EPiC Series in Computing

Volume 93, 2023, Pages 240–251

Proceedings of Society 5.0 Conference 2023

A Systematic Literature Review on Cybersecurity Threats to Healthcare Data and Mitigation Strategies

Khanyisile Vilakazi[1], and Funmi Adebesin[1]

[1] Department of Informatics, University of Pretoria, South Africa

khanyiv@gmail.com, funmi.adebesin@up.ac.za

Abstract

The incidence of cyberattacks on healthcare institutions has seen a steady increase over the years, with a massive increase of 42% in 2020. More specifically, INTERPOL reported a substantial increase in ransomware attacks on healthcare institutions at the height of the Covid-19 pandemic. This increase can be attributed to the rise in the adoption of digital technologies, such as the Medical Internet of Things (MIoT), to support healthcare services. The sensitive nature of healthcare data and the volume of data handled by healthcare institutions make them attractive to cybercriminals. When compared to financial data, healthcare data has more value on the dark web. Because a cyberattack on healthcare data could have far-reaching consequences, healthcare institutions should have effective strategies to safeguard unauthorized access. This paper presents the results of a systematic literature review (SLR) that investigated the strategies that can be used to mitigate cybersecurity threats to healthcare data. Forty-one research papers retrieved from three databases were analyzed based on specific inclusion/exclusion criteria. Synthesis of the sources yielded three main themes, namely, (i) emerging technology trends that contribute to cybersecurity vulnerability in the healthcare sector, (ii) current cybersecurity challenges in the healthcare sector, and (iii) cybersecurity countermeasures and mitigation strategies. The research results showed that a holistic approach that incorporates people, technology and adherence to regulations is required to mitigate cybersecurity threats in the healthcare sector. The study has implications for policymakers, vendors/designers of healthcare technologies, and healthcare institution managers.

Keywords

Cyberattacks, cybersecurity, cybersecurity incidents, healthcare data, mitigation strategies, systematic literature review

1 Introduction

The healthcare sector has historically lagged in the adoption and use of digital technologies (Iyanna, Kaur, Ractham, Talwar, & Najmul Islam, 2022). Some of the reasons for the slow pace of technology adoption include privacy and security concerns, poor interoperability among systems, and a generally low level of digital literacy among healthcare professionals (Tortorella et al., 2020; Tsai et al., 2020). However, the Covid-19 pandemic compelled several healthcare institutions to rapidly adopt digital healthcare technologies (De, Pandey, & Pal, 2020; Kelly, Campbell, Gong, & Scuffham, 2020; Sarfraz, Sarfraz, Iftikar, & Akhund, 2021). A consequence of the rapid adoption of digital technology was the rise in cybercrimes that targeted healthcare institutions (Lallie et al., 2021; Petracca, Ciani, Cucciniello, & Tarricone, 2020; Pranggono & Arabo, 2021). For instance, Forbes reported a massive 42% increase in cyberattacks on healthcare institutions in 2020 (Culbertson, 2021), while the International Criminal Police Organization (INTERPOL) flagged an increase in the number of healthcare institutions that were targeted with ransomware attacks (INTERPOL, 2020). Another factor that has contributed to the vulnerability of the healthcare sector to cyberattacks is the prevalence of legacy systems (Bhosale, Nenova, & Iliev, 2021). Some of the cybersecurity threats that have been reported in the healthcare sector include (Beaman, Barkworth, Akande, Hakak, & Khan, 2021; Bhuyan et al., 2020; Hijji & Alam, 2021; Pranggono & Arabo, 2021):

- Denial of service attack (DoS), where systems' resources become inaccessible to authorized users. A DoS can be on a single system or distributed across several systems, in which case it is referred to as a distributed denial of service (DDoS).
- Malware attack entails the deployment of malicious software to gain unauthorized access to computing resources.
- A ransomware attack involves the deployment of malware on a system by cybercriminals that prevent access to a system or threaten to publish personal data until a ransom is paid.
- A phishing attack uses social engineering to obtain sensitive information from an unsuspecting user, which could be used to commit a cybercrime.
- Social engineering exploits human weaknesses, ignorance and/or naivety to disclose sensitive personal information.
- Session hijacking occurs when an unauthorized user or computing device takes control of an online or web session.

Cyberattacks on healthcare data have long-term detrimental repercussions. When healthcare data is compromised, it is often difficult to restore the privacy or psychosocial harm that is caused (Argaw et al., 2020). In addition to compromising healthcare data, cyberattacks can hamper healthcare service, put patients' lives in danger and damage the reputation of the healthcare institution (Argaw et al., 2020). Table 1 provides a summary timeline of cybercrime incidents targeted at healthcare institutions at the height of the Covid-19 pandemic in 2020.

Given the rise in the incidents of cyberattacks on healthcare institutions, the purpose of this paper is to report on an SLR that investigated the strategies that could be used to mitigate such attacks. The remaining sections of the paper are structured as follows: Section 2 provides a detailed description of the research methodology. This includes the research question, the inclusion and exclusion criteria, source selection and the quality assessment of peer-reviewed papers included in the SLR. The results from the analysis of the 41 research papers are presented in section 3. The conclusion to the paper is provided in section 4. This includes the study's contribution, limitations, and implications.

Timeline	Cybersecurity Incident
13/03/2020	A ransomware attack on Brno University Hospital in the Czech Republic resulted in a shot-down of the computer system. This forced the hospital to cancel all operations and move patients to another hospital.
14/03/2020	A ransomware attack on Hammersmith Research Group in the United Kingdom resulted in the personal data of thousands of patients being published on the dark web following the institution's refusal to pay a ransom.
08/04/2020	Federal Bureau of Investigation (FBI) issued a warning about a backdoor Trojan known as "Kwampirs" malware targeting the healthcare sector. The Trojan granted remote access to attackers who then issue illegal instructions to computing devices.
28/04/2020	Microsoft issued a warning on various ransomware, including Maze, NetWalke, PonyFinal, REvil, RobbinHood, and Vatet loader that targeted critical healthcare services through the exploitation of Virtual Private Network vulnerabilities.
14/05/2020	A ransomware attack on a third-party cloud computing vendor in the United States resulted in a data breach that compromised the personal data of millions of patients.
09/06/2020	A cyberattack on Life Healthcare Group, the second-largest private healthcare group in South Africa caused the admission system, business processing system and mail servers to go offline, forcing the Group's hospitals to switch to manual processing.
10/06/2020	A data breach on a mobile health application (m-health app) in the United Kingdom allowed users to access video recordings of other patients' consultations while in a doctor's room.
18/09/2020	A data breach on Dental Care Alliance in the United States resulted in the personal data of about one million patients being compromised.
17/10/2020	A "Ryuk" ransomware attack on Sky Lakes Medical Center in the United States resulted in the non-availability of business and clinical applications.

Table 1: Timeline of cyberattacks on healthcare institutions in 2020

2 Research Methodology

The study followed an SLR based on the updated Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guideline (Page et al., 2021) and the SLR approach by Siddaway, Wood, and Hedges (2019). The research question explored was "*What are the strategies that could be used to mitigate cybersecurity threats to healthcare data"*. To scope the SLR process the following search strings were used: ("cyber") AND ("threat*" OR "attack*" OR "crime*") AND ("health*") AND ("data") AND ("secur*" OR "mitigate" OR "protect"). The searches were conducted over three databases, namely PubMed, Web of Science (WOS) and Scopus. Only peer-reviewed studies published between 2017 and March 2022 that focused on cybersecurity threats in the healthcare sector were considered for inclusion in the SLR. Studies that were not published in the English language were excluded. The source selection and screening process consisted of four phases, namely identification, screening, eligibility and inclusion (see Figure 1):

- The **identification phase** entailed searching and inputting the search strings into each of the three databases. The search strings were customized for the database as required. This process yielded a combined total of 1,395 sources from the databases, with 695 from Scopus, 615 from WOS and 85 from PubMed. An additional five articles were identified through the references in the sources included in the SLR, resulting in a total of 1,400 sources. The sources were exported into an Excel file using the following columns: Author, Title, Year, Abstract, Source Database, DOI, and Document Type. Using the

articles' titles, 69 duplicate sources were removed, leaving 1,331 records for the screening phase.

- In the **screening phase**, the remaining 1,331 records were screened using the inclusion and exclusion criteria. This process resulted in the exclusion of 780 records.
- During the **eligibility phase**, the remaining 551 records were assessed by reading their abstracts to determine their relevance. This phase resulted in the exclusion of an additional 473 records.
- Finally, in the **inclusion phase**, the remaining 78 records were assessed using four quality assessment (QA) criteria to determine their suitability for inclusion in the SLR. The QA criteria were (i) Does the study explain the different types of cybersecurity threats? (ii) Does the study focus on health data protection from cybersecurity threats? (iii) Does the study discuss strategies to protect health data against cyberattacks? (iv) Does the study reference other papers that are relevant to the current research? Sources that fully met a criterion were assigned the value 1, those that partially met a criterion were assigned 0.5, while the ones that did not meet a criterion were assigned 0. Each source could have a maximum score of 4 if it fully met all four QA criteria. Only sources that scored 2 points and above were included in the SLR. The QA process resulted in the elimination of 37 sources, leaving a final set of 41 papers for inclusion in the SLR.

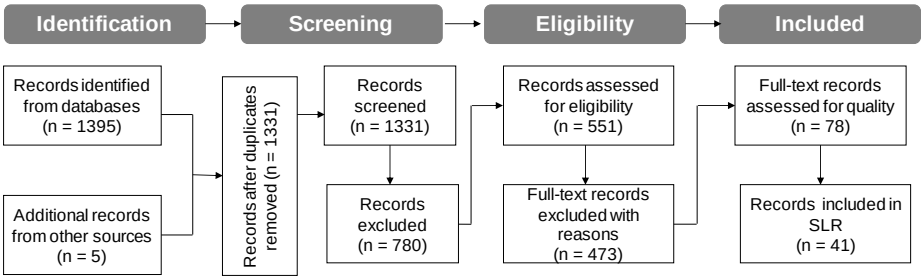

Figure 1: SLR Source selection process

3 Research Findings and Discussions

This section provides detailed discussions of the results obtained from the analysis of the 41 sources that were included in the SLR. Quantitative analysis of the 41 research papers using descriptive statistics showed that only three of the sources included in the SLR were published in 2017, there were six in 2018 and five in 2019. More than half of the sources, nine in 2020 and 14 in 2021, respectively were published at the height of the Covid-19 pandemic. This period was characterized by an unprecedented reliance on digital technologies to support healthcare services on the one hand (Petracca et al., 2020) and increased vulnerability to cyberattacks on the other (Gafni & Pavel, 2021). A decline in the number of publications in 2022, with only four, is because the sources included in the SLR were retrieved in April 2022. Hence, this number is not a true reflection of all relevant publications for 2022.

The research papers were also analyzed from a source database perspective. Almost half (19) of the sources included in the SLR were retrieved from WOS, followed by ten from Scopus, and seven from PubMed. The remaining five sources were retrieved through citations from the articles included in the SLR.

Following the descriptive quantitative analysis, a thematic analysis of the 41 research papers yielded three main themes, namely (i) emerging technology trends that contribute to cybersecurity vulnerability

in the healthcare sector, (ii) current cybersecurity challenges in the healthcare sector, and (iii) cybersecurity countermeasures and mitigation strategies. A summary of the themes and sub-themes that emerged from the research and their corresponding citations are provided in Table 2, while sections 3.1 to 3.3 provide their detailed discussions.

Theme/sub-theme	Authors
Emerging technology trends that contribute to cybersecurity vulnerability in the healthcare sector	
Medical Internet of Things (MIoT)	(Jagadeeswari et al., 2018; Sadek et al., 2022; Sun et al., 2018)
Big data	(Abouelmehdi et al., 2018; Abouelmehdi, Beni-Hssane, Khaloufi, & Saadi, 2017; Jagadeeswari et al., 2018; Seh et al., 2020)
Mobile health applications (m-health apps)	(Galetsi et al., 2022; Magrabi et al., 2019; Sannino, De Pietro, & Verde, 2020)
Cloud computing	(Ali et al., 2018; Dang et al., 2019; Jagadeeswari et al., 2018)
Current cybersecurity challenges in the healthcare sector	
Lack of cybersecurity policy	(Jalali & Kaiser, 2018; Pranggono & Arabo, 2021; Shah & Khan, 2020)
Human factor	(Bhuyan et al., 2020; Coventry & Branley, 2018; Ghafir et al., 2018; Hijji & Alam, 2021; Jalali, Bruckes, Westmattelmann, & Schewe, 2020)
Lack of consensus among stakeholders	(Jalali, Razak, Gordon, Perakslis, & Madnick, 2019; Meisner, 2018)
Inadequate investments in cybersecurity measures	(Abouzakhar, Jones, & Angelopoulou, 2017; Meisner, 2018)
Cybersecurity countermeasures and mitigation strategies	
Blockchain technology for security	(Attaran, 2020; El-Gazzar & Stendal, 2020; Jennath, Anoop, & Asharaf, 2020; Nagasubramanian et al., 2020; Shah & Khan, 2020; Shi et al., 2020; Siyal et al., 2019)
Data encryption	(Abouelmehdi et al., 2018; Alodaynan & Alanazi, 2021; Bhuyan et al., 2020; Elhoseny et al., 2021; Nagasubramanian et al., 2020; Zriqat & Altamimi, 2017)
Education and training	(Alodaynan & Alanazi, 2021; Bhuyan et al., 2020; Ghafir et al., 2018; Hijji & Alam, 2021; Kruse, Smith, Vanderlinden, & Nealand, 2017; Rajamäki, Nevmerzhitskaya, & Virág, 2018; Washo, 2021)
Password security	(Bhuyan et al., 2020; Dias, Martens, Monken, Silva, & Santibanez Gonzalez, 2021; Elhoseny et al., 2021; Jalali & Kaiser, 2018; Nunes, Antunes, & Silva, 2021; Razaque et al., 2019)
Policies and Regulations	(Bentotahewa, Hewage, & Williams, 2022; Jalali & Kaiser, 2018; Offner, Sitnikova, Joiner, & MacIntyre, 2020; Papastergiou, Mouratidis, & Kalogeraki, 2021; Shah & Khan, 2020; Swales, 2021)
Management of IT infrastructure	(Alodaynan & Alanazi, 2021; Bhosale et al., 2021; Elhoseny et al., 2021; Jalali & Kaiser, 2018; Markopoulou & Papakonstantinou, 2021)
Intrusion detection	(Alodaynan & Alanazi, 2021; Elhoseny et al., 2021; Radoglou-Grammatikis et al., 2021)
Risk management	(Abraham, Chatterjee, & Sims, 2019; Bhuyan et al., 2020; Dias et al., 2021)
Access management	(Bhuyan et al., 2020; Elhoseny et al., 2021; Habib et al., 2019; Shah & Khan, 2020)

Table 2: Summaries of research findings

3.1 Emerging Technology Trends that Contribute to Cybersecurity Vulnerability in the Healthcare Sector

One of the factors that drive the vulnerability of the healthcare sector to cybersecurity attacks is advancements in new technologies and the pressure on the sector to adopt them at the height of the Covid-19 pandemic (Petracca et al., 2020). The adoption of technologies like MIoT (Sadek, Codjo, Rehman, & Abdulrazak, 2022; Sun et al., 2018), cloud computing (Ali, Shrestha, Soar, & Wamba, 2018; Dang, Piran, Han, Min, & Moon, 2019), big data (Abouelmehdi, Beni-Hessane, & Khaloufi, 2018; Jagadeeswari, Subramaniyaswamy, Logesh, & Vijayakumar, 2018), and m-health apps (Galetsi, Katsaliaki, & Kumar, 2022; Magrabi et al., 2019) have opened healthcare data to cyberattacks.

Although technologies like MIoT can facilitate personalized medical care, the interconnection of medical devices and transmission of healthcare data over the internet expose data and medical devices to cyberthreats (Sadek et al., 2022; Sun et al., 2018). Some of these threats include selective forwarding, sinkhole, jamming, and flooding attacks (Sadek et al., 2022; Sun et al., 2018). The nature of healthcare service dictates that healthcare organizations process large volumes of sensitive healthcare data (Bhuyan et al., 2020). Consequently, the increasing adoption of big data in the healthcare sector is another driver of cyberattacks on healthcare institutions. Although the adoption of big data for health offers several benefits, including efficient service, improved patient outcomes, and better prediction of disease outbreaks (Abouelmehdi et al., 2018), the sensitive nature of health data makes their transmission in large volumes over the Internet attractive to cybercriminals, who may disclose the data on the dark web (Abouelmehdi et al., 2018).

The adoption of cloud computing enables remote access to computing resources over the Internet anytime, anywhere, thus enabling efficient healthcare service delivery (Ali et al., 2018). However, the nature of cloud computing technologies increases the vulnerability of healthcare data to cyberthreats. Management of access to resources over the Internet, virtualization, and the multi-tenancy nature of cloud computing contribute to cybersecurity risks to healthcare data (Ali et al., 2018; Dang et al., 2019; Jagadeeswari et al., 2018).

The proliferation of smart mobile devices and the consequent increase in the development and access to m-health apps and wearable health devices offer enormous opportunities for individuals and healthcare professionals (Galetsi et al., 2022; Sannino et al., 2020). Health data can be transmitted from wearable devices and m-health apps to support remote monitoring. Individuals can also use wearable devices and m-health apps to proactively promote their well-being (Galetsi et al., 2022). However, there is a risk of interception while health data is in transit from wearable devices and m-health apps, on cloud storage and the devices (Sannino et al., 2020).

3.2 Current Cybersecurity Challenges in the Healthcare Sector

As discussed in section 3.1, the Covid-19 pandemic pressed many healthcare institutions to adopt digital technologies, including MIoT, m-health apps, and big data. This move aggravated the vulnerability of healthcare data to cyberattacks. In many instances, policymakers and healthcare institutions did not have adequate policies and regulations in place to protect healthcare data from unauthorized and malicious access (Jalali & Kaiser, 2018; Shah & Khan, 2020). Where policies are in place, they are not robust enough to deal with the risks associated with remote work environments (Pranggono & Arabo, 2021).

Another cybersecurity challenge that the healthcare sector had to contend with relates to human factor issues. It is not uncommon for cyberattacks on healthcare institutions to be the result of inadvertent acts or omissions by healthcare personnel (Bhuyan et al., 2020). Healthcare professionals are generally lacking in cybersecurity awareness, which could result in social engineering attacks (Bhuyan et al., 2020; Ghafir et al., 2018; Hijji & Alam, 2021). In addition, the management of healthcare institutions often has to rely on third-party service providers for the maintenance of their IT

infrastructure because IT skills are not a core capability (Jalali & Kaiser, 2018). Furthermore, healthcare stakeholders sometimes battle to reach a consensus on cybersecurity strategy formulation and implementation (Jalali & Kaiser, 2018). Finally, inadequate resources are often allocated to cybersecurity mitigation strategies (Abouzakhar et al., 2017; Jalali & Kaiser, 2018; Meisner, 2018).

3.3 Cybersecurity Countermeasures and Mitigation Strategies

One of the strategies that could be used to combat cybersecurity threats in the healthcare sector is blockchain. Blockchain is a technology that has been applied to cryptocurrency. The technology makes use of blocks for secure storage of data, with each block carrying the data from a transaction and the hash value from a preceding block, thus creating a coherent link between the blocks (Attaran, 2020; Nagasubramanian et al., 2020). Blockchain can be used for health data management and the protection of healthcare data (Attaran, 2020; El-Gazzar & Stendal, 2020; Jennath et al., 2020; Nagasubramanian et al., 2020; Shah & Khan, 2020; Shi et al., 2020; Siyal et al., 2019). The adoption of blockchain can mitigate cyberthreats and keep sensitive health data safe (Attaran, 2020). Authors like Attaran (2020); El-Gazzar and Stendal (2020) and Shi et al. (2020) argued that the adoption of blockchain for healthcare data security could lead to financial savings from expenses associated with data breach litigations. Blockchains can also be used to protect cloud-hosted health data through keyless encryption. In addition, blockchains can be used to control access to healthcare data (Nagasubramanian et al., 2020).

Another strategy that could be used to protect healthcare data from cybersecurity threats is data encryption. Using encryption-decryption algorithms, encryption facilitates secure data communication (Zriqat & Altamimi, 2017). The encryption of health data ensures that in the event of unauthorized access, the data cannot be read without the decryption code (Elhoseny et al., 2021; Zriqat & Altamimi, 2017).

Education and training are important components of a holistic strategy to protect healthcare data from cyberattacks. People are often seen as the weakest link in the strategies that are employed to protect an organization's information system resources against cyberthreats (Jalali et al., 2020). Healthcare professionals generally have limited computer skills (Ghafir et al., 2018). Hence, it is vital that all employees, irrespective of their rank, be sensitized to cybersecurity awareness (Bhuyan et al., 2020; Ghafir et al., 2018; Rajamäki et al., 2018). Training of IT personnel working in the healthcare sector is also important to improve their awareness of the sensitive nature of healthcare data. Increased awareness among all employees (both technical and non-technical) can play a huge role in the reduction of cybersecurity incidents (Rajamäki et al., 2018). Investment in user education and training can be offset through a reduction in the costs of litigations that could result from cyberattacks (Bhuyan et al., 2020; Rajamäki et al., 2018).

Another human factor-related mitigation strategy against cybersecurity attacks is password management. Access to computing resources and healthcare data should be restricted to users that have been authenticated through username and password (Bhuyan et al., 2020; Dias et al., 2021). It is not uncommon for end-users to use weak and easy-to-guess passwords. Hence, healthcare institutions should encourage, and when necessary, enforce the use of strong passwords by employees (Bhuyan et al., 2020; Dias et al., 2021). Some of the password security measures that could be incorporated into a holistic cybersecurity strategy include (Dias et al., 2021; Elhoseny et al., 2021; Jalali & Kaiser, 2018; Nunes et al., 2021):

- Compelling employees to select strong passwords, using a combination of upper and lower-case letters, numerical values, and special characters.
- Passwords should be changed regularly to ensure the security of users' accounts.
- Manufacturers and developers should avoid hard-coding of passwords in applications and medical devices to reduce the risk of password guessing by cybercriminals.
- Users should be educated on the dangers associated with the sharing of passwords.

Analysis of the research papers included in the SLR also showed that the stipulation of relevant policies and regulations is another non-technical measure to protect healthcare data from cyberattacks (Jalali & Kaiser, 2018; Shah & Khan, 2020). Data regulations can be stipulated by a country or region. For example, the Health Insurance Portability and Accountability Act (HIPPA) is a United States Federal law that prohibits the disclosure of a patient's health information without their consent (Jalali & Kaiser, 2018). Although not specifically aimed at health data, the European Union (EU) General Data Protection Regulation (GDPR) governs the collection and processing of personal data by institutions that operate from within the EU or outside the region, but which provide goods and services to anyone that resides in an EU country (Bentotahewa et al., 2022). In the South African context, the Protection of Personal Information Act (POPIA), which regulates the collection and management of personal data, is also relevant to health data (Swales, 2021). Compliance with policies and regulations can help to mitigate data breaches (Offner et al., 2020; Papastergiou et al., 2021).

Other vital components of a holistic cybersecurity strategy include the management of IT infrastructure (Alodaynan & Alanazi, 2021; Elhoseny et al., 2021), the implementation of an intrusion detection system (Alodaynan & Alanazi, 2021; Elhoseny et al., 2021), and risk management (Abraham et al., 2019; Bhuyan et al., 2020). According to Bhosale et al. (2021), one of the reasons why healthcare institutions are vulnerable to cyberattacks is the prevalence of legacy systems. Hence, it is vital that different components of IT infrastructures, including hardware and software, are adequately maintained and upgraded to ensure that cybercriminals do not exploit their weaknesses to gain access to healthcare data (Alodaynan & Alanazi, 2021; Elhoseny et al., 2021). IT infrastructure management can also entail vulnerability management, where the vulnerability of an institution to cyberattacks is regularly assessed and classified to determine their order of priority (Dias et al., 2021). Rather than reacting to cyberattacks, healthcare institutions can be proactive by implementing intrusion detection and prevention systems to monitor their networks for suspicious activities, generate alerts to them, and automatically launch the predefined countermeasure to a potential cyberattack (Elhoseny et al., 2021; Radoglou-Grammatikis et al., 2021). A risk management approach to cybersecurity countermeasures entails conducting cybersecurity risk assessments on the configuration of health data storage location, identification of areas of vulnerabilities and recording them on a risk register, determining the severity and impact of each risk, and the preferred order of implementation of protective measures for each risk (Abraham et al., 2019; Bhuyan et al., 2020; Dias et al., 2021).

Several authors, including Habib et al. (2019) and Bhuyan et al. (2020), have reported that cyberattacks on healthcare institutions often emanate from within the institutions. This can be attributed to inadequate access control (Shah & Khan, 2020). Access management entails specifying who has access to which healthcare data, and at what level (Elhoseny et al., 2021). Effective access management can mitigate insider threats (Dias et al., 2021), reduce unnecessary exposure, and inadvertent disclosure of healthcare data by unsuspecting employees (Bhuyan et al., 2020; Dias et al., 2021).

4 Conclusions

This paper presents the results of an SLR of 41 research papers aimed at investigating the strategies that could be used to mitigate cybersecurity threats to healthcare data. Nineteen (46%) of the papers included in the SLR were from the WOS database, 10 (24%) were from Scopus, and seven (17%) were from PubMed. The remaining five (12%) papers were retrieved through citations from the articles included in the SLR. The study showed an increase in the number of publications on cyberattacks on healthcare institutions and mitigation strategies from 2020, a period characterized by increased reliance on digital technologies to support healthcare due to the Covid-19 pandemic. The dominant cyberattacks on healthcare data include DOS, malware, ransomware, phishing, and social engineering.

Qualitative analysis of the research papers revealed three main themes, namely (i) emerging technology trends that contribute to cybersecurity vulnerability in the healthcare sector, (ii) current cybersecurity challenges in the healthcare sector, and (iii) cybersecurity countermeasures and mitigation strategies. Based on the analysis of the sources included in the SLR, a holistic cybersecurity mitigation strategy should be approached at the people, technology and policy levels. The fact that people are perceived as the weakest link in an organization's cybersecurity mitigation strategy makes it imperative to incorporate and strengthen countermeasures that specifically deal with user behaviour. Hence, education and training, password management and effective access management are vital.

One of the limitations of this SLR is that the search and extraction of sources were based on specific key phrases. This meant that papers that could potentially have been relevant were excluded from the study because they did not use this study's search phrases in their keywords. The cut-off date of April 2022 also resulted in only four sources published in 2022 being included in the SLR. Another limitation is that the research was limited to sources that were published in academic journals or conference proceedings. This meant that industry papers that could have been relevant were excluded.

The paper contributes to the body of knowledge on cybersecurity in the healthcare sector through a synthesis of the strategies that could be adopted to mitigate cyberattacks on healthcare data. The study has implications for policymakers, who need to keep abreast of the latest cybersecurity threats to healthcare data to ensure that policies are relevant. Software vendors and medical device designers need to incorporate appropriate technical countermeasures into the design and development of software and medical devices. Finally, healthcare institutions have a responsibility to protect patients' healthcare data by allocating sufficient funding to cybersecurity countermeasures.

References

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of Big Data, 5*(1), 1. doi:10.1186/s40537-017-0110-7

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. *Procedia Computer Science, 113*, 73-80. doi:https://doi.org/10.1016/j.procs.2017.08.292

Abouzakhar, N., Jones, A., & Angelopoulou, O. (2017). *Internet of Things security: A review of risks and threats to healthcare sector*.

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons, 62*(4), 539-548. doi:10.1016/j.bushor.2019.03.010

Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management, 43*, 146-158. doi:https://doi.org/10.1016/j.ijinfomgt.2018.07.009

Alodaynan, A., & Alanazi, A. (2021). A survey of cybersecurity vulnerabilities in healthcare systems. *International Journal of Advanced and Applied Sciences, 8*, 48-55. doi:10.21833/ijaas.2021.12.007

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., . . . Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*(1), 146. doi:10.1186/s12911-020-01161-7

Attaran, M. (2020). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, 1-15. doi:10.1080/20479700.2020.1843887

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security, 111*, 102490. doi:https://doi.org/10.1016/j.cose.2021.102490

Bentotahewa, V., Hewage, C., & Williams, J. (2022). The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries. *SN Computer Science, 3*(3), 183. doi:10.1007/s42979-022-01079-z

Bhosale, K. S., Nenova, M., & Iliev, G. (2021, 23-25 Sept. 2021). *A study of cyber attacks: In the healthcare sector.* Paper presented at the 2021 Sixth Junior Conference on Lighting (Lighting).

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., . . . Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of Medical Systems, 44*(5). doi:10.1007/s10916-019-1507-y

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas, 113*, 48-52. doi:10.1016/j.maturitas.2018.04.008

Culbertson, N. (2021). Increased cyberattacks on healthcare institutions shows the need for greater cybersecurity. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=2b54202e5650

Dang, L. M., Piran, M. J., Han, D., Min, K., & Moon, H. (2019). A survey on Internet of Things and cloud computing for healthcare. *Electronics, 8*(7). doi:10.3390/electronics8070768

De, R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *Int J Inf Manage, 55*, 102171. doi:10.1016/j.ijinfomgt.2020.102171

Dias, F., Martens, M., Monken, S., Silva, L., & Santibanez Gonzalez, E. (2021). Risk management focusing on the best practices of data security systems for healthcare. *International Journal of Innovation, 9*, 45-78. doi:10.5585/iji.v9i1.18246

El-Gazzar, R., & Stendal, K. (2020). Blockchain in health care: hope or hype? *Journal of Medical Internet Research, 22*(7), e17199. doi:10.2196/17199

Elhoseny, M., Thilakarathne, N., Alghamdi, M., Mahendran, R., Gardezi, A., Weerasinghe, H., & Welhenge, A. (2021). Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions. *Sustainability, 13*, 11645. doi:10.3390/su132111645

Gafni, R., & Pavel, T. (2021). Cyberattacks against the health-care sectors during the COVID-19 pandemic. *Information & Computer Security*. doi:10.1108/ICS-05-2021-0059

Galetsi, P., Katsaliaki, K., & Kumar, S. (2022). Exploring benefits and ethical challenges in the rise of mHealth (mobile healthcare) technology for the common good: An analysis of mobile applications for health specialists. *Technovation*, 102598. doi:https://doi.org/10.1016/j.technovation.2022.102598

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., . . . Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing, 74*(10), 4986-5002. doi:10.1007/s11227-018-2337-2

Habib, M. A., Faisal, C. M., Sarwar, D. S., Latif, M., Aadil, F., Ahmad, M., . . . Maqsood, M. (2019). Privacy-based medical data protection against internal security threats in heterogeneous Internet of Medical Things. *International Journal of Distributed Sensor Networks, 15*, 155014771987565. doi:10.1177/1550147719875653

Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the Covid-19 pandemic: challenges and prospective solutions. *IEEE Access, 9*, 7152-7169. doi:10.1109/access.2020.3048839

INTERPOL. (2020). Cybercriminals targeting critical healthcare institutions with ransomware. Retrieved from https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

Iyanna, S., Kaur, P., Ractham, P., Talwar, S., & Najmul Islam, A. K. M. (2022). Digital transformation of healthcare sector. What is impeding adoption and continued usage of technology-driven innovations by end-users? *Journal of Business Research, 153*, 150-161. doi:https://doi.org/10.1016/j.jbusres.2022.08.007

Jagadeeswari, V., Subramaniyaswamy, V., Logesh, R., & Vijayakumar, V. (2018). A study on Medical Internet of Things and big data in personalized healthcare system. *Health Inf Sci Syst, 6*(1), 14. doi:10.1007/s13755-018-0049-x

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why employees (still) click on phishing links: investigation in hospitals. *Journal of Medical Internet Research, 22*(1), e16775. doi:10.2196/16775

Jalali, M. S., & Kaiser, J. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research, 20*. doi:10.2196/10059

Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health care and cybersecurity: bibliometric analysis of the literature. *Journal of Medical Internet Research, 21*(2), e12644. doi:10.2196/12644

Jennath, H. S., Anoop, V. S., & Asharaf, S. (2020). Blockchain for healthcare: securing patient data and enabling trusted artificial intelligence. *International Journal of Interactive Multimedia and Artificial Intelligence, 6*(3), 15-23. doi:10.9781/ijimai.2020.07.002

Kelly, J. T., Campbell, K. L., Gong, E., & Scuffham, P. (2020). The Internet of Things: Impact and implications for health care delivery. *Journal of Medical Internet Research, 22*(11), e20135. doi:10.2196/20135

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *J Med Syst, 41*(8), 127. doi:10.1007/s10916-017-0778-4

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, 1-20. doi:https://doi.org/10.1016/j.cose.2021.102248

Magrabi, F., Habli, I., Sujan, M., Wong, D., Thimbleby, H., Baker, M., & Coiera, E. (2019). Why is it so difficult to govern mobile apps in healthcare? *BMJ Health Care Inform, 26*(1). doi:10.1136/bmjhci-2019-100006

Markopoulou, D., & Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. *Computer Law & Security Review, 41*, 105502. doi:https://doi.org/10.1016/j.clsr.2020.105502

Meisner, M. (2018). Financial consequences of cyberattacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting, 6*, 63. doi:10.12775/CJFA.2017.017

Nagasubramanian, G., Sakthivel, R., Patan, R., Gandomi, A., Muthuramalingam, S., & Balamurugan, B. (2020). Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Computing and Applications, 32*. doi:10.1007/s00521-018-3915-1

Nunes, P., Antunes, M., & Silva, C. (2021). Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. *Procedia Computer Science, 181*, 173-181. doi:10.1016/j.procs.2021.01.118

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intelligence and National Security, 35*(4), 556-585. doi:10.1080/02684527.2020.1752459

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., . . . Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ, 372*, n71. doi:10.1136/bmj.n71

Papastergiou, S., Mouratidis, H., & Kalogeraki, E. M. (2021). Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures. *Evolving Systems, 12*(1), 91-108. doi:10.1007/s12530-020-09335-4

Petracca, F., Ciani, O., Cucciniello, M., & Tarricone, R. (2020). Harnessing digital health technologies during and after the COVID-19 pandemic: context matters. *Journal of Medical Internet Research, 22*(12), e21815. doi:10.2196/21815

Pranggono, B., & Arabo, A. (2021). COVID‐19 pandemic cybersecurity issues. *Internet Technology Letters, 4*(2), e247. doi:1002/itl2.247

Radoglou-Grammatikis, P., Sarigiannidis, P., Efstathopoulos, G., Lagkas, T., Fragulis, G., & Sarigiannidis, A. (2021). *A self-learning approach for detecting intrusions in healthcare systems.* Paper presented at the ICC 2021-IEEE International Conference on Communications.

Rajamäki, J., Nevmerzhitskaya, J., & Virág, C. (2018). *Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF).*

Razaque, A., Amsaad, F., Khan, M. J., Hariri, S., Chen, S., Siting, C., & Ji, X. (2019). Survey: cybersecurity vulnerabilities, attacks and solutions in the medical domain. *IEEE Access, 7*, 168774-168797. doi:10.1109/ACCESS.2019.2950849

Sadek, I., Codjo, J., Rehman, S. U., & Abdulrazak, B. (2022). Security and privacy in the Internet of Things healthcare systems: Toward a robust solution in real-life deployment. *Computer Methods and Programs in Biomedicine Update, 2*, 100071. doi:https://doi.org/10.1016/j.cmpbup.2022.100071

Sannino, G., De Pietro, G., & Verde, L. (2020). Healthcare systems: an overview of the most important aspects of current and future m-health applications. In A. El Saddik, M. Hossain, & B. Kantarci (Eds.), *Connected Health in Smart Cities* (pp. 213-231). doi:https://doi.org/10.1007/978-3-030-27844-1_11

Sarfraz, Z., Sarfraz, A., Iftikar, H. M., & Akhund, R. (2021). Is COVID-19 pushing us to the fifth industrial revolution (society 5.0)? *Pakistan Journal of Medical Sciences, 37*(2), 591. doi:10.12669/pjms.37.2.3387

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A., Agrawal, A., Kumar, R., & Khan, P. R. (2020). Healthcare data breaches: insights and implications. *Healthcare, 8*, 133. doi:10.3390/healthcare8020133

Shah, S., & Khan, R. (2020). Secondary use of electronic health record: opportunities and challenges. *IEEE Access, PP*, 1-1. doi:10.1109/ACCESS.2020.3011099

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security, 97*, 101966-101966. doi:10.1016/j.cose.2020.101966

Siddaway, A. P., Wood, A. M., & Hedges, L. V. (2019). How to do a systematic review: a best practice guide for conducting and reporting narrative reviews, meta-analyses, and meta-syntheses. *Annual review of psychology, 70*, 747-770.

Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. *Cryptography, 3*(1). doi:10.3390/cryptography3010003

Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: A review. *Security and Communication Networks, 2018*, 5978636. doi:10.1155/2018/5978636

Swales, L. (2021). The Protection of Personal Information Act and data de-identification. *South African Journal of Science, 117*(7-8), 1-3. doi:https://doi.org/10.17159/sajs.2021/10808

Tortorella, G. L., Fogliatto, F. S., Espôsto, K. F., Vergara, A. M. C., Vassolo, R., Mendoza, D. T., & Narayanamurthy, G. (2020). Effects of contingencies on healthcare 4.0 technologies adoption and barriers in emerging economies. *Technological Forecasting and Social Change, 120048*, 120048. doi:https://doi.org/10.1016/j.techfore.2020.120048

Tsai, C. H., Eghdam, A., Davoody, N., Wright, G., Flowerday, S., & Koch, S. (2020). Effects of electronic health record implementation and barriers to adoption and use: a scoping review and qualitative analysis of the content. *Life, 10*(12), 327. doi:10.3390/life10120327

Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports, 4*, 100126. doi:https://doi.org/10.1016/j.chbr.2021.100126

Zriqat, I. A., & Altamimi, A. (2017). A security model for preserving privacy of healthcare information. *International Journal of Applied Engineering Research, 12*, 14251-14258.