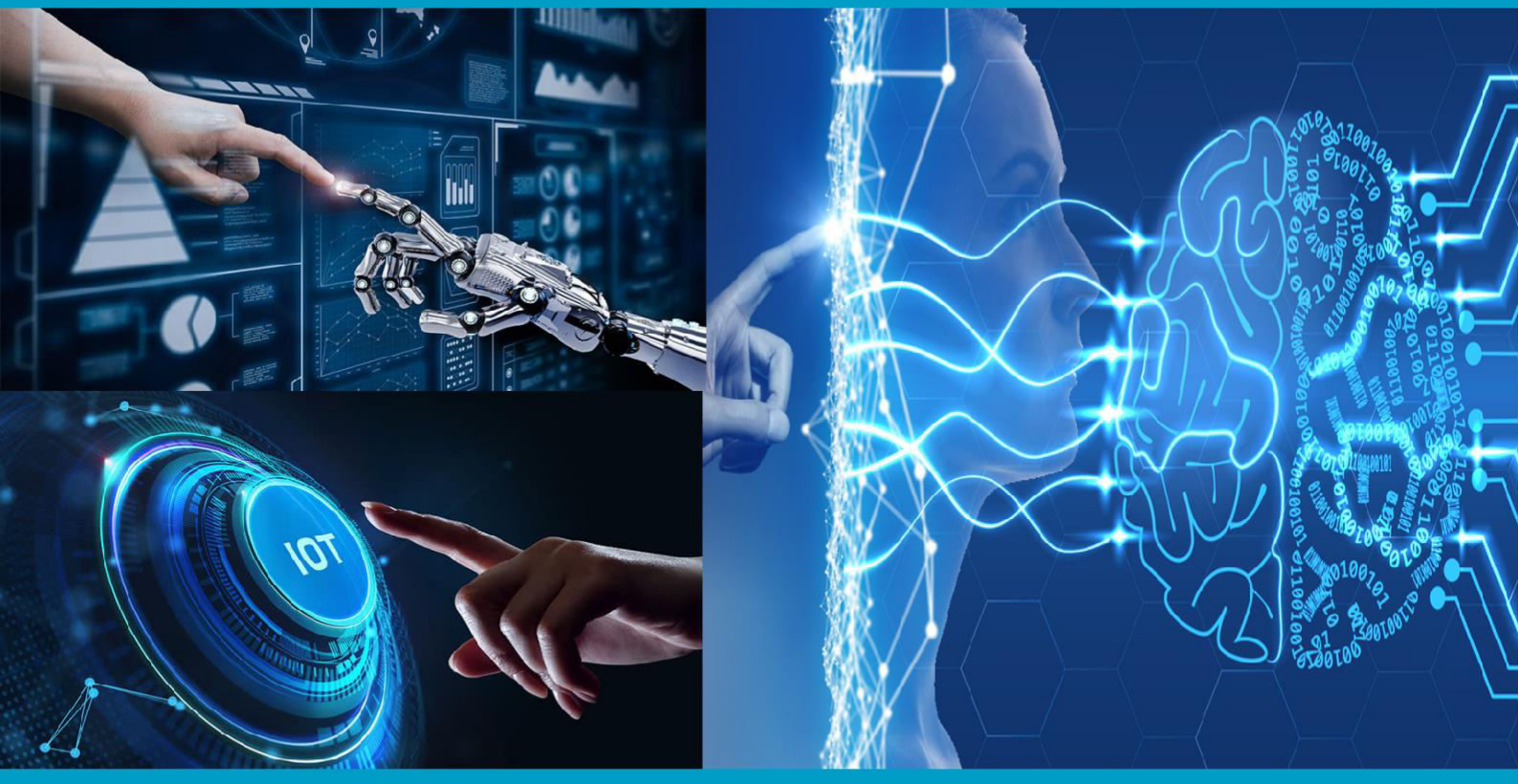
IJMRSETM

e-ISSN: 2395 - 7639



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 9, Issue 4, April 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.580

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580|

| Volume 9, Issue 4, April 2022 |

| DOI: 10.15680/IJMRSETM.2022.0904026 |

A Study Based on the Identification of Security Challenges in Implementing Cloud in the Healthcare Sector

Surksha, Rekha

Assistant Professor, CSE Department, CBS Group of Institutions, Haryana, India

ABSTRACT: This research paper includes an identification of security challenges in executing the "cloud" in the "healthcare" sector. Authentic literature is reviewed in order to accurately identify the challenges related to security in cloud technology implementation in the healthcare sector. Secondary qualitative methodology is used in this study regarding the data collection process. This research has identified open-source sharing as a key cause of cloud security challenges that can be addressed by data encryption technology.

I.INTRODUCTION

The concept of "cloud computing" includes the transmission of a wide range of computing services along with storage, servers, networking, database, analytics and intelligence. There are numerous challenges associated with the cloud which have been faced in the healthcare sector, for example, security threats. This review paper includes a problem statement, research aim, as well a review of existing literature followed by a methodology and conclusion.

II.CONTEXT OF RESEARCH

Cloud is one of the most effective solutions in order to address digital issues and problems. Thus, security is one of the focal problems which is associated with the implementation of the cloud in healthcare. In the present situation, new technology has been used in clinical services along with the increased application of "cloud computing solutions", "artificial intelligence", telemedicine and "electronic health records". Cloud computing delivers different types of services rather than owning just a simple computing system. The cloud service providers offer access to the cloud storage that includes numerous segmented clinical data of the patients in the healthcare setting. It can be noted that a wide range of information has been generated by healthcare which requires a synchronized database to access required data in a quick manner. Along with that, identification of the "security challenges" in implementing cloud in the healthcare sector is one of the key aspects which has been raised by health researchers who need to access patient's extensive data regarding any scientific analysis.

III.PROBLEM STATEMENT

Cloud security safeguards the personal data of patients in terms of medical history and clinical records including medication profiles which must be readily accessible to the authorised healthcare specialists only. The challenges related to the security of cloud computing have been influenced by the unorganised data storing process in the healthcare sector without identifying its precise physical location. The nature of cloud computing involves security issues, for example, misconfiguration of the cloud settings that lead to data breaches, insecure interfaces, unauthorised access, cyberattack, external data sharing and lack of visibility. The management of the healthcare sector has been faced with a tremendous issue because of security threats in the implementation of the cloud. New challenges in cloud implementation have emerged with the epiphany, the growth and the high use of cloud technologies in a wide range of healthcare organisations. Accordingly, there are certain new security challenges regardingaccessibleresolutions to "cloud computing" that also must be reviewed and examined.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580|

| Volume 9, Issue 4, April 2022 |

| DOI: 10.15680/IJMRSETM.2022.0904026 |

IV.AIM

This research paper aims to examine different literature associated with the identification of security challenges in cloud implementation in the healthcare sector including mitigation solutions. In this manner, this research additionally aims to evaluate possible solutions to mitigate the challenges associated with the security issues of cloud implementation in the "healthcare sector".

Objectives

- To identify security "challenges in implementing cloud in the healthcare sector"
- To examine potential solutions for addressing the identified challenges in the healthcare sector

Questions

- What are the security challenges threatening the implementation of the cloud in healthcare?
- What are the resolutions to mitigate the security challenges of cloud implementation in healthcare?

V.LITERATURE REVIEW

"Security challenges and solutions using healthcare cloud computing"

The cloud computing has been adopted by numerous healthcare organisations to keep a record of patients' data in an electronic format that allows easy accessibility to the database of health information. In this research, the authors also discussed that cloud technology allows the healthcare experts to share resources including networks, servers application software and storage tools for accessing the information of the patients. Moreover,Yao[16] also confirmed that the availability of patient data is a significant requirement in the medical, clinical and healthcare sectors. It can be noted that cloud technologies are highly anticipated in the healthcare sector in terms of patient portals, mobile apps, electronic medical records, big data analytics and devices compatible with the Internet of Things (IoT) [6]. Shorter[5] argued that cloud computing significantly focuses on the servers in healthcare organisations, networks among healthcare experts, and storage tools accessed by authorised medical staff regarding the availability of patient information in any circumstances.

On the other hand, the "cloud in electronic health records" additionally allows the patients regarding simple and wide accessibility to their health information. The way of implementation of cloud computing transforms which manner "doctors", "nurses", "clinics" and "hospitals deliver" the quality medical services to the patient's effective treatment process. More specially, the issues in the healthcare sector comprise infrastructural and operational costs, concerns, security to real-time data sharing as well as robust backup [13]. As per the perception of Mrozek[14], in-house operational and infrastructural costs in the healthcare sector have been reduced due to the application of "cloud computing" technologies.

It is very much important that the massive data stored by the healthcare organisations must be accessed by the researchers and physicians and that's why the implementation of cloud technologies faces an issue related to confidentiality concerns [3]. Based on the study of Mirshekari[12], it can be identified that the security challenge in the cloud is mainly influenced by its inherent features that compromise privacy, for example, massive infrastructure sharing, lack of network environment, proliferation and remote data storage. In this manner, both healthcare organisations and cloud computing providers are required to pay careful consideration to the exactdocumentation of "security challenges" and their properresolutions for successful implementation. According toTamrawi [1], "data encryption" is a productive line of secured processes in cyber security architecture that creates"interrupted data" use as complicated as possible to address security issues in cloud computing. However, negligent and malicious individuals might create a threat related to data security in cloud technology which can be secured by applying data encryption techniques with a higher amount of computing potency.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580|

| Volume 9, Issue 4, April 2022 |

| DOI: 10.15680/IJMRSETM.2022.0904026 |

"Security Challenges in Healthcare Cloud Computing"

According toGhazisaeedi[12], advanced technology like cloud computing is vulnerable to cyber gaps that create a negative influence on the privacy and security of a patient's EHR (electronic health records). In this type of situation, the management of the healthcare sector must carefully understand and consider the security contests of the wireless systems including the cloud. Moreover, advanced information technology has brought a revolution in medical history which has gained the aptitude to automatically store and relocate"health information" regarding the early recovery of the patients. The authorised healthcare providers should always access the health information along with the researchers who try to discover any cure, treatment or cause of any disease [11]. In this manner, a powerful calculation tool is required by healthcare organisations in order to deal with massive amounts of patient data. The healthcare specialist must complete medical information in order to deliver accurate and complete treatment for the early recovery of the patients [10]. Presently, the development of the IT industry has influenced the expansions of remote healthcare systems in order to provide health services in an efficient manner. The sureness of "users in tele-health systems" is increased due to accessible healthcare information in terms of confidentiality and communications security [8].
A considerable amount of data is being generated by developments in health care information systems regarding data processing and data storing. It can be noted that dynamic and scalable resources are required for data mining algorithms or secondary use of clinical data. The appearance of "cloud computing technology"by efficient benefits is one of the present main challenges. In order to meet the requirements of the "medical care industry", a widespreadamount of servers and computers are particularly dedicated to healthcare cloud computing regarding a secured internal communication process. As per Cilleruelo[4], cloud technology allows the registered and authorised users to contact the software and hardware by a third section in a remote location dramatically changing the mode of information storing and accessibility. On the other hand, in the field of healthcare, security is a key barriers that limit the development of "cloud computing" due to the requirement of a high level of data interoperability, incorporation and distributionamid different "healthcare" experts. In this way, a wide range of hospitals must be able to develop standard procedures and guidelines regarding the identification of security challenges with respect to enhanced information security in healthcare "cloud computing"[9].

e-Health "Cloud Security Challenges"
Computer security is an expanding area in computer science that considers the protection of electronic data and computer systems against hardware theft, unauthorised access, and data manipulation [1]. In addition to that, the significance of computer security includes protection from backdoors, denial-of-service attacks and phishing which is directly associated with cloud technology in the healthcare sector.
Privacy alternatively is measured as one of the key purposes of security issues that create enforcement for certain principles and rules in order to regulate an extension that sets a limit about how authorised people can gather, access or transmit healthcare data to a second or third party. In this manner, cloud computing technology usually operates in a shared and open environment that highly influences the security issue that makes the cloud more vulnerable to data theft, loss and malicious attack. A complete diffusion of the cloud technology is mainly hindered by the weak cloud security in the healthcare industry as a key challenge and because of that most healthcare professionals have trust issues.

VI.METHODOLOGY

This review paper has examined existing literature associated with security challenges in cloud implementation in the healthcare sector. Secondary data from various databases such as Google Scholar has been collected in this review paper in order to examine the security issues connected to the cloud faced by healthcare professionals. Moreover, qualitative research process has been applied in this research in order to achieve all research objectives.

VII.FINDINGS

It can be found that cloud computing is based on an open-source data sharing system that includes numerous advantages but malicious activities provoke security vulnerabilities in cloud technology. Based on the review of existing literature, a few mitigation strategies have been identified in order to overall security challenges in "cloud

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580|

| Volume 9, Issue 4, April 2022 |

| DOI: 10.15680/IJMRSETM.2022.0904026 |

computing", for example, data encryption technology. Moreover, it has been identified that the cloud service provider and healthcare management both jointly focus on the "security issue" in cloud implementation in the healthcare sector. Despite the fact that cloud technology includes several advantages, there are some challenges and drawbacks. In order to adopt cloud computing, healthcare organisations hesitate because of security concerns including the privacy of patients, confidentiality and service costs [15].

There are several reasons associated with the transparency of cloud technology, for example, healthcare cannot get rid of control regarding their medicinal records. According to Kotz[2], mobile computing technology has the ability to bring transformation in the healthcare industry which required modification in privacy requirements. By undertaking a broad literature, the authors also proposed a theoretical privacy outline for applications used in the healthcare sector regarding the development of cloud security assistance and cloud security. On the other hand, another framework is proposed by [7] which allows secured operations of electronic health records over the cloud between several providers of healthcare professionals.

VIII.CONCLUSION

This review paper includes an exploration of security challenges associated with cloud computing in the healthcare sector. Furthermore, a wide range of secondary information has been accessed in this review paper regarding the identification of the cloud security challenges in the healthcare sector. In this manner, possible ways to encounter this challenge are also developed in this review paper regarding the progress of an effective and efficient research paper, such as data encryption technology. It is recommended that healthcare professionals should use data encryption to mitigate cloud security challenges. This research includes a few limitations, such as a lack of data validity. In other words, the lack of data validity is a key limitation that restricted the accurate findings of this review paper.

REFERENCES

[1]Al-Issa, Y., Ottom, M.A. and Tamrawi, A., 2019. eHealth cloud security challenges: a survey. Journal of healthcare engineering, 2019.
[2]Avancha, S., Baxi, A. and Kotz, D., 2012. Privacy in mobile technology for personal healthcare. ACM Computing Surveys (CSUR), 45(1), pp.1-54.
[3]Behl, A., 2011, December. Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In 2011 World Congress on Information and Communication Technologies (pp. 217-222). IEEE.
[4]Bildosola, I., Río-Belver, R., Cilleruelo, E. and Garechana, G., 2015. Design and implementation of a cloud computing adoption decision tool: Generating a cloud road. PloS one, 10(7), p.e0134563.
[5]Chow, F., Muftu, A. and Shorter, R., 2014. Virtualization and cloud computing in dentistry. Journal of the Massachusetts Dental Society, 63(1), pp.14-17.
[6]Griebel, L., Prokosch, H.U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., Engel, I. and Sedlmayr, M., 2015. A scoping review of cloud computing in healthcare. BMC medical informatics and decision making, 15(1), pp.1-16.
[7]Ibrahim, A., Mahmood, B. and Singhal, M., 2016, May. A secure framework for sharing electronic health records over clouds. In 2016 IEEE International Conference on Serious Games and Applications for Health (SeGAH) (pp. 1-8). IEEE.
[8]Khan, F.A., Ali, A., Abbas, H. and Haldar, N.A.H., 2014. A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. Procedia Computer Science, 34, pp.511-517.
[9]Kuyoro, S.O., Ibikunle, F. and Awodele, O., 2011. Cloud computing security issues and challenges. International Journal of Computer Networks (IJCN), 3(5), pp.247-255.
[10]Lupşe, O.S., Vida, M.M. and Stoicu-Tivadar, L., 2012, April. Cloud computing and interoperability in healthcare information systems. In INTELLI: The First International Conference on Intelligent Systems and Applications.
[11]Mehraeen, E., Ayatollahi, H. and Ahmadi, M., 2016. Health information security in hospitals: the application of security safeguards. Acta informatica medica, 24(1), p.47.
[12]Mehraeen, E., Ghazisaeedi, M., Farzi, J. and Mirshekari, S., 2017. Security challenges in healthcare cloud computing: a systematic review. Glob. J. Health Sci, 9(3).

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580|

| Volume 9, Issue 4, April 2022 |

| DOI: 10.15680/IJMRSETM.2022.0904026 |

[13]Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M. and Vahedi, F., 2021. Security challenges and solutions using healthcare cloud computing. Journal of Medicine and Life, 14(4), p.448.
[14]Mrozek, D., 2020. A review of Cloud computing technologies for comprehensive microRNA analyses. Computational biology and chemistry, 88, p.107365.
[15]Sajid, A. and Abbas, H., 2016. Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. Journal of medical systems, 40(6), pp.1-16.
[16]Yao, Q., Han, X., Ma, X.K., Xue, Y.F., Chen, Y.J. and Li, J.S., 2014. Cloud-based hospital information system as a service for grassroots healthcare institutions. Journal of medical systems, 38(9), pp.1-7.

Impact Factor: 7.580

INTERNATIONAL JOURNAL
OF MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com

www.ijmrsetm.com