12-2021

# Information Security and Privacy in the Cloud of Healthcare Sector, and The Use of Miter Att&ck Framework to Keep the Healthcare Secure

Fawaz Alabdulhadi

# Information Security and Privacy in the Cloud of Healthcare Sector, and The Use of Miter Att&ck Framework to Keep the Healthcare Secure

by

Fawaz Alabdulhadi

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science in

Information Assurance

December, 2021

Starred Paper Committee:
Abdullah Abu Hussein, Chairperson
Lynn Collen
Erich Rice

## Abstract

With healthcare moving to the cloud, it is necessary to be concerned about the rising cyber-threats. The healthcare industry is one of the most targeted industries by cyber-criminals. This can be attributed to the weak security measures employed and the vast amounts of valuable data that the healthcare industry holds. To ensure that the healthcare industry is secure, this paper proposes the use of the MITRE ATT&CK framework. The MITRE ATT&CK framework presents the best possible way of staying ahead of the threat landscape by helping cyber-security experts understand adversaries' thought processes. By understanding how attackers think and the techniques that they use to gain unauthorized access to IT systems, the healthcare industry can use this information to improve its security architecture. To collect data needed for the study, the qualitative research design will be utilized. Data will be gathered from multiple sources, and the information synthesized to understand how the healthcare industry can improve its security through the application of the MITRE ATT&CK framework.

## Table of Contents

Page

Chapter Page

## List of Tables

Table Page

## List of Figures

Figure Page

# Chapter I: Introduction

## Introduction

Healthcare organizations in almost all parts of the world are migrating to the cloud, just like other organizations, to enjoy the cloud's benefits, which include cutting their information technology costs. Decisions on taking the step of migrating to the cloud elicit mixed reactions among the stakeholders, for, despite it benefiting organizations, it can increase security and privacy risks. Healthcare organizations, which handle vast volumes of greatly sensitive data that include Personally Identifiable Information, its subsets Protected Health Information, and Payment Card Industry Information, are much concerned with the increase in security and privacy risks. This increase might result from migrating to the cloud because of the many laws and regulations they have to abide by, including HIPAA regulations. However, the sector can’t abandon cloud computing technology because of its risks, for the risks can be mitigated to enable the healthcare industry’s organizations to enjoy the benefits that come with migrating to the cloud (Michalas et al., 2014).

This paper suggests using the Mitre Att&ck Framework to help healthcare organizations achieve security in the cloud environment. The Mitre Attack framework outlines the steps and common techniques that attackers use to infiltrate cloud systems. This framework also provides a comprehensive list of commonly used techniques and tactics adversaries use to exploit cloud environments. Therefore, using this framework, the healthcare organization will understand the adversaries' behavior and learn the process followed by attackers. The healthcare organization can benefit from the MITRE ATT&CK framework since they will learn how attackers evolve and understand the most common attack techniques. This paper will explore the techniques and tactics used by attackers to compromise cloud environments and explain how the healthcare IT team can mitigate and detect these attacks to enjoy the benefits of cloud computing without trading security (Basra & Kaushik, 2020).

## Problem Statement

Cloud computing platforms had increased since 2006, when Amazon.com made available its cloud platform for public use. Digital data storage is a highly important activity for any healthcare organization. It contributes to better diagnosis, caring, and treatment of patients who frequent their facilities, not forgetting easing retrieval and management of information, and achieving high efficiency in the organizations' financial management. The number of the healthcare sector that have migrated their IT operations and data to different cloud platforms is very high, eliciting fear and confusion. This makes one fall deeply into the questions: Is the patients' data that healthcare sector organizations handle using various cloud platforms secure? Is the data that cloud platform store and process only accessible to authorized users or might be accessible to unauthorized users evoking privacy violations and unintended disclosure?

The Healthcare industry is experiencing a fast increase in cyber-breaches related to financial losses, cyber-attack incidents, and the extent of exposure of sensitive records. The trend is a dangerous one as it means, if not halted, the sector will lose its clients' trust and fall into deep trouble with regulatory bodies. It can even make some of the sector's organizations fall into serious financial problems arising from massive financial losses due to hefty compensations for impacted patients, fines, and penalties for no adherence to various PHI regulations (Seh et al., 2020).

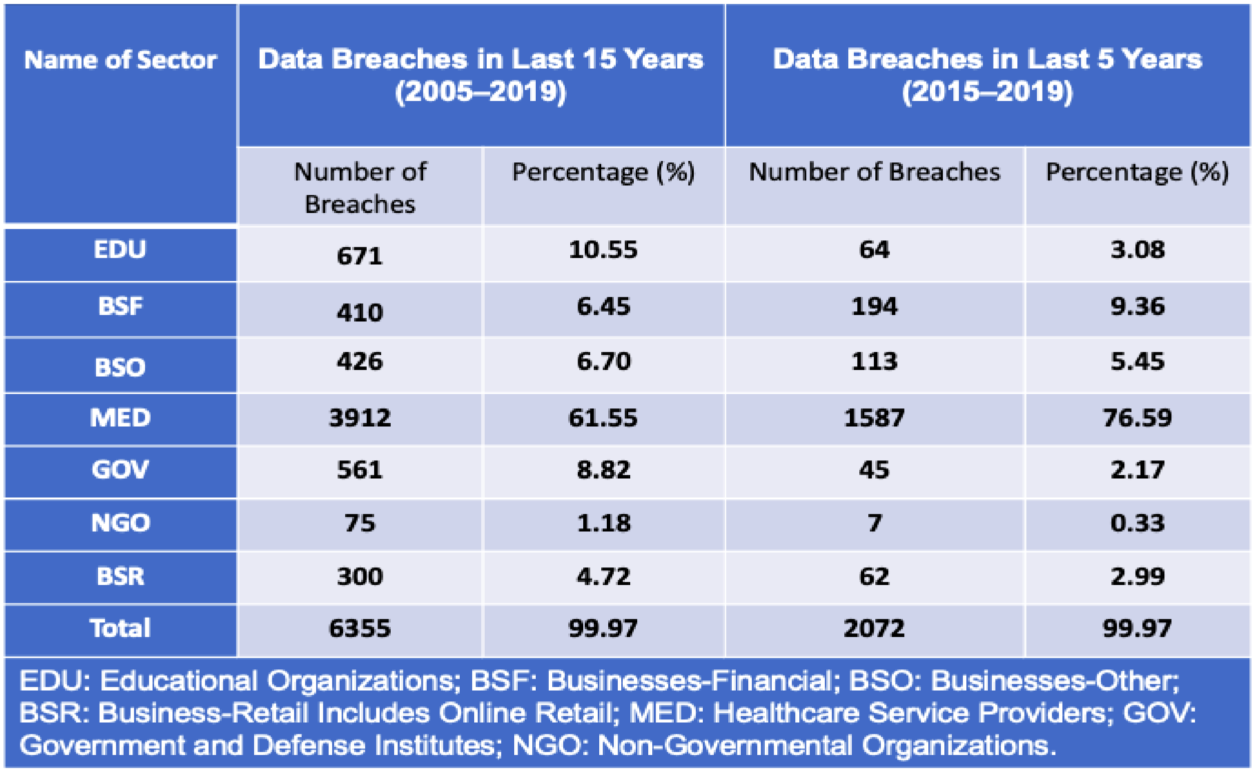
People like maintaining the privacy of their personal, financial, and health records. Handling patients’ data carelessly can lead to a cyber-breach and with articles authored between 2009 and 2020 indicating an escalating adoption of cloud computing technology, interests in cloud environment escalated. Failure to follow security best practices when handling patients’ data in a cloud platform or on transit to a cloud platform is the main problem. The use of the Mitre Att&ck Framework to optimally secure the healthcare cloud environment is the solution proposed by this paper. The Mitre Att&ck framework can help the healthcare IT team understand common tactics and techniques used by attackers and apply the recommended mitigation and detection techniques to improve the healthcare security posture.

## Nature and Significance of the Problem

Cloud computing services are listed by professionals, including managers, as items that can help spur the growth and improvement of healthcare services (Kuo, 2011). However, information/data security, which is the cloud's main challenge, is derailing healthcare organizations’ migration to the cloud. Healthcare organizations hold vast volumes of highly sensitive healthcare stakeholders’ data. As a result, data will be at risk if migrated to the almost universally accessible cloud without regard to offering the optimal data security using best practices for cyber-security incidents prevention, detection, and response (Michalas et al., 2014).

**Table 1**

*Representation of Data Breaches by Sector*



| Name of Sector | Data Breaches in Last 15 Years (2005–2019) | | Data Breaches in Last 5 Years (2015–2019) | |
|---|---|---|---|---|
| | Number of Breaches | Percentage (%) | Number of Breaches | Percentage (%) |
| EDU | 671 | 10.55 | 64 | 3.08 |
| BSF | 410 | 6.45 | 194 | 9.36 |
| BSO | 426 | 6.70 | 113 | 5.45 |
| MED | 3912 | 61.55 | 1587 | 76.59 |
| GOV | 561 | 8.82 | 45 | 2.17 |
| NGO | 75 | 1.18 | 7 | 0.33 |
| BSR | 300 | 4.72 | 62 | 2.99 |
| Total | 6355 | 99.97 | 2072 | 99.97 |

EDU: Educational Organizations; BSF: Businesses-Financial; BSO: Businesses-Other; BSR: Business-Retail Includes Online Retail; MED: Healthcare Service Providers; GOV: Government and Defense Institutes; NGO: Non-Governmental Organizations.

When it comes to classifying cyber-attacks in table1 by sector for the duration 2005-2019 and 2015-2019, the healthcare industry leads as it takes 61.55% and 76.59% of the total data breaches for 2005-2019 and 2015-2019. No other sector takes more than 10% of the total data breaches between 2015-2019. These trends indicates yearly data breaches in the healthcare industry are on an upward trajectory (Seh et al., 2020).

Due to the rise of cyber–attacks targeting the healthcare sector, this study proposes using the MITRE ATT&CK model to help the healthcare industry understand the attackers' behavior and apply the best mitigation and detection measures to avoid cyber breaches. The MITRE ATT&CK model can help healthcare centers prevent cyber-attacks.

## Objective of the Study

The study's objective is to explore cyber-trends in the healthcare sector and discuss the techniques that attackers commonly use to infiltrate cloud environments. The research will examine the methods outlined in the MITRE ATT&CK framework and how the healthcare IT team can mitigate and detect these techniques to secure their cloud environments.

## Study Questions/Hypotheses

- What trends do statistics on cyber breaches in the healthcare display?
- What should be done to halt the positive trend in increasing cyber breaches in the healthcare sector?
- How can the healthcare sector employ Mitre Att&ck Framework to attain their cloud security goals?

## Limitations of the Study

The main limitation of this study was in regard to collecting and analyzing data to answer the research questions. Since the research method is entirely qualitative, it entails collecting data from a wide range of sources. Getting these sources was a challenge since the internet contains vast amounts of information and filtering through all this information was a serious challenge. Analyzing these vast amounts of information was also tiresome and consumed a lot of project time. Another limitation of this study is that only qualitative data was used, therefore, there was no way of quantifying the results.

## Definition of Terms

- *Protected Health Information (PHI):* Information that pertains to the health of a patient. They include laboratory results, drug administered, and illnesses diagnosed.
- *Payment Card Industry Information:* Information about electronic payments that a customer makes. They include the used card’s credit card number, expiry date, and security code.
- *Privacy:* Not known by unauthorized persons.
- *Office for Civil Rights (OCR):* It’s a law enforced by the department of Health and Human sciences to violation of rights enacted to tame discrimination of individuals and other entities.
- *Health Insurance Portability and Accountability Act (HIPAA):* It’s a statue of the Unites States federal government enacted to enforce creation of patients’ data protection national standards to prevent unconsented disclosure of patients’ sensitive medical data.

## Summary

Almost every healthcare industry stakeholders accept migrating to the cloud is a necessary step. But they are divided between cloud advantages and the escalating cyber-breaches and their high damage and losses. Moving to the cloud presents numerous advantages such as increased collaboration, cutting costs and increasing interoperability. However, despite these advantages, migrating to the cloud presents inherent security risks to the healthcare sector. Studies show that the healthcare sector is the most targeted by adversaries and it leads in the number of attacks as compared to other industries. Adversaries target the healthcare industry to gain access to patient identifiable information and other sensitive data that can be used for malicious gains. Successful cyber-attacks can affect the healthcare reputation and make it liable for law suits. The healthcare organization can also suffer financial losses if it fails to implement preventive measures.

The healthcare is the most targeted due to its weak security measures. This paper proposes the use of the MITRE ATT&CK framework to help the healthcare stay a head of the growing threat landscape. Through the use of Mitre Att&ck Framework can eliminate the division, making everyone comfortable and patients' data secure. Furthermore, their privacy is guaranteed to a large extent.This is because the MITRE ATT&CK framework offers a comprehensive list of techniques and tactics that attackers use to infiltrate cloud accounts. Through the use of the techniques discussed in the MITRE ATT&CK framework, the healthcare IT team can implement the best prevention and detection measures that can help in preventing attacks.

# Chapter II: Background and Review of Literature

## Introduction

The background and literature review section provides enough information on the nature of the research problem and the solution that should be taken. This section will explore the challenge that healthcare organizations face as a result of migrating to the cloud. Cloud computing is one of the emerging disruptive technologies, and companies, including the healthcare industry, have no choice but to adapt (Nieuwenhuis et al., 2018). This is because cloud computing offers immense benefits that will also be discussed in this section.

## Background Related to the Problem

Subramanian & Jeyaraj. (2018) define cloud computing as the delivery of computing services such as databases, servers, software, analytics, networking, and intelligence over the internet to reduce resources and support faster innovation. With cloud computing, companies do not need to purchase expensive computer technology and spend enormously on maintaining these technologies. Cloud computing allows companies to rent the specific computer services that they need, such as data storage and management, software applications, servers, hosting solutions, network access, among other IT services. The popularity of cloud computing services is skyrocketing. It is estimated that by the end of 2021, the global market for cloud computing services will hit $308.5 billion. Due to this, the healthcare industry, just like other industries, is investing heavily in the migration to the cloud.

While cloud computing presents lots of advantages, it raises various concerns regarding data stored security and privacy. Some businesses are unwilling to transfer to the cloud due to data loss concerns, data privacy and confidentiality, legal and regulatory compliance, and exposure of credentials (Yang et al., 2017). Cloud computing, therefore, poses a real significant threat, and this can be evident from the rising number of cyber-attacks being recorded. Cyber-security experts predict that there will be a cyber-crime every 11 seconds in 2021, and these effects can be reflected in the healthcare sector (Morgan, 2021).  A report provided by Check Point, a famous cyber-security agency, indicates that the global healthcare sector has recorded a 45% increase in cyber-attacks since 2020 November. Based on this report, attackers employed various attack vectors such as denial-of-service attacks, ransomware, phishing, social engineering, and botnets (Bracken, 2021). All these threat actions are executed over the internet, thus making cloud computing dangerous.

Data criminals target healthcare centers since they store valuable data that can be sold in the black market or used to perform other malicious activities such as identity theft and blackmail. Hackers can access valuable information and deny physicians and patients access to this data until they pay a ransom. For instance, the Hollywood Presbyterian Medical Center was held ransom for a week by hackers. The hackers required a ransom of $17.000 to be paid in bitcoins to decrypt necessary files and information. The hackers used ransomware to encrypt the hospital’s sensitive data, affecting the healthcare facility's functioning (Mattei, 2017). This is only an example of how hackers can cause harm to healthcare centers if proper measures are not put in place to defend cloud services.

While cyber-security experts have proposed various strategies that can be used to minimize the risk of cyber-attacks on the cloud, none of these have been fully effective in ensuring that cloud computing is secure. Some of the strategies put forward to help improve cloud security include; deploying multi-factor authentication, applying intrusion detection systems, and offering anti-phishing training. However, these methods have not made the cloud secure and assure customers and organizations of security and privacy. For instance, with technology developing rapidly, malicious actors are becoming more innovative, and by-passing security measures such as intrusion detection systems are extremely easy.

To improve the security of cloud services, cyber-security teams must think like malicious actors. The MITRE ATT&CK framework offers a detailed matrix of tactics and techniques that attackers and defenders employ. Therefore, with this approach, the healthcare sector can help reduce the number of cyber-attacks and ensure sensitive information is safe since it is easy to classify attacks and assess an organization’s risk while utilizing MITRE ATT&CK.

## Literature Related to the Problem

In their survey, researchers Ahuja et al. (2012) agree that cloud computing defines businesses and how businesses are managed. Cloud computing is transforming every industry since it scales down the overall cost of utilizing IT solutions. This article predicted that by 2020, more than 80% of businesses would move to the cloud due to the cheap costs of utilizing IT resources. Companies that could not afford the cost of building infrastructure and platforms to support their applications can now easily access these services over the cloud. Cloud computing platforms offer various functionalities, such as providing various platforms with different operating systems that allow consumers to develop, test and deploy software applications using virtual servers. Since cloud computing offers these and many more advantages, the healthcare sector is investing enormously in this technology. Major companies such as Amazon, Google, and Microsoft are also investing and collaborating with healthcare organizations to maximize cloud computing benefits.

Moving to the cloud is perceived as the perfect solution, and healthcare organizations in different countries adopt this new technology. (Alharbi et al., 2016) analyzed what it takes to adopt cloud computing in Saudi healthcare organizations. Based on this study, the adoption of cloud computing in Saudi Arabia healthcare is affected by five factors; attitude toward change, pressure from business partners, relative advantage, and soft and hard financial analysis. However, this article also cites that the country's adoption of cloud computing is still relatively low due to barriers such as technological difficulties, insufficient IT infrastructure, and compatibility. However, despite these barriers, Saudi Arabia's healthcare sector is adopting cloud computing to improve its service provision.  The healthcare system of Saudi Arabia is facing challenges such as the rise of chronic disease, increase in the cost of health services, and shortage of healthcare professionals. As a result of this, many healthcare centers are willing to invest in IT technologies to mitigate these problems, which have led to the adoption of cloud computing services.

The Iraqi health care system is also facing similar challenges regarding the management of health records due to the growing complexity of data and low information technology (Meri et al., 2019). Due to these challenges, the Iraqi healthcare system is also in a rush to implement cloud computing services. By moving to the cloud, the Iraqi healthcare system aims to lower the cost of IT infrastructure, easily manage and retrieve health record data, and monitor patients' health from any location. Various literature exists showing how the health care sectors from different parts of the world are moving to the cloud.

According to Ahuja et al. (2012), moving to the cloud presents inherent risks to healthcare organizations regarding security and privacy. Healthcare organizations also face the challenge of complying with the HIPPA standards. Griebel et al. (2015) also state that the biggest problem facing the adoption of cloud services in healthcare is security and privacy.

The healthcare sector was one of the most frequently attacked sectors. In 2016, it was ranked 9th among the most commonly targeted industries by cyber-criminals (Meisner, 2017). Cyber-criminals are targeting the healthcare sector due to the massive and valuable information that this industry stores. Reports indicate that cyber-criminals target sensitive personal health data since it is more valuable on the black market than credit cards or social security numbers. Martin et al. (2017) states that the healthcare industry faces higher cyber risks than other industries due to its weak security posture.

This article also asserts that the healthcare industry is one of the most targeted cyber-criminals since it underinvests in modern information technology infrastructure.

Various healthcare organizations have faced serious cyber-attacks that call for the need to implement measures to improve cloud computing security in healthcare. Apart from the Hollywood Presbyterian Medical Center, other healthcare industries that have been affected include; the Boston Children's Hospital, the Dusseldorf University Clinic, among many other healthcare centers. In February 2020, the Boston Children's Hospital discovered a malware attack that had disrupted hundreds of computers. The malware attack is said to have affected more than 500 doctors and other healthcare providers that serve around 3,500 patients (Palumbo & Buja, 2020). As a result, numerous patients were forced to reschedule their visits.

Implications of cyber-attacks in the healthcare system can cause severe financial and health consequences. The cost of treating cyber-attacks is significantly high. In the event of an attack, organizations must utilize forensic investigation to determine the attack's cause and impact. In most cases, third-party services are required for detailed and accurate investigations. The cost of third-party forensic investigation is significantly high depending on the duration of the research. A survey by Deloitte estimates a cost of $600,000 for six weeks. Healthcare organizations also incur other charges such as breach notification and post-breach patient notification. Apart from the financial consequences, cyber-attacks can impact patient lives. Some studies have shown that the rise of cyber-attacks and data breaches can be the cause of rising heart attack deaths in the United States (Holmes, 2019).

Due to the effects of cyber-attacks in the healthcare sector, these organizations must find the best possible ways of mitigating these attacks. The healthcare sector can use the MITRE ATT&CK framework to improve the security of its cloud services and ensure patient's sensitive data is secure. According to Al-Shaer et al. (2020) the MITRE ATT&CK framework offers a rich and actionable repository of the techniques and procedures (TTP). As cyber-attacks increase in sophistication and volume, MITRE has developed a detailed public knowledge base listing the tactics and techniques usually utilized by attackers.

The MITRE ATT&CK model provides a wide range of adversary tactics and techniques geared towards helping organizations and governments develop threat models and methodologies for improving cyber-security. Based on this approach, organizations need to understand how adversaries think and the strategies that they employ. The MITRE ATT&CK model is effective in helping organizations improve post-compromise detection of attackers. With this model, the cyber-security team can easily analyze how the attackers managed to compromise the network and how they are navigating within the system. The healthcare industry can utilize this framework to identify the specific techniques that attackers can use and take the necessary preventive measures.

The MITRE ATT&CK offers 11 tactics used by attackers – initial access, execution, persistence, privileged escalation, credential access, discovery, collection, exfiltration, discovery, defense evasion, and lateral movement. Each of these tactics contains multiple techniques employed by adversaries (Brook, 2020).

The benefit of the ATT&CK model is that it allows an organization to visualize how attackers think and the entire process that they can utilize to attack the network system. In the reconnaissance stage, the attacker attempts to collect as much information as they can before the attack. The attackers can utilize techniques such as active scanning (T1595), vulnerability scanning (002), hardware and software (001, 002). By understanding these reconnaissance techniques, cyber-security experts can take preventive measures to ensure that attackers cannot gather useful information.

Cyber-security experts can also learn the various techniques that attackers use during execution. During this phase, the attackers attempt to run malicious codes to gain access into the network system. Some of the methods used during this stage include; command and scripting interpreter (T1059), inter-process communication (T1559), and Native API (T1106). Understanding these attack vectors can help an organization stay ahead of the threat landscape (Strom et al., 2018).

Pennington et al. (2019) explain how research and cyber-security teams can use the MITRE ATT&CK framework. This article outlines various levels that are required for one to gain a detailed understanding of how the MITRE ATT&CK model works. The groups outlined include; level 1, Level 2, and level 3. The levels are categorized based on how well one is conversant with the MITRE ATT&CK model, with level 1 being for novice users while level 3 is for more advanced cyber-security teams. At level 1, the security teams are looking for cyber threat intelligence that can be used to improve the decision-making process. By understanding how attackers think and the tools they are using, cyber-experts can take the necessary precaution measures.  Organizations can gain cyber-threat intelligence from organizations that have been previously targeted and understand how the adversaries compromised systems and moved through the network. Companies can also gain intelligence by analyzing adversaries groups that have been prominent in conducting successful cyber-attacks, such as the APT19 group. APT19 is a Chinese threat group that has successfully infiltrated many industries such as finance, telecommunication, and pharmaceutical companies.  By understanding this specific registry run key APT19 used, companies can prevent this attack group. Level 2 involves getting familiar with the overall structure of the ATT&CK framework, understanding adversaries' behavior, and using this information to stay ahead of any threats. Level 3 is for advanced IT teams which can map information provided by the ATT&CK model and use this information to prioritize defense measures (Pennington et al., 2019).

While the MITRE ATT&CK framework effectively helps organizations defend against the rising cyber-threats, there is a limited literature review on how this technology can be utilized in the healthcare sector. This paper, therefore, aims to fill this gap by analyzing how healthcare organizations can benefit from the use of MITRE ATT&CK.

## Literature Related to the Methodology

According to Lilly et al. (2019) application of the MITRE ATT&CK framework helps red teams, defense teams, and organizations map real-world, observed behavior and techniques. This framework provides detailed insights into the techniques and procedures that attackers can apply to infiltrate data and gain unauthorized access into network systems. While conducting this study, the researchers utilized qualitative data accessed from real life case cyber-incidents. To determine how the MITRE ATT&CK model can help organizations prevent against cyber-attacks, the researchers analyzed a 2018 spear phishing campaign by Russia's APT29 against U.S government agencies. By using the qualitative research methodology, the researchers determined that the MITRE ATT&CK framework offers the best threat intelligence that can be utilized by corporations and governments to avoid cyber-attacks.

Kang, (2019) outlines various strategies that organizations can employ to implement the MITRE ATT&CK framework. The first step is to conduct thread modeling to gain a detailed understanding of how the system operates, and the impact that will be caused if any of the system is compromised by attackers. After completing threat modeling, the second step is to identify the most suitable techniques to detect and prevent the attacks. The article relates to my research methodology since it utilizes various sources and links to explain how organizations can implement the MITRE ATT&CK model.

Researchers Al-Shaer et al. (2020) analyzed different datasets from the MITRE ATT&CK framework to determine the common tactics used by attackers. The researchers analyzed a total of 270 attack instances that are made up of 209 techniques. This study relates to my research methodology since the researchers analyzed data from different sources using qualitative and quantitative techniques. The research findings of this study show that the application of the MITRE ATTA&CK framework allows cyber-security teams to understand some of the common tactics that adversaries can take to gain unauthorized access. Some of the tactics that can be utilized include defense evasion, lateral movement, and exfiltration. Defense evasion describes the common techniques that hackers use to avoid being detected. These defense evasion techniques can include access token manipulation, abuse elevation control mechanisms, and BITS job. Lateral movement techniques that cyber-security teams should employ across the organization include remote access hacking, internal spear phishing, and exploiting remote services. Exfiltration refers to the techniques that adversaries take to steal sensitive data. Examples of these techniques include traffic duplication, transferring data to cloud accounts, and automated exfiltration (Al-Shaer et al., 2020). By understanding these techniques, organizations can stay ahead of the growing threat landscape.

Researchers Oosthoek and Doerr (2019), demonstrate how the MITRE ATT&CK framework can be used in mapping malware attacks. Malware is one of the most exploited techniques by attackers, with Verizon Data Breach Investigations' report suggesting that malware attacks make up 30% of data breaches. With the severity of malware attacks, it is necessary for cyber-experts to gain insights into how attackers exploit this technique. To accomplish this study, the researchers collected data related to malware analysis from Malpedia. Malpedia is a reputable database that offers a resource for rapid identification of malware. The researchers used the MITRE ATT&CK framework to map the 951 unique families of Windows malware. The MITRE ATT&CK framework helped the researchers to describe the malware techniques that adversaries can use to attack a system. Through the application of the MITR ATT&CK framework, the researchers collected enough information on the behavior of adversaries and this helped to implement the most suitable preventive techniques. The researchers were able to understand how attackers conduct malware attacks from the planning to execution. This information is vital since it allows the security teams understand adversary behaviors and deploy the best preventive techniques.

Researchers Liu et al. (2020) have also employed this data collection technique to analyze how the MITRE ATT&CK framework can be utilized in forensic analysis in cloud platforms.  The researchers demonstrate how the MITRE ATT&CK framework can be used to filter through the massive amounts of data on the cloud to collect evidence. The MITRE framework helped the researchers to understand how attackers move in the cloud to perform successful attacks. The steps identified that adversaries use include; reconnaissance, command and control communication, privilege escalation, lateral movement, and exfiltration of sensitive information. These are the steps that the healthcare cyber-security teams should be aware of as the healthcare migrates to cloud computing. This study proves that the MITRE ATT&CK is effective in identifying forensically valuable data.

## Summary

From the various literature material analyzed, it is evident that moving to the cloud has led to privacy and security concerns. The healthcare industry is one of the most targeted sectors due to the valuable information it stores. Attackers are interested in gaining sensitive healthcare data that can be sold in the black market and can also use this information for extortion or identity theft. Healthcare is also a target due to its weak security measures. Cyber-attacks can pose significant financial risks to the healthcare industry. Attackers mainly utilize ransomware attacks and demand vast amounts of money. The cost of dealing with cyber-attacks and ensuring that the condition has been remedied is significantly high. Cyber-attacks also put patients' lives at risk. Some studies suggest that the rising cases of heart attack deaths in the United States are a result of the increasing data breaches.

There exist a lot of literature materials that discuss the security concerns of migrating to the cloud. Studies show that while migrating to the cloud provides numerous advantages, it raises serious security concerns that the healthcare industry should be concerned about. The literature review section shows that the healthcare industry is one of the most targeted since it applies weak security measures and lacks a proper-security framework for defending against the growing number of cyber-attacks. The healthcare industry faces numerous cyber-attacks, with malware attacks topping the list.

In order to help the healthcare sector stay ahead of the threat landscape, this paper suggests the use MITRE ATT&CK framework. The MITRE ATT&CK model provides a comprehensive analysis of how the mind of adversaries works. By applying this framework, cyber-security experts can take both pro-active and preventive measures to minimize the risk of cyber-attacks. However, there is limited literature on how the MITRE ATT&CK framework can be utilized in the healthcare sector. This paper, therefore, aims to fill this gap by investigating and presenting how healthcare can benefit from this model. The next section will be describing the research methodology that will be utilized throughout this project.

# Chapter III: Methodology

## Introduction

The methodology section explains the specific data collection and analysis method that will be utilized to address the formulated research problem. This research explores how the healthcare industry can utilize the MITRE ATT&CK framework to protect against the rising cyber-threats. The research methodology which will be used is the qualitative analysis. This method was chosen since it aims to gain deep insights regarding a specific topic and effectively generate new ideas. The qualitative research design involves collecting and analyzing vast amounts of data from different sources to solve the research problem (Merriam, 2002). Through this research, I will collect data from various reputable sources such as Google Scholar, analyze the data and extract meaningful information related to the research problem. Through the use of the qualitative design, a researcher can utilize different data collection techniques such as observation, surveys, questionnaires, and secondary research (Merriam & Tisdell, 2015).

## Design of the Study

Investigating how the application of the MITRE ATT&CK framework can help secure the healthcare industry, this research will utilize the qualitative research technique. The qualitative research technique involves collecting a wide range of non-numerical data that can be analyzed to understand concepts, gain an in-depth understanding of a particular problem and generate new research ideas. Therefore, this makes the qualitative research technique ideal for this research since it aims to understand how the healthcare sector can benefit from the MITRE ATT&CK framework. This research will not utilize quantitative data since we are not dealing with numerical data. The quantitative research technique involves collecting quantifiable data that can be used to perform satirical analysis (Fakis et al., 2014). Since this study only aims at gaining an in-depth understanding of the cyber-threats that the healthcare industry is facing as a result of moving to the cloud and the application of the MITRE ATT&CK framework, the best research design is the qualitative methodology.

To collect data needed for this study, the following research questions will be used;

- What trends do statistics on cyber breaches in the healthcare display?
- What should be done to halt the positive trend in the increase of cyber breaches in the healthcare sector?
- How can the healthcare sector employ Mitre Att&ck Framework to attain their cloud security goals?

The output of this study will show how the MITRE ATT&CK model can be used by the healthcare to improve its security. This is because the framework describes how actors perform attacks from information gathering to execution. While using the MITRE ATT&CK framework, Red teams can infiltrate an information system and gain unauthorized access to sensitive data. Security teams can also benefits from this model since they can apply it to defend against attackers.

When using the MITRE ATT&CK model, advisories uses different techniques to test the strength of the target. Similarly, blue teams use these techniques to understand Red teams' tactics and counter their attack strategy.

## Data Collection

The data for this research will be collected from secondary sources. This will include utilizing the school library resources and the internet. The internet will be the primary source of data since it offers vast information from different researchers. To ensure that the data collected is accurate and valid, only reputable data sources will be used for data collection. The databases utilized in this study include; Google Scholar, Microsoft Academic Search, and Base. These search engines provide information written and reviewed by scholars, which can be relied upon to formulate hypotheses and make conclusions. To collect the specific information required for this study, the following search terms are used;

- Healthcare and cloud computing
- Benefits and drawbacks of migrating to the cloud
- What is MITRE ATT&CK?
- Application of MITRE ATT&CK in healthcare

To ensure validity of data, only sources published within the past ten years will be selected. Data sources older than ten years will be eliminated.

## Tools and Techniques

To analyze the data collected, the qualitative content analysis technique will be used. This involves analyzing the data sources collected to understand common themes and concepts.  The primary tool that will be used for data collection is a laptop. With the use of a laptop, I will collect data from a wide range of online sources such as Google Scholar, Microsoft Academic Search, and Base.

The techniques that will be used to collect data include the use of keywords such as MITRE ATT&CK, healthcare, cyber-attacks, adversaries, red teams, and white hat hackers.  I will use these search terms to look for information related to the research problem.  After collecting data, the next step will be to eliminate information that is not needed or that does not meet the selection criteria. The selection criteria that will be used to eliminate data include; credibility and timeline. Information collected from blogs and Wikipedia pages will be eliminated since this is not peer-reviewed data. Regarding validity, data sources older than ten years will be eliminated.

After eliminating unnecessary information, the next step is to analyze the data to deduct the conclusion.

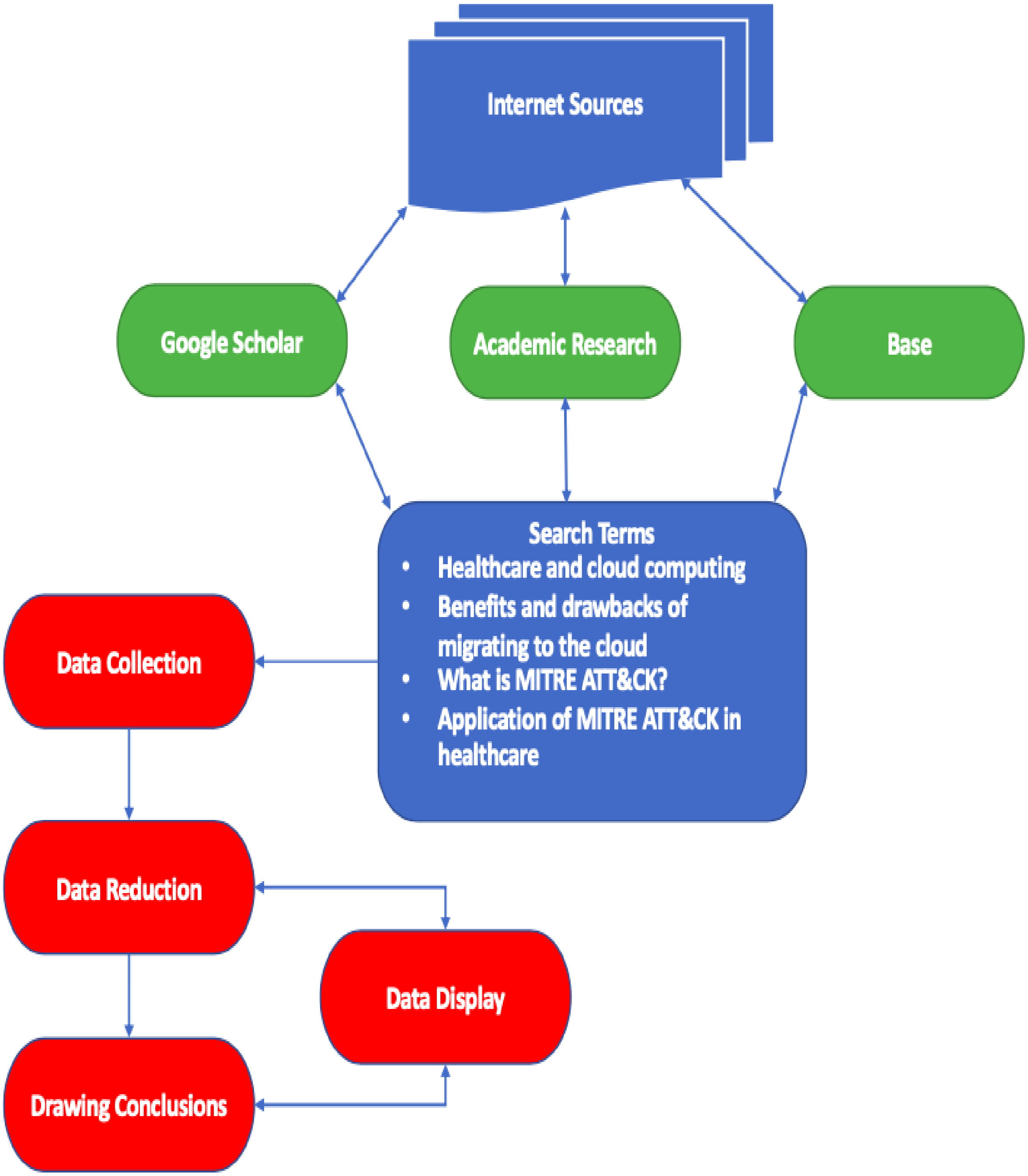
The steps include;

- Collect data from various reputable online sources.
- Eliminate data that does not meet the selection criterion.
- Analyze data and Display it in a readable form.
- Draw conclusions from the data analyzed.

The figure below is a pictorial representation of the entire process;

**Figure 1**

*Qualitative data analysis*



### Summary

The purpose of the research methodology section is to describe the steps and techniques that will be used to collect data needed for the study. While there are different types of research designs, this study will use the qualitative data collection method. The qualitative research design is best suited for this study since it aims at gaining an in-depth understanding of a given problem and provide the best possible solution. The goal of the study is to understand the security impacts of healthcare moving to the cloud and how use of the MITRE ATT&CK framework can help the healthcare industry avoid cyber-attacks. In order to collect the data needed for this study, only reputable data sources such as Google scholar will be used.

The importance of the qualitative design is that it allows researchers to use already existing data to find patterns and gain meaningful insights about a the chosen topic. This research methodology is also best suited for this research since going to the actual field to collect quantitative data would be time consuming and expensive. However, by using the qualitative research design, data can be collected from a wide range of internet sources and use content analysis technique to identify meaningful patterns.

To ensure that the data collected is accurate, only peer-reviewed articles will be selected. Peer-reviewed articles and journals contain accurate information since they are written and reviewed by professionals in the given field. To assure relevance of data, articles and journals published within the past five years will be used. This will ensure that the data collected is up-to date and can be relied upon to make conclusions.

# Chapter IV: Data Presentation and Analysis

## Introduction

After identifying the best method for collecting the required data for research, the next step is to present the data findings and analysis. The purpose of this part is to present and analyze the data findings of the research. Since this study is purely qualitative, the data analysis method that will be utilized is content analysis. The content analysis includes evaluating patterns within words (Mayring, 2014). This section will be divided into three sections; data presentation, data analysis, and summary. Under the first section, this paper will present all the data findings regarding the application of the MITRE ATTACK framework. This section will present and analyze the data findings collected from the literature review section. Since this is a qualitative study, the data findings that will be presented are collected from a wide range of sources.

The data that will be analyzed here is based on the formulated research questions. Therefore, this section will present the data findings related to trends on cyber-attacks in healthcare, cover what the healthcare needs to do in order to halt the increase of cyber-attacks and how the healthcare industry can apply the MITRE ATT&CK framework to attain their cloud security goals.

## Data Presentation

### Moving To the Cloud

The healthcare industry is making major investments in the field of cloud computing. Cloud computing is one of the leading disruptive technologies that is shaping how businesses are conducted. Through cloud computing, the healthcare industry can easily store and manage wide volumes of data and increase the efficiency of operations. Cloud computing entails implementing remote servers that are accessed via the internet to allow organizations to store, manage and process data (Ahmadi & Aslani, 2018). Cloud computing offers a myriad of advantages which makes it necessary for the healthcare industry to invest in this new technology.

Some of the main advantages of moving to the cloud include; reduced cost, facilitating better patient via collaboration and interoperability. Moving to the cloud allows different departments and doctors to easily collaborate and thus provide better healthcare services. This is because medical providers can easily share and transfer data via the cloud and collaborates even from remote locations to boost cooperation and better treatment. .another advantage of moving to the cloud is that it allows healthcare organizations to easily manage data. In cloud computing, the healthcare providers will be using electronic medical records, mobile applications and big data analytics to easily manage the data. Through cloud computing, the healthcare has no limit to the amount of data it can store and process. Since access to data is easier and better organized, healthcare providers can easily manage patient data and use this data to offer the best treatment. Cloud computing also offers the best data storage space that can be easily maintained while avoiding extra costs of maintaining physical servers.

Another major advantage of moving to the cloud is its scalability. By moving to the cloud, healthcare institutions can increase or decrease their data storage based on the flow of patients. Moving to the cloud also provides the advantage or reducing costs. The healthcare will save a lot of money that could be used to set up physical servers and data centers to store vast amounts of healthcare information. Since cloud computing operates on a subscription model, the healthcare industry can save money that could be used in purchasing expensive equipment.

More healthcare institutions are also moving to the cloud for business purposes such as business continuity and disaster recovery plans. Data recovery and backups require huge space and are necessary for any organization; this makes cloud storage the best deal. Healthcare organizations are also migrating to cloud computing to maximize on the increased processing power, something that is crucial for healthcare institutions processing data-intensive analysis such as DNA sequencing. For instance, the Icahn School of Medicine located at Mount Sinai is known for using cloud computing to process terabytes of DNA data in order to unlock the genetic secrete of ovarian and breast cancer (Vuksanaj, 2019).

As more healthcare institutions are adapting cloud computing, more healthcare services are expected to move to the cloud. One of the strongest contenders of for future cloud usage is telemedicine. Healthcare researchers believe more than 70% of routine patient appointments do not require physical interaction with a doctor. A fraction of these interactions can be moved to cloud, allowing patients and doctors to interact remotely and result in massive cost savings in healthcare delivery (Cilliers, 2014).

Another applications that is expected to take shape with the growing use of cloud computing is patient empowerment tools. Patient empowerment tools are cloud hosted applications that will help patients with chronic illness such as cancer to easily monitor their day-to-day care. These applications will provide patients with information such as nutrition, exercise and medication reminders to ensure patients adhere to the prescribed treatment.

Despite the various advantages such as lowering costs and ease of interoperability, statics show that moving to the cloud presents inherent security risks. Moving to the cloud makes it easier for malicious actors to compromise the system, access sensitive data and other critical systems such as servers. Cloud computing exposes an organizations data to malware attacks. Studies show that approximately 90% of organizations are likely to experience data breach due to popularity of cloud computing. Another challenge of transferring data to the cloud is data privacy and compliance issues. Due to privacy related concerns of transferring data to the cloud, various regulatory agencies such as GDPR and HIPAA are implementing more stringent measures. If healthcare organizations fail to properly secure the data stored on cloud storage, they are at risk of facing compliance law suits and suffer financial losses (Ahuja et al., 2012) .

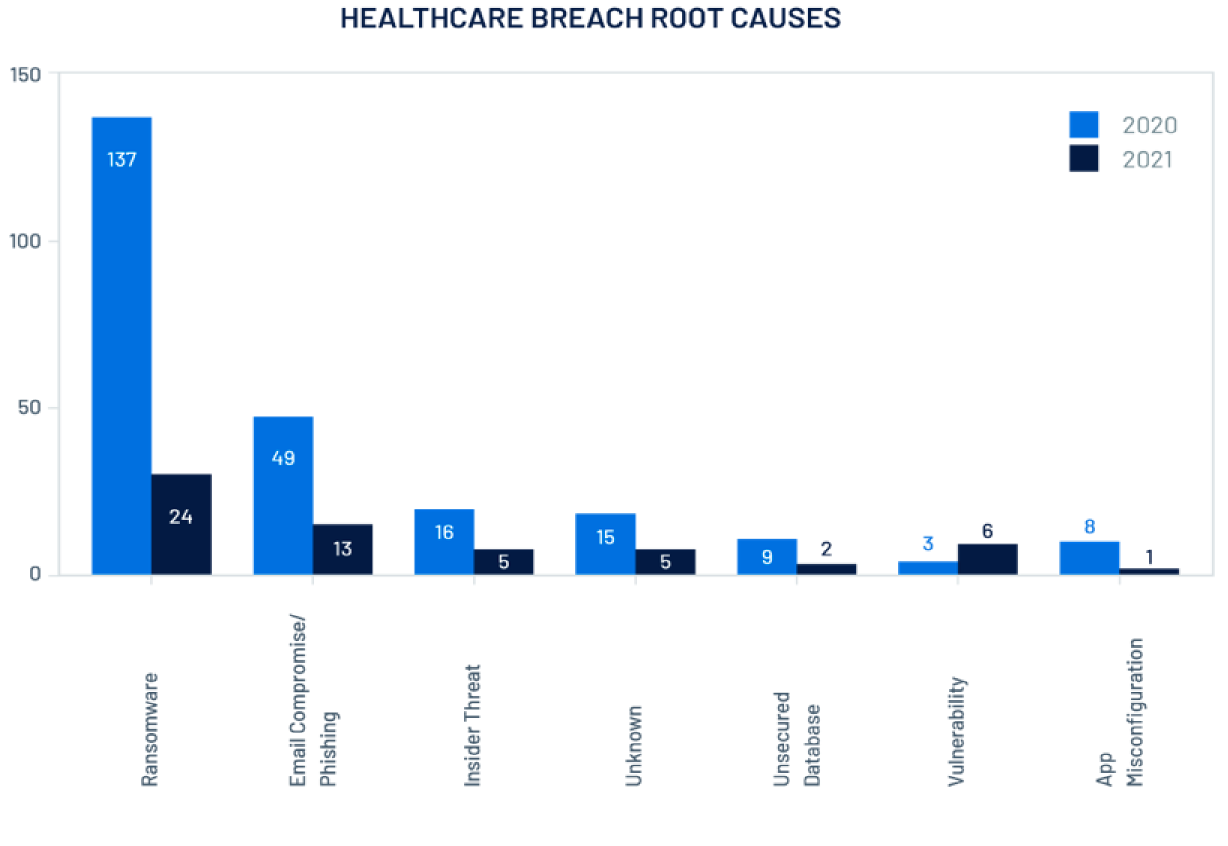
## Trends in Cybercrime

The healthcare industry is one of the most targeted by cyber-criminals. Attackers are more interested in hacking the healthcare industry due to the massive amounts of data that this industry holds. The healthcare industry stores valuable data such as personally identifiable information, credit card, and debit information that can be sold in the black market or extort patients' money. The healthcare industry also uses weak security measures that make it easy for adversaries to gain unauthorized access (Pifer, 2021).

Numerous reports cite that ransomware attacks are the most common attacks facing the healthcare industry, and these attacks have led to a significant rise of data breaches in the healthcare. The figure below represents number of incidents of various attack vectors in 2020 and the first two months of 2021.

**Figure 2**

*Main causes of healthcare data breaches*



*Source: Tenable Research analysis of publicly disclosed healthcare breach data, January 2020 – February 2021.*

Based on figure, the healthcare industry faced a total of 237 cyber-crime incidents in 2020. In 2021, the healthcare had already recorded 56 breaches just in the first two months._Ransomware attacks are the most common attack technique used by adversaries to compromise healthcare systems. From the figure above, ransomware incidents were 137 in 2020 and 24 between the first two months of 2021. Email phishing was the second cause of healthcare breaches, accounting for 49 incidents in 2020 and 13 incidents in the first two months of 2021. Insider threat was the third leading causing of healthcare breaches, accounting for a total of 16 recorded incidents in 2020, followed by unsecured database with 9 incidents, vulnerability and app misconfiguration accounted for a total of 11 incidents and 16 incidents in 2020 and first two months of 2021 respectively (Ikeda, 2021).

Ransomware attacks include sending malicious codes that can encrypt or delete sensitive data. Adversaries can conduct successful malware attacks through multiple techniques such as through email phishing, and tricking users into clicking malicious links or attachments. Since most healthcare providers are not trained on how to detect malicious links and attachments, they can be easily tricked into clicking or downloading malicious files. Once the files are downloaded, they will automatically execute into the victim system and give adversaries access into the network channel (Pifer, 2021). From the above table, we see that the healthcare sector also needs to be concerned about other techniques such as insider threat and unsecured databases.

Another important piece of data was the report provided by Check Point, which shows that in 2020, the healthcare industry recorded a 45% increase in cyber-attacks (Davis, 2021). This report also asserts that ransomware attacks are the most common in healthcare. This report by Check Point shows that Ryuk and Sodinokibi are the commonly used ransomware variants in these attacks. What is the impact of this increase of attacks?

Successful cyber-attacks can have negative financial impact on the healthcare sector and cause negative health outcomes to patients. Some of the leading healthcare centers, such as the Hollywood Presbyterian Medical Centers and Boston Children's Hospital, have faced serious data breaches that can cause financial and human loss (Winton, 2016). For instance, the malware attack targeted towards the Boston Children's Hospital affected more than 500 health providers, making it impossible for doctors to attend to their patients (Davis, 2020). This forced the patients to reschedule their visits, which could cause negative health effects to suffering patients who needed immediate attention.

As a result of the negative effects of cyber-attacks, the healthcare industry needs to implement the best security measures that will mitigate the rising cyber-attacks.

### How to prevent the cyber-breaches in the Health care industry

From the data findings presented, the healthcare industry needs to take a more proactive approach to prevent the increasing cyber-attacks. In order to stay ahead of the growing threat landscape, the healthcare industry needs to understand how adversaries think and the techniques that they apply when conducting attacks. The data collected show that the MITRE ATT&CK model provides the best strategy that the healthcare sector can apply to prevent against all types of attacks.

The MITRE ATT&CK model can help the healthcare industry avoid falling victim to cyber-attacks since this model emulates the reasoning of an adversary (Kwon et al., 2020). Through the application of the MITRE ATT&CK framework, the healthcare industry will understand the common tactics and techniques employed by attackers and use this information to implement preventive measures. For instance, the MITRE framework provides the path that attackers use to conduct successful attacks.

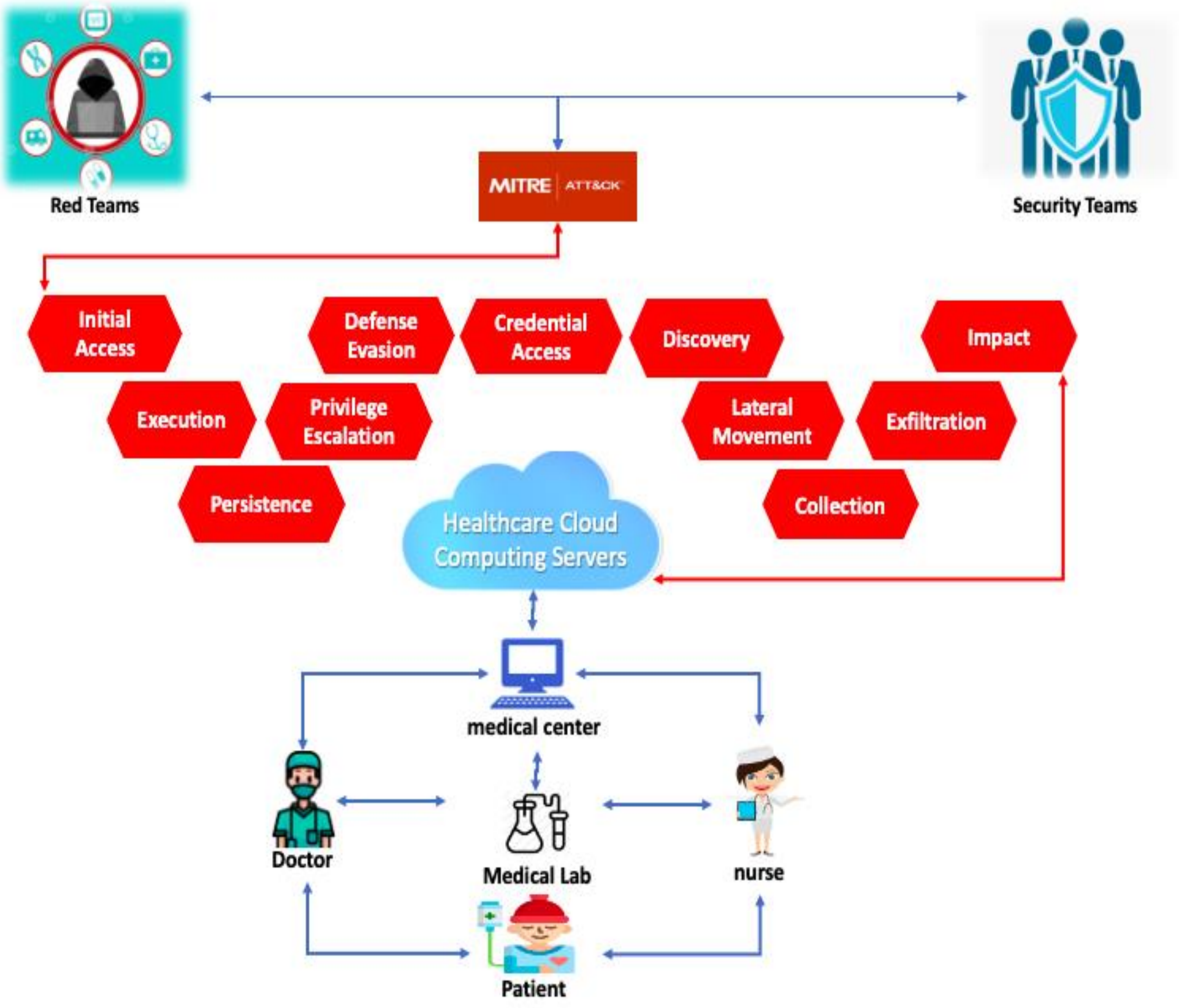
The healthcare IT team needs to map the most common attack vectors utilized by attackers to implement the best preventive strategy. The primary advantage of the MITRE ATT&CK framework is that it provides a comprehensive database of common attack techniques and provides real life examples of how attackers managed to infiltrate the network system. Through this framework, the IT team can learn from the mistakes of other organizations and take precaution measures to avoid falling victim of cyber-attacks. The MITRE ATT&CK model also offers a wide range of mitigation techniques that the healthcare team can apply to prevent against common attacks. This makes it simple for the IT team to prevent against cyber-attacks since they just need to follow the guidelines outlined in the MITRE ATT&CK model.

### How can the healthcare sector employ Mitre Att&ck Framework to attain their cloud security goals?

The healthcare industry can benefit from the MITRE ATT&CK framework by using it to map and understand current attacks. The MITRE ATT&CK model allows the healthcare industry to understand techniques and attack methods that adversaries can use to compromise their systems. The data collected indicate that the healthcare sector can use the MITRE ATT&CK framework to map the most common malware attacks. When analyzing the collected data, this paper also identified that MITRE had developed an independent Ransomware Resource for hospitals and healthcare providers. This resource was unveiled on March 3rd, 2021, and is designed to help hospitals and healthcare providers develop a resilient security process and policies that can be applied to the ever-changing threat landscape (Miliard, 2021).

**Figure 3**

*Utilizing the MITRE ATT&CK model by security teams of healthcare*



From figure 3 above, we see that healthcare security teams can stay ahead of the threat landscape by emulating the reasoning of red teams.  Figure 3 presents a step-wise model that the healthcare security teams can utilize to avoid being victims of cyber-attacks. The steps that the healthcare IT team should utilize based on figure 3 include;

1. **Initial Access –** At this stage, the attacker is trying to gain access to the network system. At this stage, attackers can use various techniques such as spearphishing and exploiting weaknesses present in the target system. At the initial access phase, the MITRE ATT&CK model defines techniques such as;

- Drive-by Compromise (T1189) – by using this technique, the adversaries target the users' browser in order to gain access into the target system. The adversaries can exploit the users' browser by using malicious ads or malicious codes such as JavaScript and iFrames. In the healthcare sector, the attackers can target the hospital's official website were users commonly visit and try to gain foothold into the system.

To prevent against this technique, the healthcare IT team should implement the following mitigation procedures;

- Application Isolation and Sandboxing – The IT team should install browser Sandboxes.
- Restrict web based content – the IT team can use ad blockers in to prevent against malicious codes that are spread through ads.

  - Update Software – To avoid users exploiting software vulnerabilities, the IT team should ensure that all software applications are updated.

Apart from the above described mitigation techniques, the healthcare can use applications such as firewalls and proxies to detect unusual activity. Using network intrusion detection systems combined with SSL/TLS can help detect initial access.

- External Remote Services (T1133) – Adversaries can use legitimate credentials to gain access into external remote services. For instance, attackers can compromise billing services using VPN and gain access into valid accounts. The attackers can also gain access by using services that do not require authentication. To gain access to external remote services, adversaries can use procedures such as wizard spider and night Dragon. Night Dragon has been effective in helping adversaries compromise VPN accounts and gain access to the target system. Wizard Spider conducts ransomware attacks and has been used to access victims' networks by using stolen credentials.

  In order to stay ahead of this threat, the following mitigation techniques should be applied;

  - Multi-factor authentication – the IT team should make use of two-factor authentication to verify users who have access to remote services.
  - Network segmentation - the IT team should deny remote access to internal network systems by using firewalls, network proxies and gateways.

- Limit access to resources over network – the IT team can limit access to remote resources by using applications such as VPNs.

The healthcare team can also detect external remote service activities by collecting authentication logs and analyzing unusual patterns. When authentication is not required in order to access remote services, the IT team should monitor for activities such as unusual use of exposed application or API.

- Phishing (T1566) – this technique entails sending phishing messages or emails in order to gain access to the target system. Phishing entails social engineering techniques such as sending emails containing malicious attachments or links. When users click on these malicious emails, the code executes itself in the target system and can be used for initial access. Some of the common procedures that have been used by attackers to conduct phishing attacks include Dragonfly and Gold Southfield. Dragonfly is a cyber-espionage group that has been able to conduct successful spearphishing campaigns to gain unauthorized access to victims system. Gold Southfield is used send malicious emails to gain access to the target machines.

In order to mitigate phishing attacks, the healthcare should apply the following mitigation techniques described in the MITRE ATT&CK model;

- Antivirus programs – installing antivirus programs will help quarantine any suspicious files or links. This will reduce chances of these files being executed in the target system.

  - Network intrusion prevention – the IT team should install network intrusion prevention systems such as File Transfer Protocols, Web Protocols and mail protocols to scan and automatically remove any suspicious files.
  - Software configuration – this entails using anti-spoofing and email authentication procedures to filter messages and help flag any suspicious messages.
  - User training – since spearphishing targets users and employees, the healthcare sector should train its users and staff on how to identify phishing emails. Users should also restrict from clicking links from suspicious sources (Jensen et al., 2017).

The healthcare industry can also use network intrusion detection systems and email gateways to detect malicious attachments and links.

- Cloud accounts (.004) – In this attack, adversaries obtain and abuse cloud accounts as a way of gaining initial access. Since the healthcare is moving to the cloud, it should apply the following mitigation measures;
  - Multi-factor authentication – the IT team should use multi-factor authentication for cloud accounts.
  - Password policies – all cloud accounts should have strong and complex passwords that are hard to guess. These passwords should also be update regularly.

- User account management - the IT team needs to periodically review cloud accounts and delete those no longer being used. It is also necessary to limit the number of users who have access to cloud accounts.

Monitoring cloud accounts to identify malicious activities is a good detection strategy.

2. **Execution –** At this phase, the malicious actor runs a malicious code in the target system. Some of the techniques that adversaries use here include;

- Power Shell - At this level, attackers can use PowerShell, which is a powerful scripting environment found in windows operating systems. This tool can allow attackers to perform actions such as information discovery and execute malicious codes. For instance, while investigating DarkSide Ransomware, PowerShell was identified as a common technique (Nuce et al., 2021). The DarkSide Ransomware was first discovered in 2020, and it operates as a ransomware-as-a-service (RaaS) variant that is capable of targeting large organizations such as hospitals. This malware utilizes techniques such as PowerShell (T1086), Account Discovery and File Permission Modification.

In order for the healthcare industry to prevent against the DarkSide malware, the IT team should apply preventive measures outlined in the MITRE ATT&CK framework such as using antivirus programs, code signing, disabling or removing programs and privilege account management.

- Anti-virus programs should be installed in all computer systems to automatically quarantine suspicious files.

  - Code signing entails setting PowerShell execution policy to execute only signed scripts. This will prevent malicious actors from using PowerShell to execute malicious codes.
  - Sometimes, removing programs such as PowerShell from the system can help prevent against attacks. However, the IT team must assess the impact of removing such programs. Without taking the necessary preventive measures, attackers can exploit the healthcare industry by using these tactics.

The IT team should turn on PowerShell logging to increase its detection capabilities.

- Malicious Link – In this technique, adversaries aim at sending malicious links to users. When users click on these malicious links, the code will be executed in the target system and give adversaries a chance to execute an attack.

To help prevent against these, the following mitigation techniques should be applied;

  - Network Intrusion Prevention – The IT team should install network intrusion systems to scan and remove any malicious links of downloads.
  - Restrict Web-Based content – The IT team should block unknown links or files and prevent them from being executed.
  - User Training – users should be trained on how to avoid malicious links and files. If links originate from an untrusted source, users should avoid clicking or downloading files.

For detection purposes, the IT team needs to regularly inspect network traffic to see if users visited malicious sites. Installing ant-virus programs can also improve detection capabilities.

3. **Persistence –** At this level, the attackers are trying to maintain their foothold in the system. The techniques that adversaries can use at this phase in the healthcare industry include;

- Account manipulation – In order to maintain access into the target systems, adversaries can manipulate account. Account manipulation consists of various actions that preserve adversary access to the victim system. In order to achieve this, the attackers can use procedures such as APT3, Calisto, Lazarus Group and Dragonfly 2.0. APT3 procedure is used to add newly created accounts to the local admin groups in order to maintain elevated access (Izycki & Vianna, 2021). This makes it really difficult for IT teams to detect the attackers. Calisto procedure is used to add permissions and remote logins to the system users. Lastly, the attackers can also use Dragonfly 2.0 to add newly created accounts to the admin group so as to maintain elevated access. Lazarus Group on the other hand is a malware program that contains functions that can be used to rename admin’s accounts.

In order for the healthcare to stay ahead of this threat, the IT team should employ the following Mitigation techniques;

- Multi-factor authentication – The healthcare IT team should require users to verify their accounts using two or more evidence such as username and password. To avoid account manipulation, the IT team should use multi-factor authentication for all system users and privileged accounts. For additional cloud credentials, the multi-factor authentication techniques should also be used to for user and privileged accounts.
- Network Segmentation – The IT team should configure tools such as firewalls that will help limit access to critical systems. Since the healthcare is moving to the cloud, the IT team can utilize cloud environments that support separate virtual private cloud (VPC) instances. Using VPC instances will help the healthcare industry segment cloud systems and thus avoid being attacked.
- Privileged account management – In this technique, the healthcare IT team should avoid using admin accounts for day-to-day operations that can expose them to adversaries.

The healthcare IT team can detect account manipulation by monitoring use credentials at unusual times or any other suspicious activity. The IT team should also monitor for unusual permission changes as this can suggest account manipulation.

- Additional Cloud Credentials – In this technique, attackers try to add controlled credentials to the healthcare cloud account in order to maintain persistence access to the target victim cloud accounts.

To mitigate additional cloud credentials, the following mitigations should be employed;

- Multi-factor authentication – all privileged accounts should use multi-factor authentication.
- Network segmentation – the IT team should configure access controls and firewalls in order to limit access to domain controllers and other critical systems.

Apart from the above mitigation measures, the healthcare IT team can also monitor unusual credential activities in order to detect any illegal activity.

- Cloud account – This is another common technique that attackers use to maintain persistence. Adversaries create cloud accounts in order to maintain access to the target systems.

The mitigation techniques that should be applied here to prevent attackers from using cloud accounts to maintain access include;

- Multi-factor authentication – before gaining access to the system, users must past multi-factor authentication test.
- Network segmentation – the IT team should configure tools such as firewalls and access controls to limit access to critical systems.

To detect cloud account usage, the IT team should consider collecting usage logs obtained from admin accounts and cloud user accounts and monitor any unusual activities.

4. **Privileged escalation –** At this level, the attackers are attempting to gain higher level permissions in the system network such as root level, local administrator, user accounts with admin access and user accounts with specific functions.

Some of the techniques which attackers can use to gain higher level permissions include; abuse elevation control mechanism, bypass user account control, access token manipulation and cloud accounts.

Since the healthcare industry is rapidly migrating to the cloud, the IT team should be concerned about this technique;

- Cloud Accounts - Through this technique, adversaries aim at obtaining and abusing credentials of cloud accounts, with the goal of gaining Initial Access, Persistence, Privilege Escalation or Defense Evasion.

To mitigate this attack, the healthcare industry can use the mitigation techniques outlined in the MITRE ATT&CK framework such as;

- Applying multi-factor authentication - Multi-factor authentication feature will ensure that only the authorized users have access to privileged accounts (Ometov et al., 2018).
- Password policies - Implementing password policies will ensure users create complex passwords that are hard to crack. Users should also be encouraged to regularly update their passwords.
- Privileged account management – This involves reviewing cloud account permission levels regularly to analyze those accounts that can allow attackers gain wide access.

To detect attacks on the cloud, the MITRE ATT&CK model suggests actively monitoring the activity of cloud accounts to detect any malicious behavior.

5. **Defense evasion –** at this level, the attacker is avoiding being detected. Some of the common techniques that the healthcare sector should watch out for include;

- Access Token Manipulation – attackers can edit access tokens in order to operate under a different user to avoid being detected.

To avoid access token manipulation, the following mitigation procedures are required;

  - User account management – all accounts should be restricted only to authorized users.
  - Privileged account management - the IT team needs to limit permissions so that users and user groups cannot be able to create tokens.

To detect access token manipulation, the healthcare sector can monitor and audit command line activity.

- Delete cloud instances – to avoid being detected, adversaries can delete cloud instances after executing malicious activities. By deleting cloud instances from the target machine, it can be almost impossible to detect that the system has been compromised.

The suggested mitigation techniques by the MITRE ATT&CK model include;

  - Audit – routinely checking for user permissions ensures that only the authorized users can deleted new instances.
  - User account management – permissions for deleting new instances should be limited based on least privilege. Only few users should have administrative roles to delete new instances.

The healthcare team should monitor their cloud environments on a regular basis to detect any unusual activity such as creation of an instance by a new user may indicate an unusual activity.

6. **Credential Access –** At this level, the attacker is trying to steal passwords and account names. Common techniques used include;

- Brute Force **–** brute force techniques are used to obtain passwords through guessing.

The mitigation techniques for this attack include;

- o Multi-factor authentication – use multi-factor authentication even on external services.
- o Password policies – users should set strong and unique passwords that are hard to crack.
- o Account use policies – after a certain number of failed login tries, the account should be locked.

In order to detect brute-force attack, the IT team should actively monitor authentication logs and application login failures to identify unusual activities.

- Credentials from web browsers – Web browsers are another target for obtaining credentials. Web browsers save credentials such as usernames and passwords that can be obtained by attackers.

The suggested mitigation technique for this attack is using password policies. Password policies should define the technical controls and user training to prevent attackers from obtaining web browser credentials.

For detection purposes, the IT team should monitor web browsers for identify malicious activities.

7. **Discovery –** At this stage, the adversaries apply multiple techniques that help them figure the victim environment. The techniques used here aim at helping the adversaries gain detailed knowledge about the target system and internal network. While multiple techniques can be used at this level, this paper will only discuss those that can be applied in the healthcare industry. Some of these techniques include;

- Account Discovery – at this phase, adversaries try to get all the accounts on the victims system. Gaining this information is important to attacker since they determine the specific accounts that exist to help in follow-on behavior.

To mitigate this technique, the healthcare IT team should configure the operating system. Operating system configuration is a mitigation technique that will help prevent admin accounts from being enumerated during application elevation using UAC.

In regard to detection, data and events should be analyzed as a chain of behavior that can introduce other activities. Therefore, any unusual chain of events should be considered a risk factor.

- Cloud account – Many industries, including the healthcare sector is utilizing cloud computing. Due to this, adversaries can attempt to gain a list of all the cloud accounts during account discovery. Cloud accounts are created and configured by organizations to enable users have remote access to the system. Adversaries can use various commands depending on the cloud service used to obtain a list of cloud account. For instance, if the organization uses AWS cloud, the attacker can use the command "aws iam list-users" to obtain cloud accounts.

The mitigation techniques that the healthcare IT team can apply to prevent account discovery include;

- Audit **–** through auditing, the IT team should regularly check user permissions to guarantee that only authorized users can discover cloud accounts.
- User account management – The IT team should limit permission to discover cloud accounts. Only specific accounts should have access to cloud accounts.

The IT team can also employ detection techniques such as monitoring command-line arguments and logs to detect malicious actions that can be used to collect information about cloud accounts.

8. **Lateral movement –** At this level, the adversary is attempting to move through the target environment and covers techniques that allow attackers to enter and control the target system remotely. Commonly used techniques as described by MITRE include;

- Exploitation of remote services – adversaries exploit remote services in order to gain access into the victim's network. Attackers can utilize system vulnerabilities such as programming error to exploit remote services.

Some of the mitigation techniques which can be applied here include;

- Disabling or removing programs – only necessary remote services should be available. If the services are not necessary, they should be disabled or removed.
- Threat intelligence program – have a good threat intelligence to identify software vulnerabilities that can be exploited by adversaries.
- Update Software – regularly updating software programs can help remove vulnerabilities.

Detecting software exploits can be challenging. However, by monitoring the behavior of endpoint systems, the IT team can detect compromised systems.

- Internal spearphishing – adversaries can use spearphishing techniques such as sending malicious links and files to deliver payload or obtain user credentials.

Mitigating internal spearphishing is almost impossible since this technique utilizes abuse of system features. The healthcare can however detect internal spearphishing by using network intrusion systems and email gateways.

9. **Collection –** Collection entails techniques that aid in the collection of data of interest. The next step after collection is to steal the data. The adversaries can target sources such as driver types, emails and browsers to collect data. The techniques that the healthcare sector should be concerned about include;

- Data from cloud storage object – If the healthcare has improperly secured cloud storage, attackers can collect data objects. By moving to the cloud, the healthcare can utilize various cloud service providers such as Amazon S3, Azure Storage or Google Cloud Storage. When storing data in these cloud platforms, attackers can easily collect data if the cloud storage is improperly secured. Adversaries can use procedures such as Fox Kitten to obtain files from the target cloud storage instances.

To prevent attackers from collecting data from the cloud storage, the healthcare should apply the following mitigation techniques;

- Audit – the IT team should frequently check permission on the cloud storage to prevent unauthorized access.
- Encrypt sensitive information – the IT team should ensure that data stored on the cloud is encrypted and that the encryption keys used are properly managed. Encrypt data will make it hard for adversaries to make use of it even if they manage to collect it.
- Filter network traffic – the healthcare sector can use IP restrictions to limit who can access cloud data. IP-based restrictions help to validate users from expected IP ranges and mitigate adversaries from using stolen credentials to access data.
- Multi-factor authentication – using multi-factor authentication can also help prevent unauthorized access to restricted files and cloud storage APIs.

  - User Account management – The IT should consider configuring user permissions and define who can access cloud storage. Using Identity Access Management controls can help in preventing unauthorized users from accessing cloud storage.

The healthcare organization can also detect unusual activity in the cloud storage by actively monitoring unusual queries.

- Email Collection - This is another technique that attackers can use to collect data needed for exfiltration. In this technique, the adversaries target user emails with the goal of collecting sensitive information such as trade secrets and personal information. This information can be valuable to adversaries and used to perform attacks. By hacking into the organization's email system, the adversaries can also collect or forward mail clients or servers. The healthcare industry should be worried about the Silent Librarian procedure that has been used since 2013 by adversaries. The Silent Librarian has been well known for targeting government agencies and private companies globally.

The mitigation techniques that the healthcare industry can apply here include;

  - Audit – the IT team should implement monitoring solutions to the email system. The admin can also use Get-InboxRule to discover malicious auto-forwarding rules.
  - Encryption – encrypting sensitive information shared of email can help prevent adversaries from stealing and making use of this information.

- Multi-factor authentication – the healthcare IT team should use multi-factor authentication for the organization’s mail servers.

For detection purposes, the healthcare IT team should monitor processes and command-line arguments for actions that could be taken to gather local email files.

10. **Exfiltration –** At this level, the attackers are trying to steal organization data. To steal data, attackers can use various techniques such as;

- Exfiltration to cloud storage - The attacker can use cloud storage services such as Dropbox and Google Docs to exfiltrate data. Exfiltration to these commonly used cloud storage services provides a good cover for the adversary, more so when the hosts within the network are already using this service.

The MITRE ATT&CK model suggests restricting web-based content as a mitigation technique. Restricting web-based content entails using web proxies to enforce external network communication and prevent use of external services that are unauthorized (Alexander et al., 2020).

The IT teams can detect this automated exfiltration attacks by monitoring process file access patterns and network behavior.

- Transfer data to cloud account – attackers can steal data by moving it to other cloud accounts where they can easily control the data.

The mitigation techniques for this attack include;

- Filtering Network Traffic – network filters will restrict transfer of data to untrusted cloud accounts.

- o Password policies – having strong passwords can help reduce chances of stealing credentials.

To detect this attack, the IT team needs to monitor account activities to detect attempts to transfer data.

11. **Impact –** At this stage, the adversary has already collected the needed data and is attempting to manipulate and destroy the data and the systems that they had access to. At this phase, attackers use techniques that disrupt the availability of data and resources and compromise the integrity of operations. Some of the techniques that the healthcare should watch out for include;

- Data encryption – adversaries may encrypt the organizations data, making it impossible for the healthcare to use it. Encrypting sensitive data is used by adversaries to demand for monetary compensation from the victim. In most cases, adversaries use malware programs that can encrypt data stored in the cloud without being easily detected.

The mitigation technique is;

- o Data Backup – The healthcare should implement a disaster recovery plan that outlines how cloud data is stored and ensure that a copy of the data is stored in another location.

To detect impact, the healthcare IT team should use process monitoring to keep track of command line parameters that are used to create suspicious files. Since the healthcare is migrating to the cloud, the IT team should also monitor for events that show that storage objects have been replaced anomalously by copies.

- Network Denial of Service **-** Adversaries can conduct DoS attacks to make critical resources unavailable for users. DoS attacks are common and thus the healthcare needs to be concerned about this attack and implement the most suitable mitigation techniques (Tupakula & Varadharajan, 2013).

  Based on the MITRE Att&ck framework, the IT team should implement the following mitigation technique;

  - Filter network traffic to detect any unusual traffic – Filtering network traffic will ensure that the servers or cloud services are not overloaded with unwanted traffic.

  The IT team can also use tools such as netwflow and SNMP to aggressively monitor network traffic in order to detect Network DoS before the traffic volume becomes enough to affect availability of services.

- Data manipulation - This entails deleting, inserting or manipulating data. Data manipulation can have adverse effects in the healthcare sector. This is majorly because the healthcare industry depends on data to make critical decisions. If the patient’s data is manipulated or deleted, it may lead to misdiagnosis and make it challenging to conduct normal business operations.

  To prevent against data manipulation, the healthcare can apply the following mitigation techniques;

- Encrypt sensitive information – all information stored and shared over the cloud should be encrypted to prevent adversaries from manipulating data.
- Remote data storage – the healthcare should back-up all sensitive data in a different location.
- Network segmentation – Identify services and critical systems that are more likely to be a target and isolate and secure them properly.

To detect data manipulation, the IT team can inspect important file hashes and any modification of suspicious values.

From the data collected, the MITRE ATT&CK model is one of the best since it can help define tactics used by attackers, identify current threats and provide the best mitigation measures that can be applied (Kwon et al., 2020).

### Data Analysis

From the data findings recorded, it is evident that the healthcare industry can benefit from the MITRE ATT&CK model since this framework offers a comprehensive analysis of the techniques that adversaries employ to conduct attacks. The MITRE ATT&CK framework is the most applicable preventive and recovery method since it provides a wide range of attack models and steps that attackers use to infiltrate computer systems (Georgiadou et al., 2021). By understanding this, the healthcare red teams can use the MITRE database to check out current attacks and what they can do to prevent this attack (Alexander et al., 2020). For instance, the cyber-attacks directed towards the Hollywood Presbyterian Medical Center could have been controlled if the hospital’s IT team had used the MITER ATT&CK framework; it would have understood how to prevent a Ransomware attack. In this attack, the attackers forced the hospital to pay a $17 0000 ransom in Bitcoin to allow access to its computer systems. The attackers used a malware program that encrypted the hospital's files, making crucial services unavailable. The malware program was capable of preventing the healthcare staff from communicating using digital devices, making delivery of services impossible. The Presbyterian cyber-attack forced the hospital to return to pen and paper.

The Hospital could have avoided this attack if the IT team had utilized the MITRE ATT&CK framework. Ransomware attacks are relatively common in the healthcare industry. This is why MITRE formulated a dedicated website for mapping healthcare malware attacks. This database was launched in 2020. With the help of this database, the healthcare industry can gain an in-depth understanding of the current malware attacks and techniques that cyber-criminals can utilize to deploy successful malware attacks.

### Summary

The healthcare industry is one of the most targeted industries by cyber-criminals. The data findings suggest that attackers are more interested in the healthcare industry due to the weak security measures used and the value of data stored by the healthcare sector. The healthcare sector leads in the number of cyber-attacks, which indicates that the industry lacks quality frameworks for staying ahead of the growing threat landscape. The healthcare industry also stores highly valuable data, such as personally identifiable information, credit and debit card information, and patient's health conditions. This data can be easily sold in the underground black market, used to black-mail patients, perform identity theft, or be used to execute other crimes. The cost impact of cyber-crimes is high, which calls for the need to take a more proactive approach to avoid being attacked. This report proposes using the MITRE ATT&CK model since it offers a more comprehensive approach to security.

The MITRE ATT&CK framework offers matrixes and tactics that attackers use. By understanding the adversaries' minds, the healthcare industry can take preventive measures to avoid falling victim to cyber-attacks.  The MITRE ATT&CK model is the bests since it offers a rich actionable respiratory of techniques and procedures used by attackers. As the healthcare industry is investing in the migration to the cloud, it is important to consider using the MITRE ATT&CK, as it offers a detailed public knowledge base listing the tactics and techniques used by attackers. Some of the common methods that attackers use include active scanning, vulnerability scanning, and hardware and software scanning. Understanding these reconnaissance techniques is important to cyber-security experts since it will allow them to take the most preventive measures against these attack techniques.

# Chapter V: Results, Conclusion, and Recommendations

## Introduction

The goal of this research is to identify the techniques of the Mitre Att&ck model that can help the healthcare sector improve its security posture as it migrates to the cloud. The results and conclusion section will cover the main points of the study and summarize the key findings of the above research. Through this section, readers will get a clear outline of what the research involves, its importance and why the suggested solutions should be implemented. This section will also explain why the selected topic is important and relevant in the current world. The goal of this section is to present the results of the study and provide recommendations. The results of this study will be presented based on the formulated research questions; what trends do statistics on cyber breaches in the healthcare display?  What should be done to halt the positive trend in increasing cyber breaches in the healthcare sector? How can the healthcare sector employ the techniques described in the Mitre Att&ck Framework to attain their cloud security goals?

## Results

The purpose of this research is to understand how the healthcare sector can utilize the techniques of the Mitre Att&ck framework to stay a head of the growing cloud cyber-security threats. To accomplish this, data was collected through qualitative methodology. The qualitative research design was chosen since it aims at gaining insights into a particular problem and exploring solutions that can be implemented. Through the qualitative research methodology, data for this study was collected from multiple reputable sources such as Google Scholar. The data was then analyzed using content analysis to extract only meaningful information related to this study.

Moving to the cloud

The healthcare industry is making massive investments in cloud computing. This is because cloud computing makes it easier for the healthcare sector to store and access data as compared to the traditional in-house servers. Moving to the cloud also will help the healthcare organization cut on costs that could otherwise be used in purchasing expensive systems. Moving to the cloud also offers the healthcare industry unlimited processing power. Healthcare companies can now process vast amounts of data such as DNA sequencing data and use this information to understand more about certain conditions. Due to these advantages, the healthcare is rushing to move to the cloud, ignoring the associated security concerns. Studies show that while moving to the cloud presents a myriad of advantages, it opens a high-way for conducting unlimited cyber-attacks. Moving to the cloud has led to a significant increase of cyber-attacks.

### What trends do statistics on cyber breaches in the healthcare display?

The results indicate that migrating to the cloud has led to a significant increase of cyber-attacks targeting the healthcare industry. Cloud computing is one of the leading disruptive technologies and companies are forced to adapt or else they will be left behind. The healthcare industry also has no option but to adapt this new technology and harness its advantages. The advantages of moving to the cloud include lowering costs and ease interoperability in the healthcare sector. Despite these advantages, moving to the cloud raises serious security concerns which the healthcare industry must address.

From the data findings, it was established that the healthcare industry is the most targeted by cyber-criminals.

The healthcare industry leads in the number of cyber-attacks, and this can be attributed to weak security measures (Martin et al., 2017). While moving to the cloud, the healthcare industry has not prioritized security, which makes it an easy target by cyber-criminals. Due to lack good security measures, adversaries can employ different attack techniques and gain unauthorized access into the healthcare sector. The literature reviews shows that various healthcare centers such as the Hollywood Presbyterian Medical Center, the Boston Children's Hospital, and the Dusseldorf University Clinic have been affected by cyber-attacks that made it impossible for these centers to continue their normal business operations. Apart from stealing patient's data, attackers can hold sensitive data ransom and demand payment from the healthcare centers. Successful cyber-attacks also can make the healthcare liable for lawsuits and affect its reputation.

### What should be done to halt the positive trend in increasing cyber breaches in the healthcare sector?

To help the healthcare stay ahead of the growing threat landscape, this research suggests the use of the MITRE ATT&CK framework. The MITER ATT&CK framework is a database that outlines all techniques and attack vectors that adversaries can use to infiltrate into network systems. The Mire Att&ck model also outlines the best mitigation and detection measures that organizations moving to the cloud can use to prevent against common attacks.

**How can the healthcare sector employ the techniques described in the Mitre Att&ck Framework to attain their cloud security goals?**

From the Mitre Att&ck framework, this research identified 11 tactics that attackers can follow to hack into the healthcare systems. The tactics discussed include; initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, exfiltration, and impact. At the initial access, adversaries are trying to gain a footprint into the target system. Adversaries can use techniques such as spearphishing and exploiting vulnerabilities in public servers to gain access to accounts. The healthcare organization can prevent these attacks by applying mitigation techniques such as restricting web-based content and user training as suggested by the MITRE framework. During execution, attackers try to run malicious program codes in the target machine. In the persistence stage, the adversary has already executed the malicious code and is trying to maintain its presence in the target system. Attackers can use techniques such as cloud accounts where they obtain and abuse cloud credentials to gain unauthorized access into the victim's system.

The next step is privilege escalation, where attackers are trying to gain higher permissions such as admin credentials or system root-level access. Techniques such as access token manipulation can be used to gain higher level access, allowing attackers to perform malicious activities without being detected. The mitigation techniques suggested at this stage include user account management and privileged account management. To avoid being detected, the adversaries use defense evasion techniques such as abuse elevation. When the adversary cannot be traced, he/she tries to steal account names and passwords in the credential access stage. Common techniques such as Brute Force can be used to gather credential information. During discovery, the attackers attempt to understand how the environment works and gain knowledge about the victim’s internal network. After learning about the target environment, the adversaries use lateral movement to enter and control remote systems in the network. Techniques such as internal spearphishing are common at this stage.

The next step is collection, where attackers gather as much information as they can to accomplish their goal. Exfiltration stage involves stealing data that has been collected. The last stage, Impact, involves attempts to manipulate, interrupt or destroy the victim’s data. Techniques such as data encryption and manipulation are used at this phase.

By understanding all these techniques, the healthcare IT team understands the mind of the adversary and can apply preventive measures to avoid falling victim to such attacks. This paper provides all the mitigation and detection techniques that can help the healthcare industry prevent against common attacks.

From the data collected, common mitigation techniques that the healthcare IT team should consider implementing include; encrypting sensitive information, performing regular audits, network filtering and using network intrusion and prevention systems. Since the goal of adversaries is to gain unauthorized access into the healthcare organizations and steal sensitive information for malicious gains, the IT team must consider encrypting all sensitive information shared and stored on the cloud platform. Encrypting data will ensure that adversaries cannot manipulate this data or sell it for monetary gains. Apart from encrypting data, the IT team needs to manage user accounts and ensure that unauthorized users don’t have elevated permissions.

The IT team should also consider using intrusion and prevention systems in order to detect unusual activity and block malicious codes from being executed. In the literature review section, we saw that a majority of cyber-attacks directed to the healthcare organization are malware based. Malware attacks involve the use of malicious programs and codes that can exploit system vulnerabilities and give attackers access into the network system from remote locations. Due to the rise of malware attacks, the healthcare IT team should prioritize malware mitigation techniques. Some of the recommended mitigation measures include data encryption and using network intrusion systems.  Intrusion detection systems help flag malicious files and prevent them from being executed. Training the staff to avoid downloading or clicking emails from suspicious sources is also necessary. Adversaries make use of phishing techniques, where they send malicious links to system users. When these links are downloaded, the malware program executes automatically without detection. Therefore, employees should avoid clicking or installing unknown links and applications.

Through this research question, all the applicable techniques and mitigation measures were described in detail to enable the healthcare industry to understand how it can prevent cyber-attacks and stay ahead of threats by applying mitigation and detection measures.

## Conclusion

The purpose of this research is to evaluate ways through which the healthcare sector can stay ahead of the threat landscape by implementing the MITRE ATT&CK framework. The healthcare industry is moving to the cloud, and this has led to a significant increase of cyber-attack related cases. Many industries are moving to the cloud to reap the benefits of cloud computing such as increased speed of communication and easier management of data. Despite these advantages, moving to the cloud comes with a cost, increased cyber-breach. Attackers can utilize a wide range of attack techniques and gain unauthorized access to cloud accounts, and the healthcare leads in the number of attacks.

Based on the study, the healthcare is one of the most targeted industries, and this can be attributed to factors such as weak security measures and failure to prioritize security (Martin et al., 2017). The healthcare industry applies weak security measures that make it easy for adversaries to compromise cloud accounts, and this is evident from various attacks such as the Hollywood Presbyterian Medical Center, the Boston Children’s Hospital, and the Dusseldorf University Clinic attacks (Mattei, 2017). In these attacks the adversaries exploited weakness in the existing systems and gained access without being detected. Successful cyber-attacks have negative effects in the healthcare sector, and thus the need to find a solution to prevent these attacks. Cyber-attackers can steal sensitive data, encrypt the data and demand for a ransom, and even delete or modify sensitive information to affect normal business operations. To prevent these attacks and the associated negative effects, this paper suggests the use of the techniques described in MITRE ATT&CK framework.

The MITRE ATT&CK framework contains a myriad of techniques that adversaries can use to compromise cloud accounts. By using this framework, the healthcare organization can understand the adversaries mind and apply prevention and detection techniques to stay ahead of the growing threat landscape. This paper identifies 11 techniques that the healthcare IT team should be concerned about. These techniques include; initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, exfiltration and impact. By understanding these attack vectors, the healthcare can apply the prevention and detection techniques described under each technique and ensure that the healthcare cloud systems are free of attacks.

## Future Work

While this paper outlined the most important techniques used by adversaries, many techniques were still not covered. Future research should focus on exploring all the techniques that are described in the MITRE ATT&CK framework. Future studies should also analyze how the MITRE ATT&CK framework can be combined with other frameworks such as FAIR to guarantee 100% security.

## References

Ahmadi, M., & Aslani, N. (2018). Capabilities and Advantages of Cloud Computing in the Implementation of Electronic Health Record. *Acta Informatica Medica*, *26*(1), 24–28. https://doi.org/10.5455/aim.2018.26.24-28

Ahuja, S. P., Mani, S., & Zambrano, J. (2012). A survey of the state of cloud computing in healthcare, Netw. *Commun. Technol*, 12–19.

Alexander, O., Misha, B., & Jacob, S. (2020). *MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy*. 43.

Alharbi, F., Atkins, A., & Stanier, C. (2016). Understanding the determinants of Cloud Computing adoption in Saudi healthcare organisations. *Complex & Intelligent Systems*, *2*(3), 155–171. https://doi.org/10.1007/s40747-016-0021-9

Al-Shaer, R., Spring, J. M., & Christou, E. (2020). Learning the Associations of MITRE ATT&CK Adversarial Techniques. *ArXiv:2005.01654 [Cs]*. http://arxiv.org/abs/2005.01654

Basra, J., & Kaushik, T. (2020). *MITRE ATT&CK® as a Framework for Cloud Threat Investigation*. 27.

Bracken, B. (2021). *Cyberattacks on Healthcare Spike 45% Since November*. https://threatpost.com/cyberattacks-healthcare-spike-ransomware/162770/

Brook, C. (2020, April 23). *What is the MITRE ATT&CK Framework? | Digital Guardian*. https://digitalguardian.com/blog/what-mitre-attck-framework

Cilliers, L. (2014). Using the cloud to provide telemedicine services in a developing country. *SA Journal of Information Management*, *16*(1). https://doi.org/10.4102/sajim.v16i1.611

Davis, J. (2020, February 12). *Malware Attack Hits Boston Children's Hospital Physician Group*. HealthITSecurity. https://healthitsecurity.com/news/malware-attack-hits-boston-childrens-hospital-physician-group

Davis, J. (2021, January 5). *Healthcare Accounts for 79% of All Reported Breaches, Attacks Rise 45%*. HealthITSecurity. https://healthitsecurity.com/news/healthcare-accounts-for-79-of-all-reported-breaches-attacks-rise-45

Fakis, A., Hilliam, R., Stoneley, H., & Townend, M. (2014). Quantitative Analysis of Qualitative Information From Interviews: A Systematic Literature Review. *Journal of Mixed Methods Research*, *8*(2), 139–161. https://doi.org/10.1177/1558689813495111

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&amp;CK Risk Using a Cyber-Security Culture Framework. *Sensors*, *21*(9), 3267. https://doi.org/10.3390/s21093267

Griebel, L., Prokosch, H.-U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., Engel, I., & Sedlmayr, M. (2015). A scoping review of cloud computing in healthcare. *BMC Medical Informatics and Decision Making*, *15*(1), 17. https://doi.org/10.1186/s12911-015-0145-7

Holmes, A. (2019). *The rise of cyber attacks and data breaches against US hospitals has been linked to an uptick in heart attack deaths*. Business Insider. https://www.businessinsider.com/cyber-attacks-hospitals-rise-in-heart-attack-deaths-study-2019-11

Ikeda, S. (2021, March 18). *Rise in Healthcare Data Breaches Driven by Ransomware Attacks*. CPO Magazine. https://www.cpomagazine.com/cyber-security/rise-in-healthcare-data-breaches-driven-by-ransomware-attacks/

Izycki, E., & Vianna, E. (2021). *Critical Infrastructure: A Battlefield for Cyber Warfare?* https://doi.org/10.34190/IWS.21.011

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems*, *34*(2), 597–626. https://doi.org/10.1080/07421222.2017.1334499

Kang, A. (2019, May 21). *How to implement and use the MITRE ATT&CK framework*. CSO Online. https://www.csoonline.com/article/3396139/how-to-implement-and-use-the-mitre-attandck-framework.html

Kuo, A. M.-H. (2011). Opportunities and Challenges of Cloud Computing to Improve Health Care Services. *Journal of Medical Internet Research*, *13*(3). https://doi.org/10.2196/jmir.1867

Kwon, R., Ashley, T., Castleberry, J., McKenzie, P., & Gourisetti, S. N. G. (2020). *Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping* (p. 112). https://doi.org/10.1109/RWS50334.2020.9241271

Lilly, B., Ablon, L., Hodgson, Q. E., & Moore, A. S. (2019). Applying Indications and Warning Frameworks to Cyber Incidents. *2019 11th International Conference on Cyber Conflict (CyCon)*, 1–21. https://doi.org/10.23919/CYCON.2019.8756949

Liu, C., Singhal, A., & Wijesekera, D. (2020). Forensic Analysis of Advanced Persistent Threat Attacks in Cloud Environments. *IFIP International Conference on Digital Forensics*, 161–180.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ*, j3179. https://doi.org/10.1136/bmj.j3179

Mattei, T. A. (2017). Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack. *World Neurosurgery*, *104*, 972–974. https://doi.org/10.1016/j.wneu.2017.06.104

Mayring, P. (2014). *Qualitative Content Analysis*. 144.

Meisner, M. (2017). FINANCIAL CONSEQUENCES OF CYBER ATTACKS LEADING TO DATA BREACHES IN HEALTHCARE SECTOR. *Copernican Journal of Finance & Accounting*, *6*(3), 63. https://doi.org/10.12775/CJFA.2017.017

Meri, A., Hasan, M., Danaee, M., Jaber, M., Jarrar, M., Safei, N., Dauwed, M., Abd, S. K., & Al-bsheish, M. (2019). Modelling the utilization of cloud health information systems in the Iraqi public healthcare sector. *Telematics and Informatics*, *36*, 132–146. https://doi.org/10.1016/j.tele.2018.12.001

Merriam, S. B. (2002). Introduction to qualitative research. *Qualitative Research in Practice: Examples for Discussion and Analysis*, *1*(1), 1–17.

Merriam, S. B., & Tisdell, E. J. (2015). *Qualitative research: A guide to design and implementation*. John Wiley & Sons.

Michalas, A., Paladi, N., & Gehrmann, C. (2014, October 15). *Security Aspects of e-Health Systems Migration to the Cloud*. https://doi.org/10.13140/2.1.1616.7367

Miliard, M. (2021, March 3). *MITRE launches ransomware support hub for hospitals and health systems*. Healthcare IT News. https://www.healthcareitnews.com/news/mitre-launches-ransomware-support-hub-hospitals-and-health-systems

Morgan, S. (2021). *CYBERCRIME FACTS AND STATISTICS*. 19.

Nieuwenhuis, L. J. M., Ehrenhard, M. L., & Prause, L. (2018). The shift to Cloud Computing: The impact of disruptive technology on the enterprise software business ecosystem. *Technological Forecasting and Social Change*, *129*, 308–313. https://doi.org/10.1016/j.techfore.2017.09.037

Nuce, J., Kennelly, J., Goody, K., Moore, A., Rahman, A., Williams, M., McKeague, B., & Wilson, J. (2021, May 11). *Shining a Light on DARKSIDE Ransomware Operations*. FireEye. https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Oosthoek, K., & Doerr, C. (2019). SoK: ATT&CK Techniques and Trends in Windows Malware. *International Conference on Security and Privacy in Communication Systems*, 406–425.

Palumbo, A., & Buja, M. (2020, February 12). Malware Attack Disrupts Computers for Hundreds of Doctors in Mass. *NBC Boston*. https://www.nbcboston.com/news/local/malware-attack-disrupts-computers-for-hundreds-of-doctors-in-mass/2076031/

Pennington, A., Applebaum, A., Nickels, K., Schulz, T., Strom, B., & Wunder, J. (2019). *Getting Started with ATT&CK*. 45.

Pifer, R. (2021, June 24). *More than 1/3 of health organizations hit by ransomware last year, report finds*. Healthcare Dive. https://www.healthcaredive.com/news/more-than-13-of-health-organizations-hit-by-ransomware-last-year-report-f/602329/

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, *8*(2). https://doi.org/10.3390/healthcare8020133

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). *MP180360 MITRE PRODUCT*. 37.

Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers & Electrical Engineering*, *71*, 28–42. https://doi.org/10.1016/j.compeleceng.2018.06.006

Tupakula, U., & Varadharajan, V. (2013). Security Techniques for Counteracting Attacks in Mobile Healthcare Services. *Procedia Computer Science*, *21*, 374–381. https://doi.org/10.1016/j.procs.2013.09.049

Vuksanaj, K. (2019, January 11). Advancing Precision Medicine Using Cloud-Based Informatics. *GEN - Genetic Engineering and Biotechnology News*. https://www.genengnews.com/insights/advancing-precision-medicine-using-cloud-based-informatics/

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

Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: Innovation opportunities and challenges. *International Journal of Digital Earth*, *10*(1), 13–53. https://doi.org/10.1080/17538947.2016.1239771