The Security Challenges in Healthcare Cloud Computing

Talal Alsuwaidani

University of Qassim, Buraydah, Saudi Arabia

Abstract

Healthcare data is one of the most sensitive data that should be protected, and its accessibility must not be available for everyone. There are several available methods of saving this type of data, including cloud computing technology. Cloud computing has become one of the leading information technologies that allow more effective computing by centralizing data storage. Recently, one of the most critical challenges facing the cloud computing environment is the security concerns, which has become a challenging issue at present and therefore has been given increasing attention. Thus, this study involves understanding the challenges facing cloud security and how to overcome them, besides the relationship between the infrastructures and maintaining healthcare data security. In this study, 20 published studies between 2013 and 2021 have been reviewed and analyzed in order to obtain the desired outcomes. This study showed that using cloud computing systems in healthcare could expose patient-sensitive data to theft or be accessed by unauthorized persons. Also, this technology involves some challenges such as legal amenabilities, lack of control, trust, consistency, and quality, besides the asset issues, data sharing, availability, secrecy and recovery, geographical data location, as well as unauthorized data access. Furthermore, this study provides several methods to preserve health information security in the cloud system.

Keywords: *Healthcare cloud computing, Security, Healthcare infrastructure, Cloud computing challenges.*

I. INTRODUCTION

A. An overview

Recently, new electronic technology has been developed that can store, transmit and use information related to health care matters for the disease, and this contributes to improving the quality, efficiency, and effectiveness of health care systems and the services provides [1]; [2]. Cloud computing technology has spread in the world in recent decades, as it has become one of the most widely used technologies. In addition, cloud computing applications are widely used in daily life and for their various activities. Cloud computing technology has become widespread in various aspects of life. It has become used in industrial and educational institutions. In addition, it has been widely applied in health care [3]. In addition to the contribution of cloud computing technology to the provision of services, it has had an important impact on the way applications were developed, which had a significant impact in reducing the time required to develop such applications and providing information technology resources.

B. Cloud Computing

Cloud computing is based on two leading technologies, grid computing and virtualization [4]. Grid computing can be defined as a group of geographically distributed computers that facilitate virtual simulation and have great computational power [4]. While virtual simulation can be defined as a way of visualizing the occurrence of things without their actual occurrence or physical form, this facilitates understanding and visualizing the nature of interactions between different systems [4]. In addition, cloud computing includes providing services over the Internet. These services, such as Software-as-a-Service (SaaS) enable users in this cloud to remotely control the operation and use of applications. Software-as-a-Service (SaaS): This considers computing resources to be a service. This includes having virtual computers in the cloud with Internet access, storage bandwidth, and guaranteed processing power. An example of IaaS is Amazon EC2, which sets up and configures virtual servers via web-based lists within minutes [5]. While concerning the platform (PaaS), it is very similar to IaaS, but it is different from IaaS in that it includes operating systems and services for applications, and a famous example of it is the Google search engine [6]. Data-Storage-as-a-Service (dSaaS): This service provides storage and bandwidth requirements which the user uses. Figure 1 shows cloud computing layers architecture.

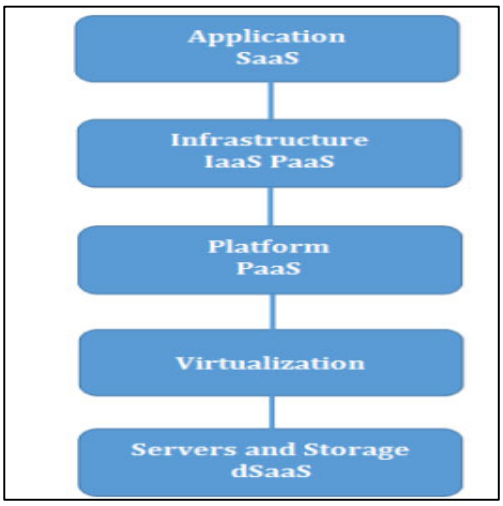

Figure 1: Cloud computing layers architecture [4].

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.96

C. Cloud computing types

1. Public Cloud:

The public cloud contributes to providing various means of preparation and convenience to the public so that billions of people can share the different resources available simultaneously, such as Microsoft, Google, and Amazon [7].

2. Private Cloud:

This type of cloud is intended for one job only. In such a cloud, highly private and sensitive data is controlled. This data is controlled in detail from where it is stored or accessed. Examples include medical care records, banks, medical offices, employment information, and other examples [7].

3. Hybrid Cloud:

This type of cloud is more complex than both public and private clouds. For example, an organization that requires maintaining the confidentiality and security of secured data on a private cloud works to provide more public content. Figure 2 shows Communication between different clouds.

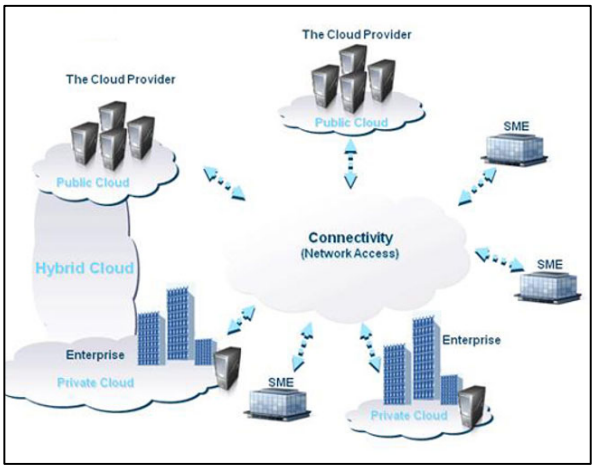

Figure 2**:** Communication between different clouds**.**

D. Cloud Computing in Health Care

Due to the many developments and improvements in cloud computing technologies in healthcare, this technology is becoming increasingly popular today. This contributed to direct and easy access to medical records and their transfer, in addition to the possibility of accessing medical care information and the patient's sick record simply and directly. The most critical thing facing hospitals at present is the vast and continuous growth of medical data, and therefore this requires the existing systems in the cloud computing technology to archive the data after completing the treatment of patients and to access and use it at any time that requires calling it. Cloud computing systems can centralize healthcare data and medical records [7].

E. The challenges of Cloud Computing Security in Health Care

Data security usually refers to protecting both data and information, and the protection of devices that store and transmit data. The most significant challenges that users face regarding privacy and security are a lack of faith in the security of data in the cloud, loss of governance, risk management, indefinite provider obedience, and organizational inertia. Security, data protection, and privacy can be enabled through policies, technology, training and vigilance programs, and technology. It is essential to maintain the safety and confidentiality of the health care area from a legal and ethical standpoint. One of the most important causes of security holes in data protection is the virtual infrastructure based on web networks. Moreover, the risks arising from cyber-attacks and hacking are among the most critical challenges facing data related to healthcare. Hackers have many methods to access and breach information security and confidentiality [8].

II. RELATED WORK

Mehraeen et al. [2] study show that many factors control health care security, such as identity management, document access to the Internet and authentication assurance, access control of the virtual cloud environment, and preventing cybercriminals from hacking the Computerized cloud. Also, this study discusses the challenges facing and hindering cloud computing technology, such as access control, data mobility, and threats related to sensitive information and software in health care institutions and the diversity of rent. This study concluded that one of the most critical measures to improve security and data protection in cloud computing is a comprehensive understanding of concerns and work to find measures and implement them effectively.

Mohiuddin and Almogren [9] discussed the security challenges that are facing cloud computing and their strategies. Due to the wide adaption of a cloud computing system in the healthcare field, the most critical aspect of this adoption is to maintain data privacy, processing, and control through using the UPECSI model, which integrates privacy within the services provided by the computerized cloud. In addition, to maintain the confidentiality Authentication by developing a two-factor authentication system based on the presence of Layer Security (DTLS) protocol by putting in a DTLS layer supported by RSA and designed for 6LoWPANs. It is located between the application and transport layers.

A study conducted by Faridi et al. [10] found that health monitoring and cloud computing are increasingly linked together since healthcare equipment provides both the proper monitoring and a collection for the records of health, establishing cloud computing services. Another outcome was found that the digitalization for anything provides the benefits for the availability of the records for the patient, although the process of saving these records is a bit difficult such as being vulnerable to vandalism, threaten, accessed by who do not have the access. Another study performed by Salehi et al. [11] showed that cloud computing is a technology growing fast in the healthcare sector. Although it is commonly used, some challenges are met in this sector.

For instance, access to data within a healthcare sector may occur, such as changing them by untrusted humans. Also, some sensitive data regarding the patient may be accessed and published by the vandals. However, although it suffers from some challenges, some strengths support the utilization of cloud computing. Based on Prathap [12], it was found that several requirements are necessary to be inserted in any sector which uses cloud computing technology, such as data storage protection and data transmission protection. The level of the required protection depends on the importance of the stored data like the healthcare sector. Prathap mentioned that by cloud computing, the internet provider will be supported with scalable resources provisioned, but the operation models play a role in obtaining the desired security.

According to Al-Marsy [13], health information systems and (HIS) as well as Electronic Health Records (EHR) have to become crucial aspects in the healthcare field because of the features which they provide since these features became lifesaving. Based on this research, it was found that by using cloud computing, the availability, reliability, intelligence in healthcare are increased, although there are some risks and challenges that are possible to be met. Some of these challenges included in this research are the expected financial performance and the required cost to achieve the desired security for transmitting the data or to keep it safe.

According to Chenthara [14], the biggest threat to the adoption in the healthcare domain is caused by involving external cloud partners: many data safety and security issues are still to be solved. Until now, cloud computing has been favored more for singular, individual features such as elasticity, pay-per-use, and broad network access, rather than as a cloud paradigm on its own.

According to Griebel et al. [15], an examination regarding the challenges that cloud computing suffers from, especially in the health field, has been conducted. Further, this research submitted an interview about the cloud experts, hospital managers, and doctors that have been carried out in order to achieve the saturation of the information. Moreover, an outcome that was obtained from this research proved that the computing cloud is a beneficial tool and must be deployed, although the available infrastructure is not considered as not encouraging, and it needs to be improved. Another outcome from this search stated that the human factors must be considered since they are essential.

Another research has been conducted by Khan, [16] technology for data obtainability, processing, management because the illegal accesses for data are met these days. Although this technology has several benefits, it suffers from many securities challenges, including lack of control, trust, consistency, and quality, besides legal amenabilities, asset issues, data availability, sharing, recovery, unauthorized data access, geographical data location, and data secrecy. However, it was concluded that these challenges could not be easily overcome if the organization was not careful enough, especially in the healthcare sector since it is a sensitive sector.

Al-Issa [17] stated that cloud computing poses opportunities and suffers from some issues; these are observed because cloud computing operates in a shared and open environment; therefore, it is vulnerable to data loss, malicious attacks, and theft. Further, the weakness of cloud security is considered one of the most critical issues hindering a complete diffusion for the cloud in the healthcare industry. An example of why healthcare professionals own various reasons not to trust the cloud is they cannot provide a way to control their medical records. Moreover, there are different security risks such as failure to separate the virtual user and privilege abuse.

According to Rath [18], cloud computing is considered the developing zone responsible for computing innovation. The most crucial point about this technology is that it neglects the need for the total framework programming and equipment to obtain the clients' applications and prerequisites. However, some standard internet programs and a significant internet association are required. A particular downside for cloud computing is observed which is regarding the security perspective although it provides the client tremendous abilities such as getting into a large number of some utilization without the necessity of having an acquiring, permit, introducing or even downloading any applications.

Furthermore, Kaur [19] study defined cloud computing as a technology that tries to ease and achieve flexibility for their data storage, upgrade their effectiveness, cost, ability, and interoperability. This new technology can empower the timely delivery of medical records to whatever they are needed. This research stated that this technology has various benefits, and the challenges can be overcome if an expert properly deals with them.

Moreover, Chauhan & Kumar's [20] study focused on the benefits of using a cloud-based healthcare system. One of the most important benefits of using the electronic cloud in the healthcare business is cost savings due to the reduced number of employees required to manage user data, reducing potential errors, and increasing data extraction speed. In addition, cloud computing significantly reduces the complexities of data technology. In addition to that, it was found that the health cloud improves performance by improving patient care so that the complete medical history of patients is displayed in the form of digital records at any time. Also, the cost of infrastructure, maintenance, the software would be less. Although cloud computing systems have various advantages when used in health care facilities, they suffer from several issues, such as the difficulty of maintaining the patient's data security.

According to Kamoona, & Altamimi [21], it was concluded from this research that health care in the field of cloud computing must include the presence of particular specifications that must be taken into account carefully and

with complete caution in order to reach a wholly safe and sound scheme and the number of security requirements that must be taken into account in the event of developing Safety systems for health care programs. Also, in this research, a detailed scheme was created that contains the methods used to secure health records. These methods were divided into two levels, the first being the encrypted level and the second the unencrypted.

Dang et al.'s [22] survey focus on the applications of the Internet of Things (IoT) in health care and the trends of particular markets in their application. Also, in this survey, the focus was on the models used in cloud computing, and in particular, fuzzy computing was discussed in detail, which is the basis for the applications used in the health care field. In addition, the reason behind the adoption of fog computing for healthcare applications was discussed because, after deep research, it was found that it is the most suitable for such intelligent applications. Shabbir et al.[23] study focused on the most critical security strategies and practices that should be put in place to prevent weaknesses in the computerized electronic cloud of health care systems or in order to prevent any potential security breaches, and this concern is due to privacy and security due to the importance of health information in addition to that these security measures contribute to take full advantage of health services and facilitate dealing with them. The Encryption Standard (MES) has been adopted in stratified modelling systems to provide health information security. In addition, a comparison was made between the use of the proposed model for developing information security in the computerized cloud for healthcare systems in comparison with the standard algorithms in health information security, and it was found that the performance of the proposed model outperforms

The study of Darwish et al. [24] outlines new concepts for healthcare applications such as CC and IoT (CloudIoT-Health). The main objective of this paper is to present the current vision for the integration of CC and IoT into healthcare applications. By providing and analysing the latest technologies and gap analysis within the different levels of integration components in addition to detailed analyses in CloudIoT-Health systems. Through all the research related to the integration of CC and IoT, in this paper, a comprehensive review was prepared in health care systems, in addition to identifying the challenges facing future research directions and working to provide a bibliography on a large scale.

According to Al Nuaimi et al. [25], the problems that impede the implementation of e-health systems within the computerized cloud were presented. During this study, the existing solutions within the computerized cloud for health care systems were reviewed, whether these solutions were proposed or realistically implemented. In addition, this research paper includes the most critical technical or technical problems in order to reach solutions within the framework of cloud computing, and provide many solutions for applications related to electronic health, and compare them with current issues.

According to Bharati et al. [26], this study was conducted in order to focus on the strengths and weaknesses in addition to the challenges facing cloud computing on the Internet of Things and its use in the field of health care. An analysis of some of the current limitations in computational capacity, scalability, communication protocols, data security, and infrastructure was conducted. The characteristics of cloud computing and its privacy issues were discussed. A framework for healthcare over the Internet (IoThNet) was introduced that enables hospitals to collect patient information through a persistent data layer. This study also touched on the use of smartphone applications that contribute to follow-up and diagnosis of patients, clinical communication, and drug review.

A study has been completed concerning the infrastructure aspect by Malik, and Kumar [27]. This study highlights the importance of checking the trustiest of data security and credibility regarding cloud computing infrastructures. For instance, health sectors depend on the infrastructure aspect indirectly. It was found that improving infrastructure leads to enhancing mobility, and mobility contributes to keeping the security of the health data and detecting the illegal leak of information as fast as possible.

III. METHODOLOGY

A. The aim of the research

The main aim of this research is to investigate the challenges regarding security in the cloud computing field. Hence, this research provides a full detailed review of the issues which commonly meet the healthcare cloud computing security. In addition, the significant challenges and issues will also be included and discussed based on the level of the security of ensuring trust data and the compliance concerns through several related works, which is twenty.

B. Research Questions

- How the cloud computing of healthcare can be protected these days?
- What are the main critical security concerns that are commonly faced in the cloud computing of healthcare?
- How to ensure the trustiest of data security and regarding the infrastructures of cloud computing?

C. *Data collection process*

In this step, several relevant sources will be analysed. The content of these studies must correspond to this study's selected topic, which security challenges in healthcare cloud is computing. The primary purpose of this step is to organize the selected related studies in order to facilitate the data analysis process. This will be done by determining the link between each study and the previous research questions to reach beneficial results. Furthermore, the process of sources collection started by identifying a suitable related keyword: healthcare cloud computing, security of healthcare information, healthcare infrastructure, as well as cloud computing challenges. The included related studies that will be analysed in this study have been conducted between 2013 and 2021. Figure 3 shows the framework of the study sources selection.

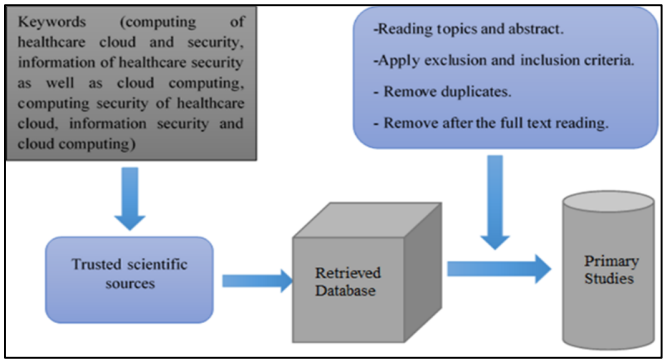

Figure 3: The study sources selection.

IV. RESULTS AND DISCUSSIONS

Twenty resources between 2013 and 2021 were reviewed and compared to obtain adequate answers to the study's questions and achieve the aim of this study. The main results of the resources and their relationship to the study questions are summarized in Table 1.

Table 1: A comparison between the reviewed studies.

Author/s	Results	Related Results		
		Q1	Q2	Q3
Mehran et al. (2017)	The results of this study show measures to improve security and data protection in cloud computing.	✓		
Mohiuddin and Almogren [9]	A system was developed to improve security in cloud computing.		✓	
Faridi et al. [10]	The difficulty of saving data in cloud computing systems.		✓	
Salehi et al. [11]	the infrastructures can enhance the security of the data in cloud computing systems			✓
Prathap [12]	several requirements must be incorporated to over clouding computing challenges in health care facilities	✓		
Al-Marsy [13]	There are some disadvantages and challenges, such as the high required cost for achieving the required security for transmitting the data.	✓		
Khan, [16]	This technology suffers from many securities challenges.		✓	
Al-Issa [17]	Some weakness regarding cloud security is deemed one of the most critical issues hindering a complete diffusion for the cloud in the healthcare industry.		✓	
Rath [18]	A particular downside in cloud computing is observed that is regarding the security perspective.	✓		
Kaur [19]	The challenges can be overcome if an expert correctly deals with them.		✓	
Chauhan & Kumar [20]	Although cloud computing systems have various advantages when used in health care facilities, they suffer from several issues, such as the difficulty of maintaining the patient's data security.			✓
Kamora, & Altamimi, 2018	a creation that contains the methods used to secure health records is implemented in this research.	✓		
Chenthara et al. [14]	The privacy and security of data can be obtained by identified carefully studied procedures in intelligent healthcare solutions.		✓	
Dang et al. [22]	The adoption of fuzzy computing in healthcare applications were discussed, and it was found to be the most suitable for such intelligent applications.	✓		
Shabbir et al. [23]	It was found that the proposed model in this study is better than the traditional algorithms.	✓		
Darwish et al. [24]	This paper provided a comprehensive review of the systems used in the treatment of health care.	✓		
Al Nuaimi et al. [25]	In this research paper, technical problems are discussed in order to find solutions in cloud computing.		✓	
Bharati et al. [26]	this study provides an analysis of some current limitations in cloud computing systems.		✓	
Griebel et al. [15]	Developing new laws that help control the new cloud computing system.	✓		
Malik and Kumar, [27]	It was found that improving infrastructure leads to enhancing mobility, and mobility contributes to keeping the security of the health data and detecting the illegal leak of information as fast as possible.			✓

After collecting the results of the research resources, they were analyzed in order to reach comprehensive answers to the study questions that were previously identified in the methodology chapter. Based on the reviewed studies that were organized and analyzed in this paper, it was found that a relatively large number (8 studies) of the analyzed studies that have been conducted between 2015 and 2021 discussed the critical security concerns and challenges that are

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.96

commonly faced in the cloud computing of healthcare. Therefore, it was observed that there are several security concerns, which are commonly faced in the cloud computing of healthcare since the data can be vulnerable to threaten, vandalism, or can be obtained by untrusted people. Also, another problem related to the cloud computing of healthcare is the publication of sensitive information by the vandals. Moreover, there is another challenge of using the cloud computing of health care related to financial issues. Achieving a high-security level for data transmission and keeping it safe requires a high cost. Besides, other challenges facing the application of the cloud computing of healthcare are legal amenabilities, lack of control, trust, consistency, and quality, besides the asset issues, data sharing, availability, secrecy and recovery, geographical data location, as well as unauthorized data access. The second aspect that has been studied was regarding the methods and measurements of protecting the cloud computing of healthcare; it was found that there were nine studies (between 2017 and 2021) that discussed this aspect, which provides evidence regarding the importance of studying this topic. Based on reviewed studies, it was found that despite the many benefits of the electronic cloud, the security threats it faces may negatively affect data privacy, so it is necessary to protect and provide security for healthcare data within the cloud. Therefore, there are many privacy and security measurements in electronic health care systems, as follows including:

- Data integrity - This ensures that unauthorised persons can make no changes to patients' health information.
- Data encryption- is the most secure approach in order to maintain the confidentiality of sensitive data and to ensure that only authorized persons have access to it.
- Ensuring data reliability - This grants the authorized authority access to patients' healthcare data.
- Auditing - This ensures the protection of health data by monitoring it by tracking activity logs.

The complete comprehension and efficient implementation of healthcare cloud computing dependent issues and data protection are vital to increasing security.

The last aspect reviewed is about the impact of cloud computing infrastructures on data security insurance. Based on Table 1, three studies ranged between 2013 and 2021 have investigated this aspect; the results showed that there is a relationship between the infrastructures and ensuring of the trustiest for the data security and credibility. For example, the infrastructures can enhance the security of the data if the implementation process is carried out by a professional team that does not leave any loophole within the implemented network. Furthermore, infrastructures contribute to achieving the trustiest of data security if implemented based on the engineering standards the wrong way. Moreover, improving infrastructure leads to enhancing mobility, and mobility contributes to keeping the security of the health data and detecting the illegal leak of information as fast as possible.

V. CONCLUSION

The security concern has been the most significant impediment to cloud computing adoption. Major problems regarding healthcare cloud computing include access control and identity management of virtual cloud environments, cybercriminals, Internet-based access, authorization, and authentication.

This study has been conducted in order to determine and examine the challenges and risks of health care data cloud computing and how to overcome them; Also, the relationship between the trustiest of data security and the cloud computing infrastructures was explored. This was done through a review of 20 studies about cloud computing security, which were analysed, and determined their compatibility with the study's questions; after that, the related helpful information has been extracted, then this information and results were discussed. The results showed that the significant security challenges included in healthcare cloud computing are that data can be treated, vandalism, or can be obtained by untrusted people. Another problem is the publication of sensitive healthcare information by the vandals, besides the financial issues. Furthermore, there are many privacy and security measurements in cloud computing systems, including data integrity, data encryption, ensuring data reliability, and auditing. In addition, it was concluded that the infrastructure of cloud computing systems plays a significant role in enhancing data security if it was carried out by profession based on the engineering standards wrong way. In general, this study provided a comprehensive review of the most prominent problems facing cloud computing of healthcare data as well as some valuable solutions to these problems.

REFERENCES

[1] H. Löhr, H. Görtz, A. Sadeghi, Horst. G, and M. Winandy. Securing the E-health cloud.

[2] Mehraeen, E., Ghazisaeedi, M., Farzi, J., & Mirshekari, S. (2017). Security challenges in healthcare cloud computing: a systematic. Glob. J. Health Sci, 9(3).

[3] E. Chikhaoui, J. Sarabdeen and R. Parveen. Privacy and Security Issues in the Use of Clouds in e-Health in the Kingdom of Saudi Arabia. 2017.

[4] L. Barthelus, Northern Virginia Community College. Adopting cloud computing within the healthcare industry: opportunity or risk? Volume 4, Issue 1, 2016.

[5] J. Hurwitz, R. Bloor, M. Kaufman and F. Halper, Cloud computing for dummies, Wiley Publishing, Inc., Indianapolis, Indiana, 2010.

[6] G. Reese, ―Cloud Application Architectures, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2009.

[7] K, Chamandeep, H. Mourad, and S. Banu. "Security and Challenges using Clouds Computing in Healthcare Management System." (2019).
[8] N.S., Safa, Information security conscious care behaviour formation in organizations. Computer & Security, 2015.05.012
[9] Mohiuddin, I., & Almogren, A. (2020, April). Security Challenges and Strategies for the IoT in Cloud Computing. In 2020 11th International Conference on Information and Communication Systems (ICICS) (pp. 367-372). IEEE.
[10] Faridi, F., Sarwar, H., Ahtisham, M., & Jamal, K. (2021). Cloud computing approaches in health care. Materials Today: Proceedings.
[11] Salehi, A. W., Noori, F., & Saboori, R. (2019). Cloud Computing Security Challenges and its Potential Solution. *American Journal of Engineering Research*, *8*(10), 165-175.
[12] Prathap, R., & Mohanasundaram, R. (2021). A study of security challenges from a federated cloud perspective. In Impacts and Challenges of Cloud Business Intelligence (pp. 182-193). IGI Global.
[13] Al-Marsy, A., Chaudhary, P., & Rodger, J. A. (2021). A Model for Examining Challenges and Opportunities in Use of Cloud Computing for Health Information Systems. Applied System Innovation, 4(1), 15.
[14] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE Access, 7, 74361-74382.
[15] Griebel, L., Prokosch, H. U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., ... & Sedlmayr, M. (2015). A scoping review of cloud computing in healthcare. *BMC medical informatics and decision making*, *15*(1), 1-16.
[16] Khan, A. W., Khan, M. U., Khan, J. A., Ahmad, A., Khan, K., Zamir, M., … Ijaz, M. F. (2021). Analyzing and Evaluating Critical Challenges and Practices for Software Vendor Organizations to Secure Big Data on Cloud Computing: An AHP-Based Systematic Approach. IEEE Access, 9, 107309–107332.
[17] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: a survey. Journal of healthcare engineering, 2019.
[18] Rath, M. (2019). Security challenges and resolution in cloud computing and cloud of things. In Applying Integration Techniques and Methods in Distributed Systems and Technologies (pp. 79-102). IGI Global.
[19] Kaur, C., Mourad, H. M., & Banu, S. S. (2019). Security and Challenges using Clouds Computing in Healthcare Management System.
[20] Chauhan, R., & Kumar, A. (2013, November). Cloud computing for improved healthcare: Techniques, potential and challenges. In 2013 E-Health and Bioengineering Conference (EHB) (pp. 1-4). IEEE.
[21] Kamoona, M. A., & Altamimi, A. M. (2018, July). Cloud E-health Systems: A Survey on Security Challenges and Solutions. In 2018 8th International Conference on Computer Science and Information Technology (CSIT) (pp. 189-194). IEEE.
[22] Dang, L. M., Piran, M., Han, D., Min, K., & Moon, H. (2019). A survey on Internet of things and cloud computing for healthcare. Electronics, 8(7), 768.
[23] Shabbir, M., Shabbir, A., Iwendi, C., Javed, A. R., Rizwan, M., Herencsar, N., & Lin, J. C. W. (2021). Enhancing security of health information using modular encryption standard in mobile cloud computing. IEEE Access, 9, 8820-8834.
[24] Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K., & Muhammad, K. (2019). The impact of the hybrid platform of Internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. Journal of Ambient Intelligence and Humanized Computing, 10(10), 4151-4166.
[25] Al Nuaimi, N., AlShamsi, A., Mohamed, N., & Al-Jaroodi, J. (2015, March). e-Health cloud implementation issues and efforts. In 2015 International Conference on Industrial Engineering and Operations Management (IEOM) (pp. 1-10). IEEE.
[26] Bharati, S., Podder, P., Mondal, M. R. H., & Paul, P. K. (2021). Applications and Challenges of Cloud Integrated IoMT. In Cognitive Internet of Medical Things for Smart Healthcare (pp. 67-85). Springer, Cham.
[27] Malik, J., & Kumar, S. (2021). A Novel Consumer-Oriented Trust Model in E-Commerce. Smart and Sustainable Intelligent Systems, 413-425.

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.96