable devices. Emerging technologies are applied to explore their importance within the healthcare systems in addition to addressing research challenges and issues.	AI & Blockchain
[S23]	Introduces a new holistic security mechanism called "SentinelPlus" which is a machine learning-base security management suite. The suite includes data loss prevention, automated security configuration management, ransomware detection and intrusion detection system.	ML
[S24]	Vulnerability analysis within the healthcare infrastructure to provide reasons as to why certain areas are being attacked. With the use of existing security standards, evaluation of their challenges is shown regarding their potential solution.	Vulnerability Assessment
[S27]	Created a new system that brings defense-in-depth as part the healthcare infrastructure using a Machine Learning backbone. The system can provide contextual awareness to detect anomalous behavior with improvement in accuracy over time through feedback from security analysts.	ML
[S28]	Proposes BiiMED which is a Blockchain framework for Enhancing Data Interoperability and Integrity regarding EHR-sharing. Includes various solutions such as access management and decentralized Trusted Third-Party Auditor (TTPA).	Blockchain

Table 4. (continued)

Primary Study	Key Qualitative & Quantitative Data Reported	Types of Security Applications
[S29]	Proposing a need for a system capable of proactively gathering advanced data analytics techniques to profile user's behavior for pattern and anomaly identification.	ML
[S30]	Research of the newest blockchain technology solution paired with AI technologies in both healthcare and food industry. Data will only be focused on healthcare portion of the study.	AI

All selected primary studies had a focus or theme that is relevant to answering the research questions, in which all studies had to include both healthcare and ransomware research as well as provide solutions that focused on machine learning, artificial intelligence, and/or blockchain. Studies that had a focus on other solutions were labeled out such as risk transference, cyber resiliency, or vulnerability assessment as these were solutions that helped understand the current infrastructure used within healthcare systems. On the other hand, studies that provided solutions through technology were the primary target of this study due to each technology's capability to work with one other. Machine learning, artificial intelligence, and blockchain had to at least be mentioned or focused in each of the included primary studies. However, this can also be differentiated through percentages.

Different Themes Found in Primary Studies

Table 4 shows key qualitative and quantitative data as well as the type of security application it focused on for each included primary study. Using the current data, Figure 4 was created to illustrate the different themes found.

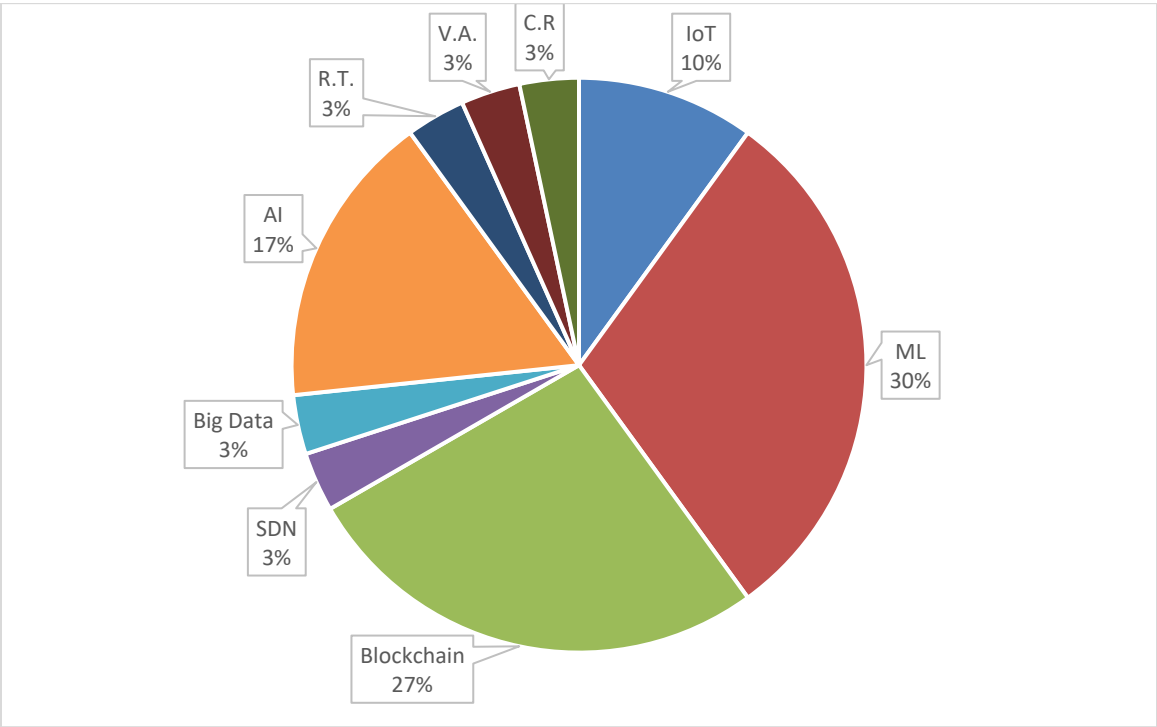

Figure 4. Different Themes within the Primary Studies

Figure 4 shows the percentages of the different themes within the 24 primary studies. The themes identified highlight the security applications commonly used within the healthcare ecosystem. *Machine Learning (ML)* was the most identified theme in the primary study indicating that many solutions and current technologies found in the healthcare ecosystem was machine learning. *Blockchain* was the second most popular theme with a percentage of 27%. The studies in this theme discussed various frameworks, both new and old, with a combination of other technologies such as artificial intelligence or machine learning. Artificial Intelligence (AI) is third at 17% and studies that mentioned AI mainly discussed development of new security mechanisms with other technologies. IoT was the fourth common theme of study, accounting for 10%, because many devices used in healthcare are mostly connected to the Internet in some fashion. Acknowledgement of IoT indicates that improvement. The final theme is a variety of other solutions considered in healthcare. Risk transference, vulnerability assessment, big data, and cyber resiliency are all the last themes that were in the primary studies with the percentage of 3% of each category. Although these studies are different from the other common themes mentioned previously, these are important themes in healthcare. The next chapter will further dissect the relationship of the primary studies and the research questions of this study.

CHAPTER FIVE:

LIMITATIONS, DISCUSSION, & FURTHER STUDY

Chapter Five will discuss the limitations, discussion, & further study of this study. Limitations are the presented problems that came to doing this SLR. Discussion dissects the relationship between included primary studies and how they are relevant to the research questions. Further study will highlight possible implementations for other researchers to continue.

Limitations / Challenges

The SLR process had been an on and off struggle to begin the selection process as one of the factors is the expertise level. Some areas of the study could have been further elaborated through expert of the topic while in this study, general level language was used. Another problem that arose was the time given to do this study as this study was only conducted within a 3-month period. Areas may have been further detailed, elaborated, or included to further address the objective of the study. Backtracking steps within SLR process were not conducted due to time constraints and, again, might have failed to include certain details for the study. Due to healthcare's environment being very large and vast, some areas of the selected primary studies target specific genres within healthcare which introduce solutions that may not work in other areas of healthcare. Although these are some of the downsides, the results may further educate the impacts that ransomware has on healthcare and how many researchers have written about them.

Discussion

The initial keyword search used in the preliminary stages of this SLR demonstrates that ransomware is commonly used in the healthcare environment. The technologies of machine learning, artificial intelligence, and blockchain have only begun their combative security measures against ransomware attacks as the evolution and detection systems were outdated or not quickly enough to see these attacks. Many of the selected primary studies are experimental proposals or concepts of solutions to combat the increase of known ransomware attacks, however, little quantitative data is expressed to indicate whether the proposal are plausible or need further research. To further understand the idea of the reasons healthcare attacks are prone to attacks is to see what the healthcare architecture (Martínez et al., 2022). Furthermore, the common technologies that were seen in almost all studies were artificial intelligence, blockchain, and machine learning.

Approaches to the improvement of current artificial intelligence were talked about in several primary studies. As an example, the development of an AI-powered hybrid approach for the use of ransomware detection formed various families that ransomware to categorize them and indicate a higher accuracy rating than AI alone (Poudyal & Dasgupta, 2021). AI with the combination of other security technology like machine learning or blockchain further improvement the accuracy rating of detection and combating ransomware, one study went with an API-based ransomware and others using machine learning (Almousa et al., 2021; Rani & Dhavale, 2022a; Wazid et al., 2023).

The capabilities that machine learning has and the solutions it can solve in healthcare is significant. Dealing with ransomware attacks can lead many healthcare organizations to go back to pen and pencil, but with machine learning and its features the selected studies prove its use case. A study introduces a new security mechanism called “SentinelPlus” which leverages a machine learning suite to include other security protocols and technologies (Janith et al., 2021). Another study analyzed accuracy rating of various ML models with a sample ransomware data set to test which ML model can be extended to be a ML-based detection system for ransomware (Rani & Dhavale, 2022a).

Blockchain technology was shown in several primary studies proposing various solutions and providing new frameworks. As an example, one study proposed a Blockchain-enabled Security Framework to detect and defend from ransomware attacks for Smart Healthcare (BSFR-SH) (Wazid et al., 2023). Regarding the topic of Smart Healthcare, two studies provided various views with their solutions on it, one using Bayesian grey filter-bases convolution neural network (BGF-CNN) to provide a solution with the use of blockchain and the other targeting using AI with blockchain to identify attacks on wearable devices (Alabdulatif et al., 2022; Ch et al., 2022). Other studies outlined new frameworks within the mHealth application and used other existing technologies with blockchain such as AI and IPFS (Kumar et al., 2021; Vithanwattana et al., 2021; Vyas et al., 2022).

The selected primary studies provided various experimental solutions and researched various types of devices or systems that are used in the healthcare space. Although some solutions may be applicable to some studies, they all prompt the dangerous impacts that ransomware has given to healthcare organizations. For this study, the primary studies were selected because of their contribution to finding the answers that were asked in Chapter 1.

RQ 1: What Current Ransomware Attacks are Used in Healthcare Systems?

This systematic literature review is meant to uncover the reasons why ransomware is increasing within healthcare. To find this answer, researched focused on two main keywords, “healthcare” and “ransomware.”

With these keywords in placed, there was an abundant number of articles providing great details of the specifics and intricacy of ransomware attacks but was not used due to the focus of the study.

The most known and used ransomware attack originated from the WannaCry ransomware attack back in 2017 (Rani & Dhavale, 2022a). Iterations of WannaCry may be labeled by various names, but they all are within the same family of crypto ransomware. Another type seen within healthcare is Locker ransomware. Although this type is not commonly seen unlike crypto ransomware, iterations of locker ransomware have used advanced technology that goes under the radar of current security controls (Poudyal & Dasgupta, 2021).

RQ 2: What Ransomware Attacks are Likely to Appear in the Future?

Of course, current ransomware attacks will appear in the future with more sophisticated methods used. This question strives to answer a predictable outcome based on the given information provided by the primary studies. Knowing that artificial intelligence, machine learning, and blockchain are being used as security measures, future iterations of ransomware may resolve in taking advantages of the weakness and challenges of these technologies (Ghosh et al., 2023). In addition, the healthcare ecosystem and the current infrastructure have areas that can be further leveraged by ransomware due to their recent development incorporating remote capabilities and devices (Martínez et al., 2022). Internet of Things (IoT) devices such as implantable medical devices (IMDs), body area networks (BANs), or implantable and wearable medical devices (IWMDs) immobilize new threats (Hathaliya & Tanwar, 2020). With the increase in ransomware attacks and more technologies implemented in healthcare, the more complicated the mitigation and improvement methods will become.

RQ 3: What Solutions or Methods have been Used to Prepare, Prevent, and Recover from These Types of Attacks?

Many primary studies discussed in this systematic literature review have indicated the common solution and methods that have worked for the healthcare environment. Machine learning (ML), blockchain, and artificial intelligence (AI) were the targeted focus of this study, however, these may not be the only solutions out there. These technologies were combined with one other to identify possible solutions that improved security measures in healthcare, such results had accuracy ratings averaging 99% leading to development of SentinelPlus, uses ML models as security mechanisms, AIRaD, uses ML with AI for ransomware detection, BSFR-SH, uses blockchain to secure smart healthcare systems, and more solutions mentioned previously (Janith et al., 2021; Poudyal & Dasgupta, 2021; Wazid et al., 2023). To summarize, the selected primary studies all provide some solution to the problem whether it be in vulnerability assessment, developing a new framework, or using existing solutions with existing frameworks to better secure the healthcare environment from ransomware.

Further Study

This research has identified available recent research why ransomware has increased in the healthcare industry. The focus of this research is to understand the grounds of previous studies and centralize them to find trend of where ransomware is heading in the healthcare industry.

Future research on this topic should experiment with the developed solutions and methods using in-depth details of ransomware occurrence using data breach data to accurately test in a live-simulated environment. Additionally, inclusion of other solutions or application-specific information can help solidify areas mentioned in this study.

REFERENCES

Alabdulatif, A., Khalil, I., & Saidur Rahman, M. (2022). Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis. *Applied Sciences*, *12*(21), Article 21. https://doi.org/10.3390/app122111039

Almousa, M., Basavaraju, S., & Anwar, M. (2021). API-Based Ransomware Detection using Machine Learning-Based Threat Detection Models. *2021 18th International Conference on Privacy, Security and Trust (PST)*, 1–7. https://doi.org/10.1109/PST52912.2021.9647816

Ashraf Uddin, M., Stranieri, A., Gondal, I., & Balasubramanian, V. (2020). Dynamically Recommending Repositories for Health Data: A Machine Learning Model. *Proceedings of the Australasian Computer Science Week Multiconference*. https://doi.org/10.1145/3373017.3373041

Athinaiou, M. (2022). *Model-based Management of Cyber Resiliency for Healthcare Systems* [PhD Thesis]. University of Brighton.

Awaludin, A., Sulistyadi, W., & Chandra, A. F. (2023). Analysis of Attacks and Cybersecurity in the Health Sector during a Pandemic COVID-19: Scoping Review. *Journal of Social Science*, *4*(1), Article 1. https://doi.org/10.46799/jss.v4i1.512

Bertia, A., Xavier, S. B., Kathrine, G. J. W., & Palmer, G. M. (2022). A Study about Detecting Ransomware by using Different Algorithms. *2022 International Conference on Applied Artificial Intelligence and Computing*

(ICAAIC), 1293–1300. https://doi.org/10.1109/ICAAIC53929.2022.9792587

Boddy, A., Hurst, W., MacKay, M., & El Rhalibi, A. (2019, May 23). Establishing Situational Awareness for Securing Healthcare Patient Records. *International Journal on Advances in Life Sciences*. The Tenth International Conference on eHealth, Telemedicine, and Social Medicine eTELEMED 2018, Rome, Italy. http://researchonline.ljmu.ac.uk/id/eprint/10038/

Boddy, A., Hurst, W., Mackay, M., & Rhalibi, A. E. (2017). A Study into Data Analysis and Visualisation to Increase the Cyber-resilience of Healthcare Infrastructures. *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, 1–7. https://doi.org/10.1145/3109761.3109793

Ch, R., Srivastava, G., Nagasree, Y. L. V., Ponugumati, A., & Ramachandran, S. (2022). Robust Cyber-Physical System Enabled Smart Healthcare Unit using Blockchain Technology. *Electronics*, *11*(19), 3070. https://doi.org/10.3390/electronics11193070

ELGawish, R., Hashim, M., Abo-Rizka, M., & ELGohary, R. (2022). Detecting Ransomware within Real Healthcare Medical Records Adopting Internet of Medical Things using Machine and Deep Learning Techniques. *International Journal of Advanced Computer Science and Applications*, *13*(2), 591–597.

Fernández Maimó, L., Huertas Celdrán, A., Perales Gómez, Á. L., García Clemente, F. J., Weimer, J., & Lee, I. (2019). Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments. *Sensors (14248220)*, *19*(5), 1114. https://doi.org/10.3390/s19051114

Ghosh, P. K., Chakraborty, A., Hasan, M., Rashid, K., & Siddique, A. H. (2023). Blockchain Application in Healthcare Systems: A Review. *Systems*, *11*(1), Article 1. https://doi.org/10.3390/systems11010038

Gopinath, S., & Olmsted, A. (2022). Mitigating the Effects of Ransomware Attacks on Healthcare Systems (arXiv:2202.06108). arXiv. https://doi.org/10.48550/arXiv.2202.06108

Hathaliya, J. J., & Tanwar, S. (2020). An Exhaustive Survey on Security and Privacy Issues in Healthcare 4.0. *Computer Communications*, *153*, 311–335. https://doi.org/10.1016/j.comcom.2020.02.018

Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020). Blockchain technology for Healthcare: Enhancing Shared Electronic Health Record Interoperability and Integrity. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 310–317. https://doi.org/10.1109/ICIoT48696.2020.9089570

Janith, K., Iddagoda, R., Gunawardena, C., Sankalpa, K., Abeywardena, K. Y., & Yapa, K. (2021). SentinelPlus: A Cost-Effective Cyber Security Solution for Healthcare Organizations. *2021 3rd International Conference on*

Advancements in Computing (ICAC), 359–364. https://doi.org/10.1109/ICAC54203.2021.9670892

Kadel, R., Shrestha, H., Shrestha, A., Sharma, P., Shrestha, N., Bashyal, J., & Shrestha, S. (2022). Emergence of AI in Cyber Security. *International Research Journal of Modernization in Engineering Technology and Science*.

Kioskli, K., Fotis, T., & Mouratidis, H. (2021). The Landscape of Cybersecurity Vulnerabilities and Challenges in Healthcare: Security Standards and Paradigm Shift Recommendations. *Proceedings of the 16th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3465481.3470033

Kumar, S., Bharti, A. K., & Amin, R. (2021). Decentralized Secure Storage of Medical Records using Blockchain and IPFS: A Comparative Analysis with Future Directions. *Security & Privacy*, *4*(5), 1–16. https://doi.org/10.1002/spy2.162

Martínez, A. L., Pérez, M. G., & Ruiz-Martínez, A. (2022). A Comprehensive Review of the State of the Art on Security and Privacy Issues in Healthcare. *ACM Comput. Surv.* https://doi.org/10.1145/3571156

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care

Delivery Organizations, 2016-2021. *JAMA Health Forum*, *3*(12), e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses. *ACM Trans. Comput. Healthcare*, *2*(3). https://doi.org/10.1145/3453176

Porath, J. (2023). Typing a Terrorist Attack: Using Tools from the War on Terror to Fight the War on Ransomware. *Pepperdine Law Review*, *50*(1), 139–190.

Poudyal, S., & Dasgupta, D. (2021). Analysis of Crypto-Ransomware using ML-Based Multi-Level Profiling. *Ieee Access*, *9*, 122532–122547. https://doi.org/10.1109/ACCESS.2021.3109260

Rani, N., & Dhavale, S. V. (2022b). Leveraging Machine Learning for Ransomware Detection (arXiv:2206.01919). arXiv. https://doi.org/10.48550/arXiv.2206.01919

Tetteh, B. (2019). Does HIPAA Provide enough Protection for Healthcare in the Age of Ransomware and Current Cybersecurity Threats. *MUSC Theses and Dissertations*. https://medica-musc.researchcommons.org/theses/237

Thamer, N., & Alubady, R. (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), 210–216. https://doi.org/10.1109/BICITS51482.2021.9509877

Villarreal, E. R. D., García-Alonso, J., Moguel, E., & Alegría, J. A. H. (2023). Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security. *IEEE Access*, *11*, 5629–5652. https://doi.org/10.1109/ACCESS.2023.3236505

Vithanwattana, N., Karthick, G., Mapp, G., & George, C. (2021). Exploring a New Security Framework for Future Healthcare Systems. *2021 IEEE Globecom Workshops (GC Wkshps)*, 1–6. https://doi.org/10.1109/GCWkshps52748.2021.9681967

Vyas, S., Shabaz, M., Pandit, P., Parvathy, L. R., & Ofori, I. (2022). Integration of Artificial Intelligence and Blockchain Technology in Healthcare and Agriculture. *Journal of Food Quality*, *2022*, e4228448. https://doi.org/10.1155/2022/4228448

Wazid, M., Kumar Das, A., & Shetty, S. (2023). BSFR-SH: Blockchain-Enabled Security Framework Against Ransomware Attacks for Smart Healthcare. *IEEE Transactions on Consumer Electronics*, *69*(1), 18–28. https://doi.org/10.1109/TCE.2022.3208795

Yeo, L. H., & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in Health Information Management*, *19*(Spring), 1i.