A Review of Data Breach Cost in Cloud Computing

Muhammad Afif Fathullah(✉), Anusuyah Subbarao, and Saravanan Muthaiyah

Faculty of Management, Multimedia University, Cyberjaya, Malaysia
muhdafiffathullah@gmail.com

Abstract. In this technological age, there has been rapid advances in technology such as in cloud computing. There are benefits, opportunities, and values to be gained from these technologies. However, there has also been introduction of new risks and challenges such data breaches in a cloud computing environment. Data breaches are dangerous to organizations in all sectors as it allows unauthorized users to access their confidential data which will come at a cost to these organizations. This paper will review data breaches in cloud computing environments and will discuss the costs of these data breaches and what factors will affect these costs.

Keywords: Cloud Computing · Data Breaches · Risk · Challenges

1 Introduction

The rapid advances in technology in this age, brought on by the fourth industrial revolution have pivoted the most industries to using electronic record and systems such as health information system and cloud computing from paper-based system [1–3]. This is as modern technology such as internet of things (IoT), cloud computing, Artificial Intelligence (AI), Machine Learning (ML) has allowed for organizations and providers to provide better and cost-productive services to their customers and clients [3, 4].

Cloud computing is regarded as the backbone of digital transformations in organizations as cloud computing store the digitalize data of an organization. This will lead to digitalization of an organization as they start to use digital tools such as blockchain to secure their data stored in the cloud. This will then lead to a digital transformation for an organization as their processes are now done digitally. The Covid-19 pandemic has shown the importance of the digitalization of an organization with how they manage their operations and businesses with digital tools. Digital transformations are especially important in the many sectors as it allows healthcare them to be more flexible and efficient in their processes.

However, using Cloud Computing, Health/Hospital Information System (HIS) systems and modern technologies also have a downside. This is as organizations from most sectors who have adopted these systems and technologies have also been introduced

A. Asmawi (Ed.): ICTIM 2022, AEBMR 228, pp. 199–209, 2022.
https://doi.org/10.2991/978-94-6463-080-0_17

to different and new security risks and uncertainties that differ from paper-based systems [3–6] Risk in general terms refer to events and/or effects that can have negative repercussions in both personal and organizational level [7].

Risk events and/or effects may happen in a cloud computing and modern technologies environment due a multitude of reasons including software and hardware vulnerabilities, security failures, and human error. Data breaches are one of the risks that organization have to face in adopting cloud computing architecture and modern technologies as these databases and technologies are suspectable to being infiltrated by unauthorized users [3, 8, 9].

Data breach happens when an unauthorized user gain classified and private information such as customers and employee's data, intellectual property data and other sensitive data [10]. Data breach is a risk that all sectors and organization who adopt electronic system and records such as cloud computing and related technologies will have to take into consideration and face. The purpose of this paper is to know what is the cost of data breach in cloud computing and their related factors. As such, to fulfil this purpose, review of the impact of data breach in cloud computing based on the "*2021 IBM Data Breach Report*" is done.

The rest of this paper is separated into the following sections. Section 2 will explore the related literature in relation to cloud computing and data breach. This is followed by Sect. 3, which will illustrate IBM experience and information on data breach in cloud computing. Lastly, Sect. 4 will chronicle the conclusion of this paper.

2 Literature Review

2.1 Trend of Cloud Computing

[11] defines cloud computing as "computing resource deployment and procurement model that enables an organization to obtain its computing resources and applications from any location via an Internet connection". Cloud computing is progressively being seen as a major driver for business innovation [12]. This is as cloud computing allows for organizations to operate in competitive environment without focusing on scaling, maintenance, and failure [13] as all of the scaling, maintenance, and failure is borne by the cloud computing vendor. This allows for organizations to focus mainly on their daily operations without having difficulties in managing their data hardware and software as these are handled by their vendors. Essentially, it can be said that by adopting cloud computing organizations are 'buying time' as it completely eliminates the time spent by their employees in managing the organization data hardware and software.

Cloud computing can be deployed in several models with the most common being public cloud, private cloud, community cloud and hybrid cloud [11, 14]. One of the major differences in these deployment models are those who has access to cloud infrastructure. Essentially, there are four deployment models 1) public cloud model where a cloud infrastructure is shared and used by multiple organizations; 2) private cloud model where a cloud infrastructure is used only by one organization; 3) community cloud model where the cloud infrastructure is shared by several organizations in one community/sector and are used by the organizations in the community and lastly 4) hybrid cloud model is a

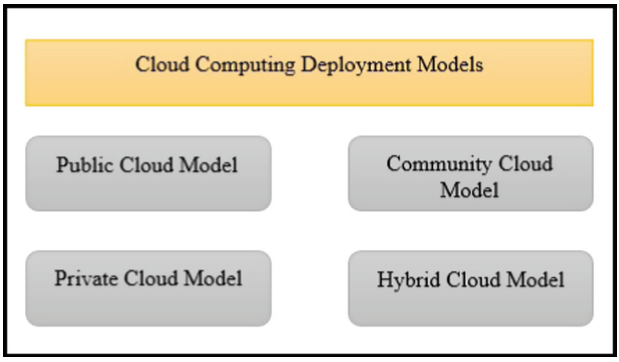

Fig. 1. Cloud Computing Deployment Models

combination of more than one of the previously mentioned deployment models as can be seen in Fig. 1.

There are also several cloud service delivery model that can be deployed in cloud computing such as Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a Service (SaaS) [11, 15]. IaaS services allows for organizations to manage their resources such as data storage, networking, and servers completely on the cloud without having to buy the hardware examples are Amazon Web Services (AWS) and Microsoft Azure. PaaS services allows for organizations to develop, host, build, and deploy their own apps/software through the cloud examples are AWS Elastic Beanstalk and Windows Azure. Meanwhile, SaaS services are cloud products, tools, and applications that are offered by the vendors examples are Microsoft O365 online and Oracle ERP. Furthermore, with the progression of technology there have been more service delivery model being offered by vendors such Blockchain as a service (BaaS).

The advent of BaaS in cloud computing is significant. As it gives cloud computing adopters an option to purchase blockchain for their cloud architecture. This is an added benefit for cloud computing architecture as blockchain and cloud computing synergize well. As cloud computing can be said to be where the organization data is stored and blockchain is how to make sure that the data is secured. It was also stated by [16] that blockchain "is very robust against attacks and failures, and provides different methods of access control." which is very important in most sectors as a lot of data, are sensitive data especially the customers' data. This gives security to organizations that even if they are on a public, community or hybrid cloud that only those who have permission to access their data are able to access it.

Cloud computing is increasingly being adopted in all sectors in the world. This is as it has been stated by [17] that cloud computing possesses unique features such as "on-demand self-service" and "broad network access" that are asserted to be able augment organization from most sectors by strengthening their traditional in-house information technology (IT) approaches. This shows that cloud computing has tremendous potential to benefit organizations form most sectors and industries.

Cloud computing offers many benefits to organizations such as scalability, online delivery of software and virtual services [18]. This is as cloud computing vendors allow

organizations to buy their cloud computing as according to their respective needs. This means that organizations can buy cloud computing services according to their requirements and allow for them to scale their usage of cloud computing services as they require.

Cloud computing has also shown positive impact in some organizations by allowing them to have better "cost savings", "improved agility", "enhanced efficiency", "better resource integration", "more business opportunities", and "simplification of complex work resources" [19, 20]. This is as cloud computing allows for organizations to use recent technology innovation such as data analytics and machine learning solutions and established solutions such as "Enterprise Resource Planning (ERP)" online on scale.

These solutions which are very helpful to organizations can improve an organization agility, efficiency, resource integration, and more without having the organization being burdened with high cost. In a nutshell cloud computing allows for organizations to reduce operating costs and improve performance of business applications which brings positive impact to an organization.

2.2 Data Breach in Cloud Computing

Data breaches in simple terms are when protected and confidential records and data such patient's medical records are accessed by unauthorized users [11, 21, 22]. Data breaches may happen because of several reasons such as different security methods or protocols between different cloud computing systems and environments that makes the data suspectable to breach during transit between these systems. Furthermore, it may also happen when the data is in its storage and are pilfered there.

Besides that, in an outsourced computing environment such as the cloud the potential for data breach may be more likely because of outsourced services that sidestep personnel, logical, and physical controls. Data breaches are dangerous as if this risk materialized it will allow for the unauthorized users to modify, steal, view, transfer, and other nefarious actions to the data [23].

Data breaches will bring massive repercussion to an organization as they can compromise the confidentiality, integrity, and availability of the organizations data [24]. These compromised data can have a massive range from customers data to employee data to intellectual property data and can even compromise other sensitive data of the organization [10].

3 IBM Experience of Cloud Data Breach

IBM have done data breach report for several years with their most recent one conducted in the year 2021. This report differs from their previous years report as it has provided some knowledge and insight into the cost of data breaches in cloud computing environment specifically and what are their effects. Firstly, the IBM report had found that there are differences on the average cost of data breach depending on the cloud deployment model as can be seen in Fig. 2.

From Fig. 3, it can be seen that public cloud has the highest average cost of data breach at $ 4.80 million followed by private cloud at $ 4.55 million with hybrid cloud

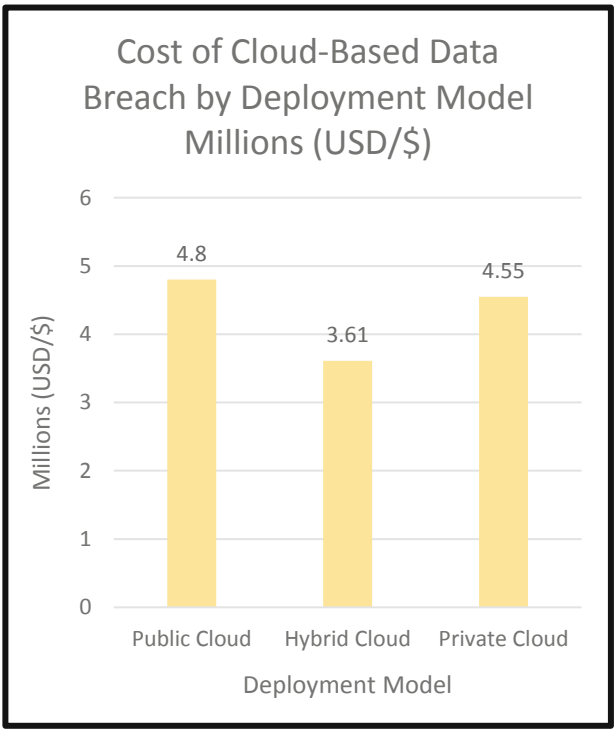

Fig. 2. Cost of Data Breach by Deployment Model [10]

having the lowest average cost at $ 3.61 million. It can be seen there are stark differences in cost of data breach between different deployment model especially difference between hybrid cloud and both public and private cloud. This is as hybrid cloud data breach cost an average $ 1.19 million and $ 0.94 million or in percentage terms 28.3% and 23% less than public and private cloud respectively as can be seen in Fig. 3. This may be attributed to the hybrid cloud model being a combination of other deployment models such as public and cloud that may take advantage of strengths from both deployment models and reinforce their weaknesses [25]. This shows that using hybrid cloud deployment is less risky compared to standalone public or private cloud in terms of data breach exposure as its cost is the lowest.

The level of cloud migration has also been stated by the IBM report to be factors and variables that have effects on the cost of data breach in the cloud. From Fig. 4, it can be seen that organizations with a high level of cloud migration had a higher cost of data breach at $ 5.12 million compared to organizations with a low level of cloud migration at $ 3.46 million. This means that organizations that opt to implement a low-level cloud migration have a data breach cost or exposure that are 38.7% lower compared to an organization that had opted for high-level of cloud migration.

The IBM 2021 data breach report has also state that the stage of an organization cloud modernization journey is a factor that affects their ability to identify and contain data breaches. This is as organizations that are in a mature cloud modernization stage

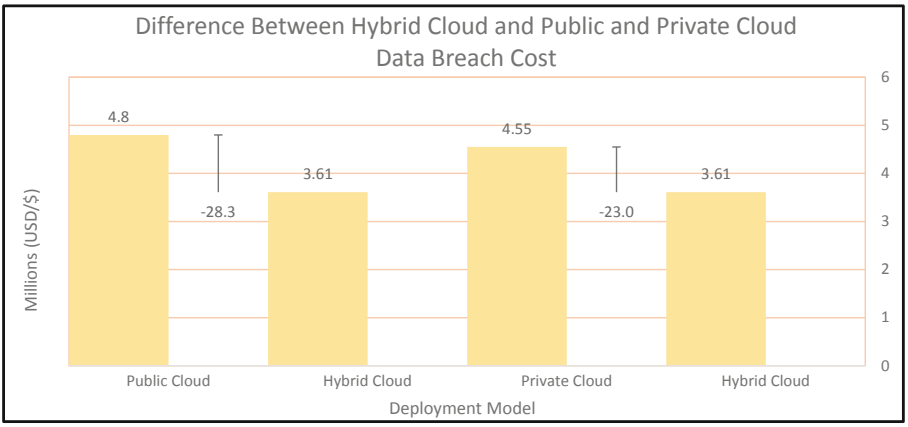

Fig. 3. Difference Between Hybrid Cloud and Public and Private Cloud Data Breach Cost

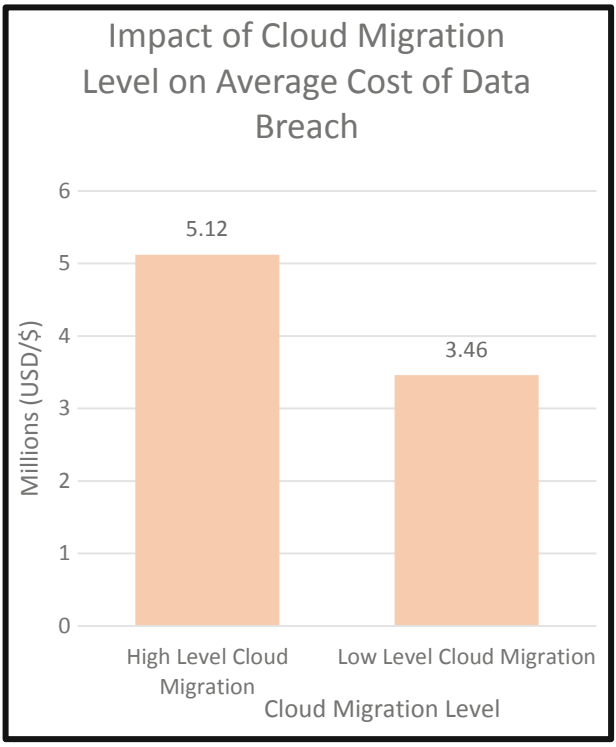

Fig. 4. Impact of System Complexity on Average Cost of Data Breach in the Cloud [10]

takes shorter time to identify and contain data breaches compared to organizations that are in the middle and early stage of their cloud modernization journey as can be seen in Table 1.

Table 1. Days Took to Treat Data Breach by Cloud Modernization Stage [10]

Cloud Modernization Stage	Days Took to Identify Data Breach	Days Took to Contain Data Breaches	Total Days Took to Treat Data Breaches
Mature Stage	193	59	252
Middle Stage	211	67	278
Early Stage	231	98	329

The days took to treat data breach in a cloud computing environment is one of the factors that affect cost of data breach. This is as it has been stated by IBM (2021) that "the longer it took to identify and contain a data breach, the more costly the breach", as such it can be inferred that organizations in the early stage of cloud modernization journey incur the highest cost of data breach. Meanwhile, organizations that are further along in their cloud modernization journey and are in the mature stage incur less severe cost of data breach compared to organizations in the middle and early stage.

This is as, through the IBM 2021 report which had given the global average days it took to identify, contain, and treat data breach and the global average cost of data breach that is 287 days and $ 4.24 million respectively. This would mean that the average of data breach per day is $ 14, 773.52. As such, with this we can calculate the average cost of data breach by cloud modernization stage with: 1) Mature Stage: 252 days X $ 14,773.52 = $ 3,722,927.04; 2) Middle Stage: 278 days X $ 14,773.52 = $ 4,106,963.5; and lastly 3) Early Stage: 329 days X $ 14,773.52 = $ 4,860,488.08. This shows that organizations in mature and middle stage of cloud modernization incur less cost of data breach compared to the average cost of data breach. Meanwhile, organization that are in the early stage of cloud modernization incur more that the average of data breach in case of a data breach.

Furthermore, another interesting fact that were found from the IBM report is that organizations with different degrees and level of digital transformation incur different cost of data breach. This associate with cloud computing as it has been established that cloud computing is the backbone of digital transformation. As such, it can be said that the degree or level of digital transformation can be said to be a degree or level of cloud implementation. Figure 5 shows the average cost of data breach according to their degree and level of digital transformation.

From Fig. 5, it can be seen that organizations with no digital transformation have the highest average of data breach at $ 5.01 million followed by very significant digital transformation at $ 4.26 million, minimal digital transformation at $ 4.13 million, significant digital transformation at $ 3.97 million and lastly moderate digital transformation with lowest average cost of data breach at $ 3.78 million. The figure shows that organizations which have implemented digital transformation no matter the degree or level have lower average cost of data breach compared to organizations that have not implemented digital transformation. Besides that, there are also significant differences between the average cost of data breach by organizations that have no digital transformation and very significant digital transformation which had incurred the second highest average cost is $ 0.75 million which is 16.18% less. This is a stark contrast compared to the difference

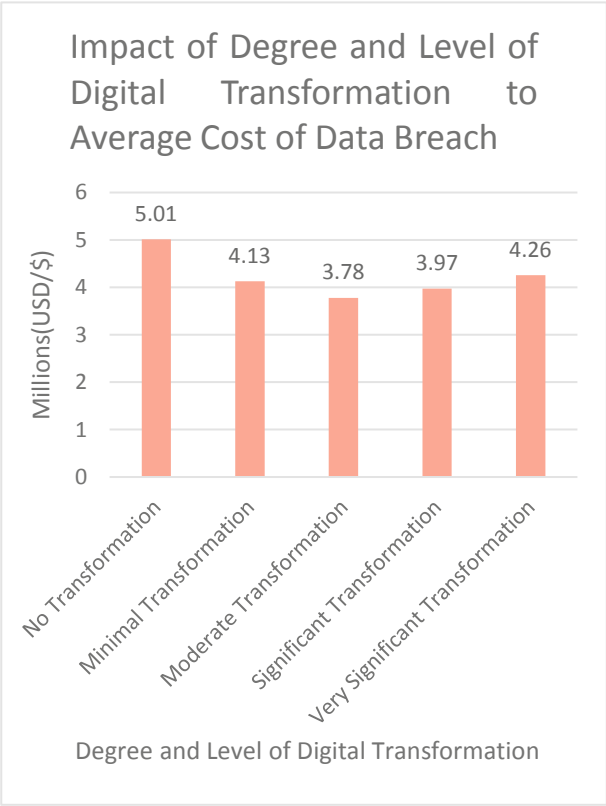

Fig. 5. Impact of Degree and Level of Digital Transformation to Average Cost of Data Breach [10]

of average cost of data breach between organization that implemented moderate transformation which had the lowest average cost and very significant digital transformation which is $ 0.48 million which is 11.94% less as can be seen in Fig. 6. This shows that across-the-board organizations that have implemented digital transformation have less exposure due to data breaches compared to organization that did not implement digital transformation.

From this review, it can be inferred that there are several factors that organizations need to take into consideration regarding the threat and cost of data breach in a cloud computing environment. These are cloud deployment models, level of cloud migration, their stage of cloud modernization, and their level and degree of digital transformation.

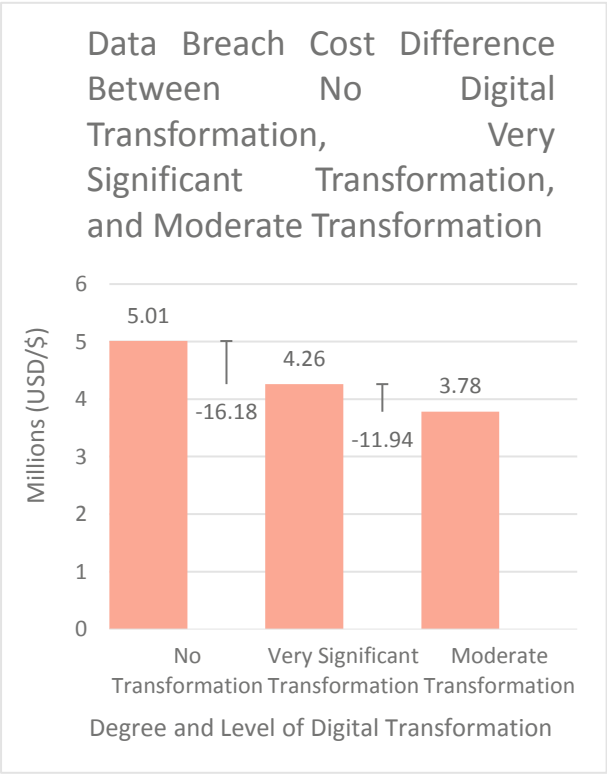

Fig. 6. Cost Difference Between No Digital Transformation, Very Significant Digital Transformation, and Moderate Transformation

4 Conclusion

Rapid advances of technology cause by the industrial revolution 4.0 such cloud computing have created many opportunities and benefit for organization in most sectors which has created more value for these organizations. However, challenges and risk have also been created such as data breach which must be able to identify, evaluate, understand, and if needed control and treat these risks as to maximize on the benefit and opportunities that these technologies can bring. This paper acknowledges the cost and exposure that a data breach in a cloud computing environment can cause. It has shown the factors that organizations must take into consideration in regard to data breaches in the cloud computing environment which are 1) deployment models, 2) levels of cloud migration, 3) their stage of cloud modernization, and 4) their level and degree of digital transformation. These information and data shown can be used further to truly understand the cost of data breach in a cloud computing environment by using calculation techniques such as cost-benefit analysis and etc.

Acknowledgments. We are grateful to Multimedia University, Faculty of Management, family members, and other individuals for their kind support and encouragement.

Authors' Contributions. The first author was responsible the resources acquisition and writing of the draft and paper. The second and third author are responsible for supervision and reviewing of the paper. All authors were responsible for the conceptualization of the paper.

References

1. Simeone, A. Caggiano, L. Boun, & R. Grant., "Cloud-based platform for intelligent healthcare monitoring and risk prevention in hazardous manufacturing contexts," *Procedia CIRP*, 99, 50–56. 2021, https://doi.org/10.1016/j.procir.2021.03.009
2. R. Rahman, & T. Mahmud., "Integrating Cloud Computing in E-healthcare: System Design, Implementation and Significance in Context of Developing Countries," *5th International Conference on Electrical Engineering and Information Communication Technology (ICEEICT),* 2021.
3. A.H Seh, M. Zarour, M. Alenezi, A.K. Sarkar, A. Agrawal, R. Kumar, & R.A. Khan, "Healthcare data breaches: Insights and implications," In *Healthcare (Switzerland)* (Vol. 8, Issue 2), 2021. MDPI AG. https://doi.org/10.3390/healthcare8020133
4. M.J. Rahman, B.I. Morshed, B. Harmon, & M. Rahman., "A pilot study towards a smart-health framework to collect and analyze biomarkers with low-cost and flexible wearables," *Smart Health*, 2022. https://doi.org/10.1016/j.smhl.2021.100249
5. R.J. Kauffman, D. Ma, & M. Yu., "A metrics suite of cloud computing adoption readiness," *Electronic Markets*, *28*(1), 11–37, 2018. https://doi.org/10.1007/s12525-015-0213-y
6. Z.R. Alashhab, M. Anbar, M.M. Singh, Y.B. Leau, Z.A. Al-Sai, & S.A. Alhayja'a., "Impact of Coronavirus Pandemic Crisis on Technologies and Cloud Computing Applications," *Journal of Electronic Science and Technology*, *19*(1), 25–40, 2021. https://doi.org/10.1016/j.jnlest.2020.100059
7. P. Hopkin., *Fundamentals of Enterprise Risk Management – Understanding, evaluating and implementing effective risk management*, 2017.
8. E. AbuKhousa, N. Mohamed, & J. Al-Jaroodi., "e-Health Cloud: Opportunities and Challenges," *Future Internet*, *4*(3), 621–645, 2012. https://doi.org/10.3390/fi4030621
9. S. Mitropoulos, & A. Veletsos., "A Categorization of Cloud-Based Services and their Security Analysis in the Healthcare Sector," *SEEDA-CECNSM 2020 - 5th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference*, 2020. https://doi.org/10.1109/SEEDA-CECNSM49515.2020.9221808
10. IBM., "IBM Cost of a Data Breach Report", 2021.
11. COSO., "COSO Enterprise Risk Management for Cloud Computing", 2012.
12. Ali., D. Warren, & L. Mathiassen., "Cloud-based business services innovation: A risk management model," *International Journal of Information Management*, 37(6), 639–649, 2017. https://doi.org/10.1016/j.ijinfomgt.2017.05.008
13. N. Mekawie, & K. Yehia., "Challenges of deploying cloud computing in eHealth," *Procedia Computer Science*, *181*(2019), 1049–1057, 2021. https://doi.org/10.1016/j.procs.2021.01.300
14. O.K.J. Mohammad., "Recent trends of cloud computing applications and services in medical, educational, financial, library and agricultural disciplines," *ACM International Conference Proceeding Series*, 132–141, 2018. https://doi.org/10.1145/3233347.3233388
15. L.P. Junior, M. Alexandra Cunha, M. Janssen, & R. Matheus., "Towards a framework for cloud computing use by governments: Leaders, followers and laggers," *ACM International Conference Proceeding Series*, 155–163, 2020. https://doi.org/10.1145/3396956.3396989
16. M. Hölbl, M. Kompara, A. Kamišalić, & L.N. Zlatolas., "A systematic review of the use of blockchain in healthcare," *Symmetry*, *10*(10), 2018. https://doi.org/10.3390/sym10100470

17. F. Gao, & A. Sunyaev., "Context matters: A review of the determinant factors in the decision to adopt cloud computing in healthcare," *International Journal of Information Management*, *48*(July 2018), 120–138, 2019. https://doi.org/10.1016/j.ijinfomgt.2019.02.002
18. Sultan, N., Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management*, *34*(2), 177–184, 2014. https://doi.org/10.1016/j.ijinfomgt.2013.12.011
19. Alghamdi, L.E Potter, & S. Drew., "Validation of architectural requirements for tackling cloud computing barriers: Cloud provider perspective," *Procedia Computer Science*, *181*, 477–486, 2021. https://doi.org/10.1016/j.procs.2021.01.193
20. Maniah, B. Soewito, F.L. Gaol, & E. Abdurachman., "A systematic literature Review: Risk analysis in cloud migration," *Journal of King Saud University - Computer and Information Sciences*, 2021. https://doi.org/10.1016/j.jksuci.2021.01.008
21. NSH., "Health and social care. Disability," 88–105, 2018. https://doi.org/10.4324/9781315624839-5
22. N.S. Abouzakhar, A. Jones, & O. Angelopoulou., "Internet of Things Security: A Review of Risks and Threats to Healthcare Sector," *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, IThings-GreenCom-CPSCom-SmartData 2017*, *2018-Janua*, 373–378, 2018. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.62
23. H. Abrar, S.J. Hussain, J. Chaudhry, K. Saleem, M.A. Orgun, J. Al-Muhtadi, & C. Valli., "Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry," *IEEE Access*, *6*, 19140–19150, 2018. https://doi.org/10.1109/ACCESS.2018.2805919
24. Verizon., "*DBIR 2021 Data Breach Investigation Report*.", 2021.
25. A.M. Helmi, M.S. Farhan, & M.M Nasr., "A framework for integrating geospatial information systems and hybrid cloud computing," *Computers and Electrical Engineering*, *67*, 145–158, 2018. https://doi.org/10.1016/j.compeleceng.2018.03.027