Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Risk Classes of Cloud Computing Project in Healthcare: A Review of Technical Report and Standards

Muhammad Afif Fathullah[1,*], Anusuyah Subbarao[1], Saravanan Muthaiyah[2], Dragos Taralunga[3]

[1] Faculty of Management, Multimedia University, 63100 Cyberjaya, Selangor, Malaysia
[2] International Medical University, Bukit Jalil, 57000 Kuala Lumpur, Malaysia
[3] Faculty of Electronics, Telecommunications and Information Technology, National University of Science and Technology Politehnica Bucharest, 060042 Bucharest, Romania

ARTICLE INFO

Article history:
Received 3 November 2023
Received in revised form 22 January 2024
Accepted 12 March 2024
Available online 25 April 2024

Keywords:

Cloud computing; Risk management; Cybersecurity; Literature review

ABSTRACT

Cloud computing has been shown to have positive impacts on the organization such as “cost savings”, “enhanced efficiency”, etc. Cloud computing has been implemented in multiple sectors around the world including the healthcare sector. The rise of chronic illnesses requires the assistance of new technologies such as cloud computing to bring flexibility and convenience to treat these illnesses. However, as with all IT architecture projects, there are risks and challenges to adopting cloud computing. As such this study aims to find the prevailing risk classes of cloud computing projects in healthcare through risk classes discussed in technical reports and standards. This study will employ TLR as a method for this study. Through this study, we found five technical reports and standards that discuss the risk management of cloud computing. The result shows that there are 13 prevalent risk classes of cloud computing. We hope that the results discovered through this study can help academics, researchers, and practitioners to recognize what are the prevalent risk classes currently discussed regarding cloud computing and whether the discussion has matured or not.

1. Introduction

Chan *et al.,* [1] defined cloud computing as a "computing resource deployment and procurement model that enables an organization to obtain its computing resources and applications from any location via an Internet connection". It was stated by Alashhab *et al.*, [2] that there will be a “Compound annual growth rate (CAGR)” of 22.59% which is a substantial surge in the exodus of "application services" to "cloud computing environment (CGE)" in the current times. Cloud computing is gaining traction around the world in a multitude of sectors due to its positive influence such as "better cost savings", "improved agility", "enhanced efficiency", "better resource integration", "more business opportunities", and "simplification of complex work resources" on several organizations [2,3].

[*] *Corresponding author.*
E-mail address: afif.fathullah@mmu.edu.my

https://doi.org/10.37934/araset.44.1.169180

One of the sectors that have been implementing cloud computing is the healthcare sector. Vidya Priya Darcini *et al*., [4] state that due to the rise of chronic illnesses which require prompter and superior care, the appeal and demand for digital healthcare systems is growing. Furthermore, New technologies such as cloud computing bring positive impacts for monitoring and communication purposes due to their resilience and accessibility Vidya Priya Darcini *et al*., [4]. It has been stated by *Al-Issa et al*., [5] that cloud computing can give certain benefits to the healthcare sector which are:

i. improved patient care
ii. cost saving
iii. energy saving
iv. robust disaster recovery
v. research
vi. solving the scarcity of resources
vii. rapid deployment
viii. data availability

The United Kingdom (UK) National Health Service (NHS) used "Amazon Web Services (AWS)". They used the cloud computing resources of AWS for data processing services and AI call centres. Their implementation had respectively improved the time it took for them to process their data to 137 seconds from 137 minutes which is a 2600% or 26-fold improvement and a saving of approximately £520,000 [6,7]. Oracle a cloud computing vendor (CCV) has also come out with a cloud computing service for the healthcare sector called Oracle Connected Care Services *Oracle Corporation* [8]. Oracle stated that this service offers benefits as shown in Table 1. This discussion shows that more efficient processes and increased agility can be granted to healthcare organizations without them being laden with an enormous cost through the adoption of cloud computing.

Table 1
Oracle connected care use cases and benefits [8]

Use Case	Benefit
Stroke Care for Rural & Remote Communities	- Reduced door-to-needle time - Improved patient outcomes - Reduced readmissions
Myocardial Infarction (MI) Emergency Treatment	- Reduced door-to-balloon time - Improved patient outcomes - Reduced readmissions
Paediatric Cardiology Infants with Single Ventricle Syndrome	- Reduced ED visits - Improved patient outcomes - Maximizing the effectiveness and efficiency of the care team
Skilled Nursing Facilities	- Reduced Medicare penalties from unplanned ED visits & readmissions - Reduced transportation costs - Maximizing the effectiveness and efficiency of the care team
Clinical Trials	- Improved management of chronic conditions - Reduced dropout rate - Reduced travel requirements - Reduced study costs associated with site visits

However, as with all IT architecture projects, there are risks and challenges [9-11] in adopting cloud computing [12,13]. The risks and challenges that are faced in cloud computing adoption in the healthcare sector have been said to be able to disrupt the benefits gained from the adoption and even cause more complications Abrar *et al*., [14]. These complications can stem from various risks such as data leakage, security, and compliance issues, public perception, etc. which could be caused by threats, vulnerabilities, and probabilities indicator such as privacy breaches, insufficient due diligence, lack of experts, etc. (Fathullah *et al.,*) [15] These risks also come with their own set of consequences such as loss of data confidentiality and privacy, loss of data availability and reliability, loss of life, etc. (Fathullah *et al*.,) [15] These risk along with their causes and consequences are a challenge that must be tackled for the adoption of cloud computing in the healthcare sector as more complications can arise from not tackling these issues.

Besides that, it had been stated by Mekawie & Yehia [13] that "risk management was considered critical however according to their interviewees this factor is neglected and often forgotten". This makes the discussion on risk classes that affect cloud computing important as it allows for the facilitation of risk management by categorizing the risk affecting it. Moreover, as cloud computing in healthcare involves managing increasingly desirable health data, it is evolving into a high-risk technology. Therefore, it is imperative to conduct effective risk management Deswandri *et al.,* [16], which is essential not only to guarantee safety in design Deswandri *et al*., [16] but also to establish a secure environment Mohd Yusof *et al*., [17] for the utilization of cloud computing in healthcare.

This study aims to fill the gap in existing research by investigating the risks associated with cloud computing projects, specifically focusing on the risk classes outlined in technical reports and standards due to the limited number of such studies. As such this study aims to:

i. find the prevailing risk classes of cloud computing projects in healthcare
ii. discover the risk classes discussed in technical reports and standards

This study will deploy a traditional literature review (TLR). Moving forward, this paper will present the research methodology, the results, the discussion, and finally the conclusion.

2. Methodology

2.1 Traditional Literature Review

This study used the TLR as a method to review technical reports and standards. Jesson *et al*., [18] stated that there were two stages in a TLR which are cyclical with the first stage comprising a summary of the articles found followed by a second stage in which the results of the first stage are compared and contrasted to achieve the outcome. Meanwhile, Li and Wang [19] stated that a TLR comprises six stages with them being:

i. "Defining the Problem"
ii. "Searching for Literature"
iii. "Selecting Studies"
iv. "Reading the Literature"
v. "Organizing the Data"
vi. "Writing the Review".

As such this study has adapted these two methods for the TLR as shown in Figure 1.

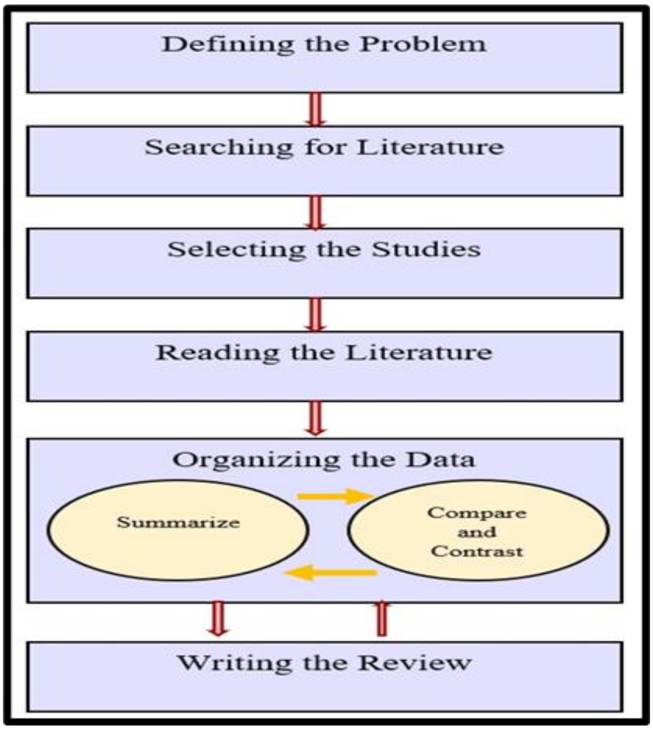

Fig. 1. TLR Stage

2.1.1 Defining the problem

The problem of this study was defined by its' aims which are:

i. to find the prevailing risk classes of cloud computing projects in healthcare
ii. to discover the risk classes discussed in technical reports and standards

2.1.2 Searching for literature

The researchers of this study did not have access to a specific library of technical reports and standards as such the literature was searched through "Google Search Engine". There were several keywords and Boolean operators used for this search which were "Cloud Computing" And "Healthcare", And "Risk Management". From this search, not only technical reports and standards were found but also online articles as such forward snowballing was also used in this study by exploring the references of these online articles to find technical reports and standards.

2.1.3 Selecting the studies

The inclusion criteria of this study were:

i. Technical report and standard
ii. The full text of the technical report and standard is available
iii. Technical report and standard that is related to topics of the research question
iv. Technical report and standards that are related to cloud computing and risks.

The exclusion criteria of this study were:

i. a Duplicate of the technical report and standard
ii. a technical report and standard that were written in other languages except English
iii. a technical report and standard not related to cloud computing and risks.

2.1.4 Reading the literature

The technical report and standard were read by the researchers. Furthermore, the main points relating to this study's aims were highlighted by the researchers.

2.1.5 Organizing the data

The data found in the technical report and standards were summarized. Following this, the data from the technical report and standards were compared and contrasted with each other.

2.1.6 Writing the review

A review of the technical report and standards was written.

3. Results

3.1 Technical Report and Standards

This study conducted an LR of technical reports and standards that discussed categories of risks that could be faced by organizations that wish to adopt and implement cloud computing. We found five technical reports and standards that discussed typical risks that may be faced by organizations as shown in Table 2

Table 2
Technical Report and Standards

No	Name	Abbreviation
1	“COSO 2012 Cloud Computing Thought Paper” [1]	COSO 2012
2	“NHS 2018 Health and Social Care Cloud Risk Framework Paper” [20]	NHS 2018
3	“COSO 2021 Enterprise Risk Management for Cloud Computing” [21]	COSO 2021
4	“IBM Cost of Data Breach 2021” [22]	IBM 2021
5	“IBM Cost of Data Breach 2022” [23]	IBM 2022

Through the LR conducted on the abovementioned technical report and standards, 24 risk classes were found as can be seen in Table 3.

Table 3
Typical Risk of Cloud Computing

Technical Report and Standard	Typical Risks
COSO 2012	“Disruptive force” “Residing in the same risk ecosystem as the Cloud Service Provider (CSP) and other tenants of the cloud” “Lack of transparency” “Reliability and performance issues” “Vendor lock-in and lack of application portability or interoperability” “Security and compliance concerns” “High-value cyber-attack targets” “Risk of data leakage” “IT organizational changes” “Cloud service provider viability”
NSH 2018	“Confidentiality” “Integrity” “Availability” “Impact of Breach” “Public Perception” “Lock – In”
COSO 2021	“Reliability and Vulnerability” “Multi-tenancy, Data Leakage, and Data Theft” “Single Point of Failure” “Compliance” “Cyber Attacks” “Shadow IT”
IBM 2021	“Data Breach”
IBM 2022	“Data Breach”

However, several of the risk classes have similarities that are significant enough to allow for them to be consolidated into one risk. These risks were consolidated based on their description and their effect on cloud computing implementation and adoption. These consolidated risks are shown in Table 4.

The consolidation of risks as shown in Table 4 has decreased the total number of typical risks from 24 to 13. This is as 16 risks have been consolidated into five risks. From this, it can be seen that both similar and unique risks are discussed through these five technical reports and standards.

Table 4
Consolidated Risk

No	Consolidated Risks Name	Technical Report	Risk Name
1	“Risk of Data Leakage”	COSO 2012	“Risk of data leakage”
		NSH 2018	“Confidentiality” “Integrity” “Impact of Breach”
		COSO 2021	“Multi-tenancy, Data Leakage, and Data Theft”
		IBM 2021	“Data Breach”
		IBM 2021	“Data Breach”
2	“High-value cyber-attack targets”	COSO 2012	“High-value cyber-attack targets”

		NSH 2018	“Confidentiality” “Integrity”
		COSO 2021	“Impact of Breach” “Cyber Attacks”
3	“Reliability and performance issues”	COSO 2012 NSH 2018 COSO 2021	“Reliability and performance issues” “Availability” “Reliability and Vulnerability”
4	“Vendor lock-in and lack of application portability or interoperability”	COSO 2012 NSH 2018	“Vendor lock-in and lack of application portability or interoperability” “Lock – In”
5	“Security and compliance concerns”	COSO 2012 COSO 2021	“Security and compliance concerns” “Compliance”

Table 5 maps the risk classes with the reports and standards that discuss them.

Table 5
Mapped Risk Classes to Reports and Standards

Risk Classes ID	Risk Classes Name	COSO 2012	NSH 2018	COSO 2021	IBM 2021	IBM 2022
R1	“Disruptive Force”	■				
R2	“Residing in the same risk ecosystem as the CSP and other tenants of the cloud”	■				
R3	“Lack of transparency	■				
R4	“Reliability and performance issues”	■	■	■		
R5	“Vendor lock-in and lack of application portability or interoperability”	■	■			
R6	“Security and compliance concerns”	■		■		
R7	“High-value cyber-attack targets”	■	■	■		
R8	“Risk of data leakage”	■	■	■	■	■
R9	“IT organizational changes”	■				
R10	“Cloud service provider viability”	■				
R11	“Public Perception”		■			
R12	“Single Point of Failure”			■		
R13	“Shadow IT”			■		

Meanwhile, Table 6 lists the risk classes along with their description.

Table 6
Risk Classes Definition

Risk Classes ID	Risk Classes Name	Definition
R1	“Disruptive Force”	“Cloud computing can disrupt some business models. This is as those that embrace cloud computing might be able to bring new ideas and innovation to the market faster which may force other competitors to follow suit and adopt cloud computing.”
R2	“Residing in the same risk ecosystem as the CSP and other tenants of the cloud”	“The nature of cloud computing in which new dependency relationships with CSP are created with respect to legal liability, risk universe, incident escalation, incident response, and other areas. This is because if the CSP neglects or fails in its responsibilities, it could have legal liability implications for the CSP's customer organizations but not vice versa.”
R3	“Lack of transparency”	“A CSP is unlikely to share specific information about its processes, operations, controls, and methodologies. This includes the processes and subcontractors processing the data and where they are located. They may also not be forthcoming with their failures such as data corruption events.”

R4	“Reliability and performance issues”	“Reliability and performance issues is a risk that cloud computing is suspectable to. Although quality of service (QoS) agreements can be structured with the CSP, cloud computing availability may not necessarily reach 100% uptime.”
R5	“Vendor lock-in and lack of application portability or interoperability”	“Many CSPs offer their software tools with their cloud computing packages. These tools may be proprietary and do not work with tools or cloud solutions of other vendors. This may affect the portability, interoperability, and flexibility of an organization's cloud infrastructure.”
R6	“Security and compliance concerns”	“Security requirements and policies of an organization's cloud computing architecture have to comply with national and regional governance legislation and policies. These legislations and policies must be followed by both the organization and their CSPs to ensure privacy and data security, and violations will bring serious consequences to the organization.”
R7	“High-value cyber-attack targets”	“Cloud computing architecture and resources can be used as a platform for launching attacks, hosting spam through viruses, worms, malware, etc. In the context of healthcare data, the attackers may modify or expose these healthcare records which is life-threatening for the patients/customers of a healthcare organization.”
R8	“Risk of data leakage”	“A cloud computing multi-tenant environment runs the risk of data leakage that does not exist in dedicated servers and resources used exclusively by one organization. In an outsourced computing environment such as the cloud, the potential for a data breach may be more likely because of outsourced services that sidestep personnel, logical, and physical controls.”
R9	“IT organizational changes”	“If cloud computing is adopted to a significant degree, IT management staff may not have the capability to conduct adequate IT skills assessment for IT staff and organizational professionals for the implemented services.”
R10	“Cloud service provider viability”	“CSPs may go bankrupt and shut down their services or CSPs may change and modify their services which will affect the client organizations.”
R11	“Public Perception”	“There is a risk of public concern over the use of cloud computing for healthcare data as it is a widely available and shared computing environment. There is also the challenge of how to educate end users on cloud computing usage.”
R12	“Single Point of Failure”	“A potential risk posed by a flaw in the design, implementation, or configuration of a circuit or system in which one fault or malfunction causes an entire system to stop operating.”
R13	“Shadow IT”	“Ad hoc and unauthorized use of IT services for work.”

4. Discussion

From Figure 2, it can be seen that there are differences in which risk classes are discussed in technical reports and standards. However, due to the limited number of technical standards and reports found, a percentage comparison was instead used as shown in Eq. (1).

$$p = \frac{n}{m}\ \mathrm{x}\ 100\% \qquad (1)$$

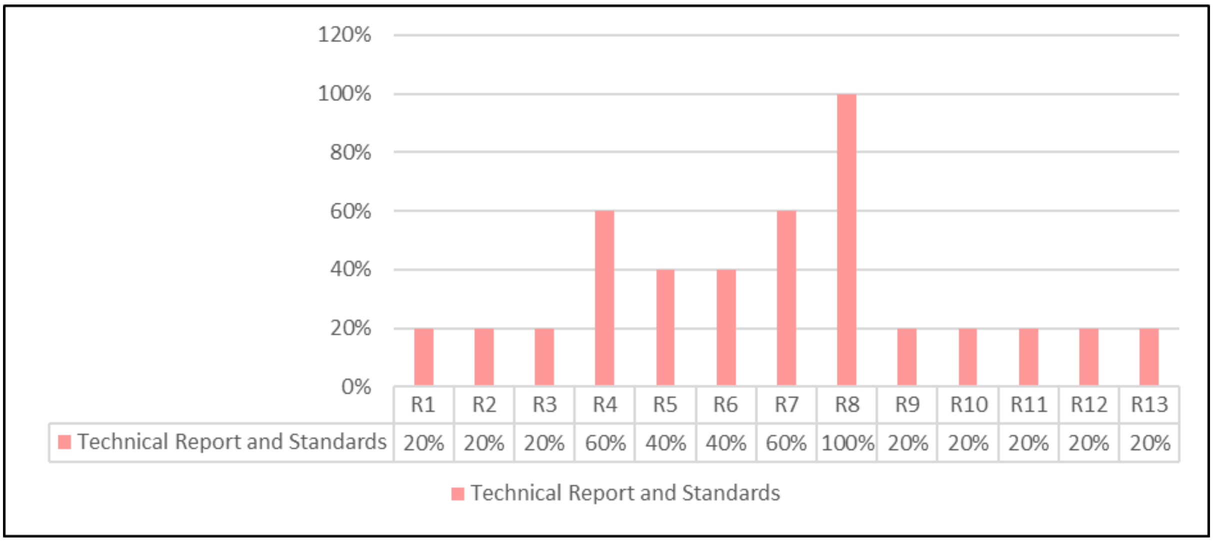

Fig. 2. Technical Report and Standards Risk Classes

where n represents the number of technical reports and standards that discuss the risk class and m represents the total number of technical reports and standards found. The percentage comparison was divided into five levels for a fair comparison to be done as shown in Table 7.

Table 7
Percentage Level

Percentage Level		Level
Minimum	Maximum	
1%	20%	1
21%	40%	2
41%	60%	3
61%	80%	4
81%	100%	5

From the percentage levels in Figure 2, it can be seen that eight risk classes are in level 1 with the risk classes being “R1 - Disruptive Force”; “R2 - Residing in the same risk ecosystem as the CSP and other tenants of the cloud”; “R3 - Lack of transparency”; “R9 - IT organizational changes”; “R10 - Cloud service provider viability”; “R11 - Public Perception”; “R12 - Single Point of Failure”; “R13 - Shadow IT”.

Furthermore, it can also be seen that two risk classes are in level 2 which are “R5 - Vendor lock-in and lack of application portability or interoperability” and “R6 - Security and compliance concerns”. Besides that, another two risk classes are in level 3 which are R4 - Reliability and performance issues and “R7 - High-value cyber-attack targets”.

Lastly, it is shown that there is only one risk class in level 5 with the risk class being R8 - Risk of data leakage. These results show that a majority of risk classes being discussed in technical reports and standards are not unanimously being agreed on with only one risk class agreed across all technical reports and standards found. This shows that the discussion on risk classes apart from the risk of data leakage (R8) has still not matured.

Meanwhile, the discussion of the risk of data leakage(R8) has matured as it has been discussed in all technical reports and standards. Furthermore, IBM 2021 [22] and IBM 2022 [23] show that the cost of cloud computing data breaches is also changing across the three public, private, and hybrid cloud models. The public cloud model's average cost of data breaches had increased from $4.80 million in 2021 to $5.02 million in 2022. Meanwhile, the Private cloud model average cost of the data breach had decreased from $4.55 million in 2021 to $4.24 million in 2022. Lastly, the average cost of a data breach in a hybrid cloud model has increased from $3.61 million in 2021 to $3.80 million in 2022.

5. Conclusion

To conclude, the goal of this study was

i. to find the prevalent risk classes of cloud computing projects in healthcare
ii. to discover the risk classes discussed in technical reports and standards

The first and second goals were achieved through the discovery of 13 consolidated risk classes related to cloud computing discussed in the technical report and standards which were:

i. “Disruptive Force"
ii. “Residing in the same risk ecosystem as the CSP and other tenants of the cloud"
iii. “Lack of transparency"
iv. “Reliability and performance issues"
v. “Vendor lock-in and lack of application portability or interoperability"
vi. “Security and compliance concerns"
vii. “High-value cyber-attack targets"
viii. “Risk of data leakage"
ix. “IT organizational changes"
x. “Cloud service provider viability"
xi. “Public Perception"
xii. “Single Point of Failure"
xiii. “Shadow IT "

Furthermore, this study revealed that certain risk classes, such as "Data Leakage," are consistently discussed across all technical reports and standards. However, there are also unique risk classes, such as "Public Perception," which are addressed only in specific technical reports and standards. This indicates that the discourse on many risk classes has not fully developed, except for "Data Leakage", which is a common theme across all technical reports and standards. As such future studies may explore these risk classes that have not yet matured to test their viability along with discovering its causes, consequences, and control procedures. We hope that the results discovered through this study can help academics, researchers, and practitioners recognize what are the prevalent risk classes currently discussed regarding cloud computing in healthcare.

Throughout this study some limitations have been faced, firstly, as we did not have access to a database of technical reports and standards, we were only able to use a search engine to find the relevant articles. Second, as there were not a lot of technical reports and standards and academic papers that discussed risk management of cloud computing in healthcare specifically, articles that discussed the risk of cloud computing were also incorporated into the study.

Moving forward, we will validate the risk classes we have found with expert participants on whether they have relevance or not in the current technological climate along with their maturity. We also believe that more studies regarding risk management of cloud computing can be done especially in essential sectors such as healthcare to increase the quality of life of citizens. This is to maximize the positive aspects of embracing digital transformation technologies such as cloud computing, we must know what are the risks along with their causes and consequences that might exist when adopting them.

Acknowledgment
This work was supported by a grant from the National Program for Research of the National Association of Technical Universities - GNAC ARUT 2023. The authors are also grateful to Multimedia University (MMU) Malaysia for their support.

References

[1] Chan, W., E. Leung, and H. Pili. "COSO Enterprise Risk Management for Cloud Computing." (2012).

[2] Alashhab, Ziyad R., Mohammed Anbar, Manmeet Mahinderjit Singh, Yu-Beng Leau, Zaher Ali Al-Sai, and Sami Abu Alhayja'a. "Impact of coronavirus pandemic crisis on technologies and cloud computing applications." *Journal of Electronic Science and Technology* 19, no. 1 (2021): 100059. https://doi.org/10.1016/j.jnlest.2020.100059

[3] Soewito, Benfano, Ford Lumban Gaol, and Edi Abdurachman. "A systematic literature Review: Risk analysis in cloud migration." *Journal of King Saud University-Computer and Information Sciences* 34, no. 6 (2022): 3111-3120. https://doi.org/10.1016/j.jksuci.2021.01.008

[4] Isravel, Deva Priya, and Salaja Silas. "A comprehensive review on the emerging IoT-cloud based technologies for smart healthcare." In *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pp. 606-611. IEEE, 2020.

[5] Al-Issa, Yazan, Mohammad Ashraf Ottom, and Ahmed Tamrawi. "eHealth cloud security challenges: a survey." *Journal of healthcare engineering* 2019 (2019). https://doi.org/10.1155/2019/7516035

[6] Amazon Web Services. "Using AWS in the Context of NHS Cloud Security Guidance." (2019).

[7] Amazon Web Services. "Guidance for NHS Trusts Adopting AWS Cloud Services." (2019).

[8] Oracle Corporation. "The Clinically Integrated Supply Chain Improving Safety, Traceability, and Value." (2019).

[9] Hampton, John. *Fundamentals of enterprise risk management: How top companies assess risk, manage exposure, and seize opportunity*. Amacom, 2009.

[10] Hopkin, Paul. *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers, 2018.

[11] ISO31000. 2018. BS ISO 31000. "2018 BSI Standards Publication Risk Management — Guidelines." *BSI Standards Publication,* 26. (2018).

[12] Al-Hujran, Omar, Enas M. Al-Lozi, Mutaz M. Al-Debei, and Mahmoud Maqableh. "Challenges of cloud computing adoption from the TOE framework perspective." *International Journal of E-Business Research (IJEBR)* 14, no. 3 (2018): 77-94. https://doi.org/10.4018/IJEBR.2018070105

[13] Mekawie, Nermeen, and Kesmat Yehia. "Challenges of deploying cloud computing in eHealth." *Procedia Computer Science* 181 (2021): 1049-1057. https://doi.org/10.1016/j.procs.2021.01.300

[14] Abrar, Hina, Syed Jawad Hussain, Junaid Chaudhry, Kashif Saleem, Mehmet A. Orgun, Jalal Al-Muhtadi, and Craig Valli. "Risk analysis of cloud sourcing in healthcare and public health industry." *IEEE Access* 6 (2018): 19140-19150. https://doi.org/10.1109/ACCESS.2018.2805919

[15] Fathullah, Muhammad Afif, Anusuyah Subbarao, and Saravanan Muthaiyah. "A Systematic Review: Risk Management of Cloud Computing Projects in Healthcare." *International Journal of Management, Finance and Accounting* 4, no. 2 (2023): 83-115. https://doi.org/10.33093/ijomfa.2023.4.2.5

[16] Tyas, Ratih Luhuring, Dinnia Intaningrum, Idris Eko Putro, Ahmad Riyadl, Irvan Dwi Junianto, Alfitri Meliana, Rika Andiarti, and Arif Nur Hakim. "Risk Assessment of Solid Propellant Rocket Motor using a Combination of HAZOP and FMEA Methods." *Journal of Advanced Research in Fluid Mechanics and Thermal Sciences* 110, no. 1 (2023): 63-78. https://doi.org/10.37934/arfmts.110.1.6378

[17] Yusof, Mohd Fahmi Mohd, and Roslina Mohammad. "Risk management framework and practices for boiler operations in Malaysia." *Progress in Energy and Environment* (2023): 26-38. https://doi.org/10.37934/progee.23.1.2638

[18] Lacey, Fiona M., Lydia Matheson, and Jill Jesson. "Doing your literature review: Traditional and systematic techniques." *Doing Your Literature Review* (2011): 1-192.

[19] Li, Shaofeng, and Hong Wang. "Traditional literature review and research synthesis." *The Palgrave handbook of applied linguistics research methodology* (2018): 123-144. https://doi.org/10.1057/978-1-137-59900-1_6

[20] NSH. "Health and Social Care. Disability." (2018): 88–105. https://doi.org/10.4324/9781315624839-5

[21] Sobel, P. J., J. Burns, D. C. Murdock, J. C. Thomson, P. K. Miller, and V. Cheng. "COSO 2021 Enterprise Risk Management for Cloud Computing." *The Institute of Internal Auditors (IIA) Preface COSO Board Members Authors Mike Grob Principal, Consulting Crowe LLP-Chicago. (*2021).

[22] IBM. “Cost of Data Breach Report 2021.” (2021). https://doi.org/10.1016/S1361-3723(21)00082-8

[23] IBM. “Cost of Data Breach Report 2022.” (2022). https://doi.org/10.12968/S1353-4858(22)70049-9