https://doi.org/10.48009/1_iis_2020_227-238
Issues in Information Systems
Volume 21, Issue 1, pp. 227-238, 2020

DIGITAL HEALTH: DATA PRIVACY AND SECURITY WITH CLOUD COMPUTING

Akshay Mittal, University of the Cumberlands, amittal3061@ucumberlands.edu

ABSTRACT

Digital health is the convergence of digital technology in healthcare. The emerging technology and the use of changes are needed in healthcare for advancements and better outcomes. With the use of new innovations, new threats and challenges are emerging in the industry, which needs to be managed for efficient operations. The paper talks about the rising demand for integrating data with highly enabled technologies in the field of medical, biomedical, and healthcare. The availability of data at the central location of any Medical or healthcare organization would primarily serve the major concern of data availability with security. At the same time, the data is being treated in terms of data security and healthcare privacy as the key to improving issues related to the same and also to gain insights and lower the costs. This paper aims to present the digital healthcare and privacy that applies to the healthcare industry and also to discuss the advancements that are being implemented in digital health, the challenges they face with the data while shifting it, and moreover concerned with data breaches and privacy. The paper includes the detailed findings of the technology being used to store data that is called cloud computing. It allows accessing a lot of data with easier handling techniques and lets consumer use their files without downloading them. This makes the management easier, and it needs less maintenance and saves costs. Primarily the concern is over data privacy and security, which is maintained as per government rules and regulations. Additionally, the implementation of the health insurance portability and accountability act (HIPPA) stays accountable for managing data privacy and protection of the digital data.

Keywords*:* Digital Health, Healthcare, Data Privacy in Healthcare, Cloud Computing, Data Security in Healthcare, and Cloud Computing.

INTRODUCTION

The information technology and their advancements are being implemented in digital health to provide better facilities. Organizations in the healthcare industry shift their data on clouds with cloud computing and making it central to obtain flexibility and easy access to data. They face various challenges while shifting the data to clouds and even after. The data with cloud computing is open to vulnerabilities and needs to be secured. The digital health is concerned about data breaches and data privacy. Cloud computing and cloudlets are technological advancements, implementation of which have become a necessity and not an option for healthcare organizations (Jonah, 2018). Two of the major issues facing healthcare data security include user errors in the adoption of technology and lack of awareness in capturing and storing data. Most medical practitioners rarely think about the capture of digital data because their main duty is to offer medical care to patients. Additionally, some patients may not be as cautious as their healthcare providers when handling data because they are oblivious to the threat of cybercrime (Bartoletti, 2019).

The future healthcare industry will be information-centric that allows us to manage complexities. With cloud computing, electronic health records (EHRs) are maintained. These records need to be protected. Unauthorized access, data theft, data manipulation, phishing, and denial-of-service (DoS) attacks are the emerging threats of digital health with respect to cloud computing (Maria, 2019). The confidential data can be protected by securing the system with authentication and authorization tools, transmitting the data in encryption form, and using the trusted cloud computing service providers (Lustgarten, Garrison, Sinnard & Flynn, 2020). Basically, this article is all about healthcare that can be merged with digitalization managed through the integration of various advanced technologies like cloud computing that may help to overcome the issues related to security and the privacy of data at healthcare centers. This article states the explanation regarding the idea behind digital healthcare in the medical industry. The use of technology like cloud computing helps to manage huge data easily and also segregates it as per the organization's use. The data privacy and security of the patient can also be tackled as per government rules and measures. This paper will first give a background on the healthcare sector in regard to digital advancement and then review the literature on the challenges,

management issues, and statistics on digital data in the healthcare industry. Additionally, the paper will discuss the privacy and security of digital health and present the findings on the review of the literature.

BACKGROUND

The healthcare industry is converging with digital technologies to increase the efficiency in their practices and make medicine personalized to deliver quality healthcare (Duggal, Brindle & Bagenal, 2018). The reason behind the growing demand for diverse medical care and additional resources is the dramatic increase in average life expectancy. Healthcare moved to cloud computing as it started generating a significantly high amount of data on a regular basis. The data generated by the healthcare industry is important and needs to be preserved for decision making and to provide good quality services for patients (Hathaliya & Tanwar, 2020). The implementation of cloud computing is cost-effective, minimizes operation cost, and facilitates real-time data collection, data storage, and transmission of data. It forces healthcare to shift the operations to the cloud and implement cloud computing services in their organizations. A large number of data can be exchanged by the healthcare organization in a secure and efficient manner when the concept of cloud computing is used (Aziz, 2016). While healthcare providers may be cautious during the exchange of data, patients may be prone to errors, thus exposing their data to malicious hackers. For instance, when accessing their lab work from the provider's portal, the patient's medical privacy is in his or her hands meaning that if they store or send the data in an unencrypted format, then it may be subject to unauthorized access by hackers (Beaulieu-Jone et al., 2019).

The global challenges of cloud computing can be addressed with innovations and technologies assisting the organization (Ahmed & Rajput, 2020). The patients' personal information like name, address, and contact details along with their medical history is stored with healthcare organizations that are confidential and critical that needs to be preserved and secured. Privacy and security are the major concern of healthcare in implementing cloud computing services. Cloud computing infrastructure can be used in a healthcare organization through electronic health records (EHR) (Doman, 2020*)*. In this process, the healthcare data is shifted from traditional paper-based records to electronic records via EHR and is stored on networks allowing remote access. However, the shift to EHR comes with a risk because there are several touchpoints where unstructured data arise, and certain medical workers may not be familiar with capturing and storing such data since their main duty, as taught in school, is to care for the patients. When frontline clinicians fail to think about where their data is stored, the IT department generally has a hard time keeping data safe (Beaulieu-Jone et al., 2019). As the volume of data grows, the cost and impact of on-premise data centers may overwhelm most IT departments. For instance, wearable health monitors produce unstructured data such as steps taken, breathing, and body movements, among others, and should be managed well to plan for the patients' recovery (Price & Cohen, 2019).

In order to serve medical and healthcare management access to the data from different resources that are readily available via cloud computing, IBM and active healthcare management developed a new clinical information management system to offer a practical solution called 'Collaborative Care Solution' in 2010. This system can be used by organizations to access records remotely. Cloud computing in healthcare is a new concept, and the use of innovation and technology in this field could give rise to emerging threats and challenges. Traditionally data was stored on a physical system giving access only to the particular organization in a particular location to enhance the services. There was thus a need to shift the data to a more flexible system for enhancing the services. Healthcare organizations decided to opt for digital health and cloud computing, and its implementation provides flexibility in managing, accessing, and transferring data on clouds in cloud computing (Semantha, Azam, Yeo & Shanmugam, 2020). The information of healthcare contains critical data of patients, including name, address, and medical history, which need to be secured. Cloud computing manages the privacy and security of the data with authentication and authorization tools. The cloud computing service provider's history must be considered before choosing the right service provider as the organization's complete data is exposed to the service providers and increase the chance of a data breach. Privacy can be lost by placing the data in cloud computing due to less security. Thus, the implementation models must be able to identify the threats to the system and the attacks (Lina, 2016).

LITERATURE REVIEW

Devi & Manju (2014), in their paperwork, proposed a novel framework that can recognize patient-centric privacy for personal health records in cloud computing. In this process of recognition, the patients were asked to encrypt the data by themselves with the help of encryption tools and attributes. The encryption used in the process of recognition was

double encryption mentioned where the first encryption is done by the CSP. Multiple EHR owners and users came together to design a framework that could address the challenges to reduce the complexity of key management in case of an increased number of users in healthcare organizations. There was a complexity in key management in the framework, but the advantage was that it automatically encrypts or decrypts the data, and then it is stored in the system (Devi & Manju, 2014).

Divya (2016) proposed a system to improve the efficiency of the treatment of patients by providing an environment where the patients' records are stored to be referenced by the doctors. This system was designed to handle the medical history of individuals across the country by storing their records in one place. These records can be accessed by all the registered hospitals with the patients' consent. The requirement to obtain access to this database is the hospital license and registry for ease. The license is required as the organization needs to provide a unique access code for the database. The database system stored the data of the patients under their personalized number when the data was first entered. With this system implementation, the patients will not have to carry their past medical history records along with them while visiting another doctor since it will already be available on the system through their unique ID. In addition, the data will also be available for the users to read and view. Data confidentiality and privacy can be achieved with high efficiency. Various kinds of malware attacks can be reduced by an efficient access control system. The only drawback found in this system was a slow adoption of cloud computing. All the other systems were performing well in terms of storage, computation, and communication overhead (Divya, 2016).

Kingsford (2017) proposed that access to the organizations' data, growth, and increase in research and development is due to the implementation of big data. With this advancement in information technology, the industry gained popularity, efficiency, and accuracy. The main concern for healthcare organizations is about the security of the readily available data stored on their EHR, the access of which is provided to doctors' patients, researchers, and data scientists by moving the data on clouds. This easy access is a threat to the privacy and confidentiality of the patient's data. The authors solve emerging threats by using different frameworks, guidance, laws, and regulations. The disadvantage of this system is that the relation of big data privacy and data privacy is at high risk in healthcare (Kingsford, 2017).

According to Medhekar & Nguyen (2020), the significant rise in the use of EHR and other healthcare technology has to the abundance of data and information that malicious hackers target. The modern world is characterized by BYOD (bring your own device) whereby patients and medical workers come to the medical institution with their own mobile devices leading to the rise of several instances of unstructured data. Patients are now choosing to leave healthcare providers who fail to protect their data, thus costing a significant portion of their revenue. Liebler & McConnell (2020) report that Accenture, which is a Fortune 500 company providing technology, business, and management consulting, claims that 25 percent of patients were affected by breaches in healthcare provider data between 2015 and 2019. Accenture reports that over 6 million people will thus be victims of medical identity theft, and 4 million of them will be forced to pay for the damage out of their pockets (Liebler & McConnell, 2020).

Glasper (2019) claims that big tech companies such as Apple, IBM, and Amazon have started entering the medical space and partnering with healthcare providers to offer medical solutions for the modern patient. Even as the big tech names enter the medical scene, there is still a trust deficit because fewer patients are willing to share their data and personally identifiable information with medical institutions. According to Rock Health's 2018 National Consumer Health Survey, only 11 percent of respondents reported willingness to share their health data with the tech companies. As we progress into the digital world and as tech behemoths like Apple partner with medical health providers, there is a great need for all entities involved to uphold their responsibilities, follow the relevant laws and regulations, and maintain trust of the patients to quell the privacy concerns of the patients (Glasper, 2019).

According to Banerjee, Hemphill & Longstreet (2018), to realize the promise of digital health, corporations that partner with healthcare providers need to ensure that their patients' data is safe, secure, and free of error. Beyond the promise of security, healthcare organizations also have to maintain the confidentiality and privacy of their patients' data. There is a baseline expectation from the patients and even the workers concerning the health plans when working with digital health corporations (Banerjee, Hemphill & Longstreet, 2018). Therefore, the success of digital health corporations will hinge n whether the patients feel comfortable enough to share their personally identifiable information and personal health data that can possibly affect their employment.

PRIVACY AND SECURITY OF DIGITAL HEALTH

Digital health is the technique of using digital and information technologies in the healthcare organization to enhance the quality of the services. The research is focused on cloud computing and emerging threats due to the implementation of cloud computing in healthcare organizations. Organizations have implemented cloud computing for processing data. EHR used by organizations transfers data on clouds in encrypted form so that the individuals can access the data remotely. The implementation of cloud computing can be understood by the cloud computing architecture.

Cloud computing is a technology that uses internet and remote servers to store data and allow consumers to use the stored data and applications via internet access without downloading the files on remote computers. The growth of cloud computing is due to the efficiency in computing by a centralized server used to store and process data. It uses three different models that can be used as per the need. The use of cloud computing not only speeds up operations with easy management but also requires less maintenance and is cost-efficient. It brings attractive benefits like remote storage, flexible on-demand access, universal data access, storage management, and avoiding extra capital expenses. It does not need any special hardware or software for its implementation and maintenance (Arunkumar, 2017).

The cloud computing architecture is basically divided into two parts the front end and the backend. The client's computer and the applications that allow the users to perform the operations on clouds come under the front-end. The backend of the cloud computing architecture comprises of servers, data storage systems like EHR, and various other systems. This architecture of cloud computing allows any type of programs and applications to be stored on clouds. Also, there is a central server administration system to monitor the smooth functioning of applications on cloud computing and the flow of data under a set of rules and protocols that differ with countries and governments. Server virtualization is used to minimize the need for additional physical machines by fooling the physical server (Arunkumar, 2017).

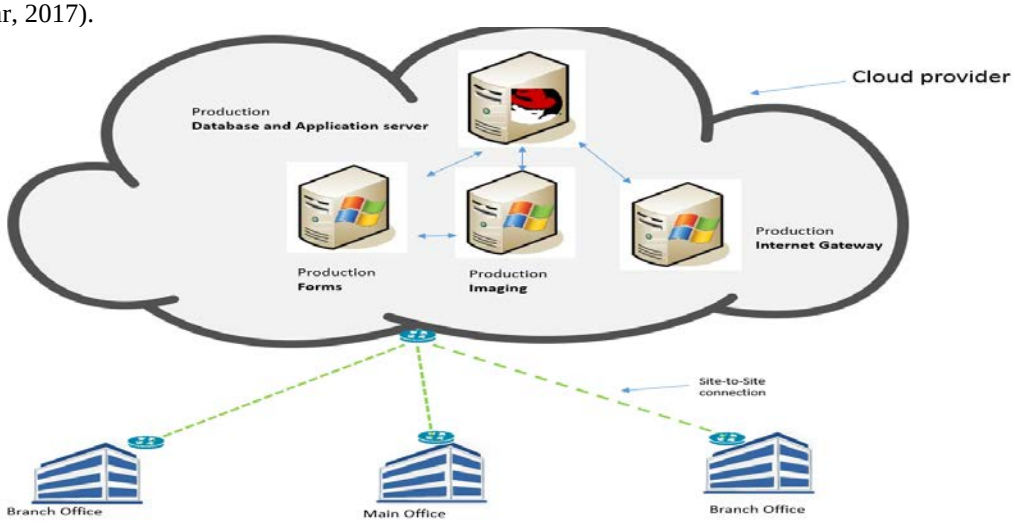

Figure 1. Cloud Computing Architecture (Arunkumar, 2017)

The security and privacy in healthcare are maintained by high-security measures, government regulations, and rules, and comply with legislation to ensure the patients' data protection. The health insurance portability and accountability act (HIPPA) was implemented to manage the privacy and security of patient's data. This law was made even before the implementation of cloud computing in healthcare and even before the digital health. Under HIPPA, the patient's information can't be used for research or any other purpose without patients' consent and authorization (Aziz, 2016).

The digital health service providers come with built-in security measures in EHR. This ensures a safe environment for creating, storing, processing, communicating, and managing the patient's data. It is the responsibility of healthcare to educate consumers about their role in security. Role-based access can also be provided to the patients. EHR uses different encryption techniques with one key for encrypting the data while transmitting. The organizations with huge data use the PKI as it is one of the expensive encryption forms. The small organizations use user-based, and role-

based access to handle the data securely. This method can be used for reasonable performance and small storage (Aziz, 2016).

The digital health includes tools to manage and monitor access in the system by creating logs. This system helps to prevent the system from a data breach. In the case of a data breach, the attacker can find out by investigating the system logs. The authorization and authentication tools like facial recognition and digital signature are used for the safety and security of the patient's data. Proper flow of information and effective communication is required in any healthcare organization as it is a matter of health. The administration and the medical staff must be linked, and a way of communication must be fixed to ensure the proper flow of data. Thus, EHR is maintained, which is accessed and managed by both. This information is made available for enhancing the services and increasing the accuracy. The laws for security and the privacy of data are different for different countries.

Given below are a few examples of the laws and enactments implemented in different countries:

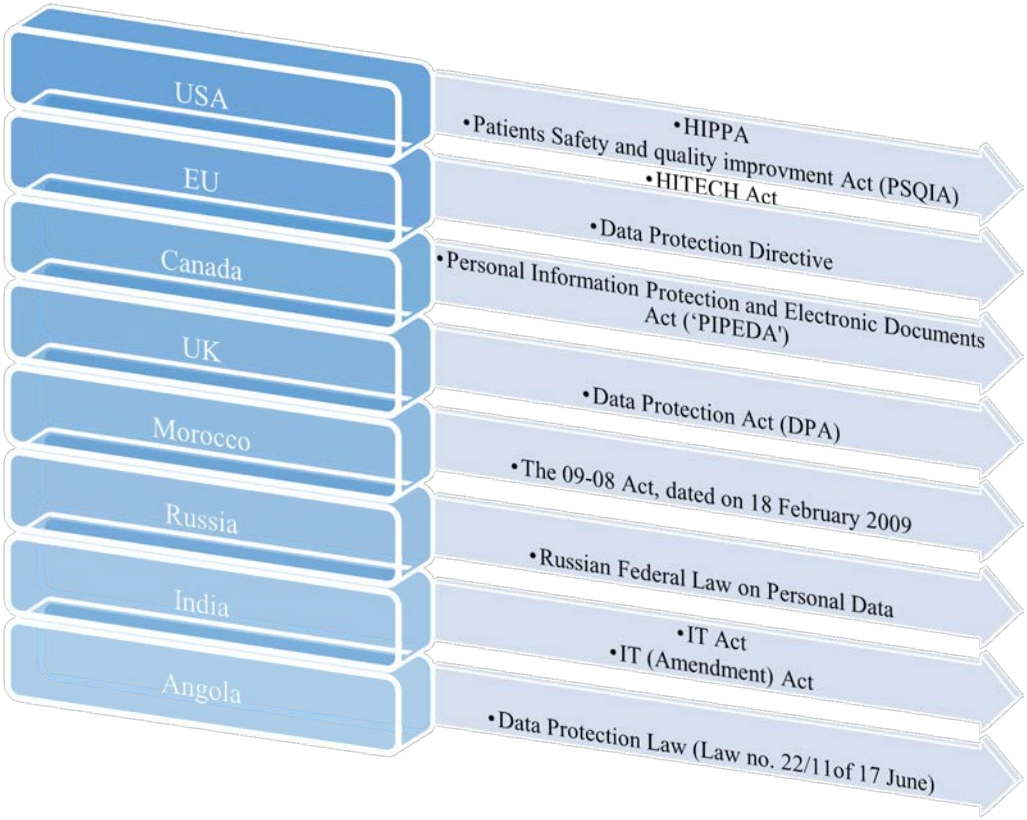

Figure 2. Laws and Enactments of Different Countries (Joni, 2020)

RESEARCH METHODOLOGY

Introduction

The research study was purely qualitative and aimed at exploring and presenting digital healthcare and the privacy that applies to the healthcare industry and discussing the advancements that are being implemented in digital health, the challenges faced, data breaches and privacy concerns. The research methodology thus entailed a deep review of literature mapping and evaluating the body of literature to identify the challenges faced in the provision of confidentiality and the privacy of patient's data and the advancements that have been made in healthcare provision to keep patients' data safe. The review of the literature was possible through an iterative keyword search that yielded sources to be used for writing the results section. Snyder (2019) recommends the literature review as a research

methodology given the explosion of knowledge and information in the field of business research. This paper follows the guidelines that Snyder offers to conduct and write a good literature review paper.

Steps of Methodology

The first step in the methodology section involved the identification of suitable keywords that would be input in databases to identify suitable sources for the study. It follows that the second step of the methodology section was inputting the keywords and selecting the best sources for use. The researcher then modified the keywords to select the best sources for use and remove irrelevant ones. The third step was thus the manual refinement and modification of the results to select the best sources for use.

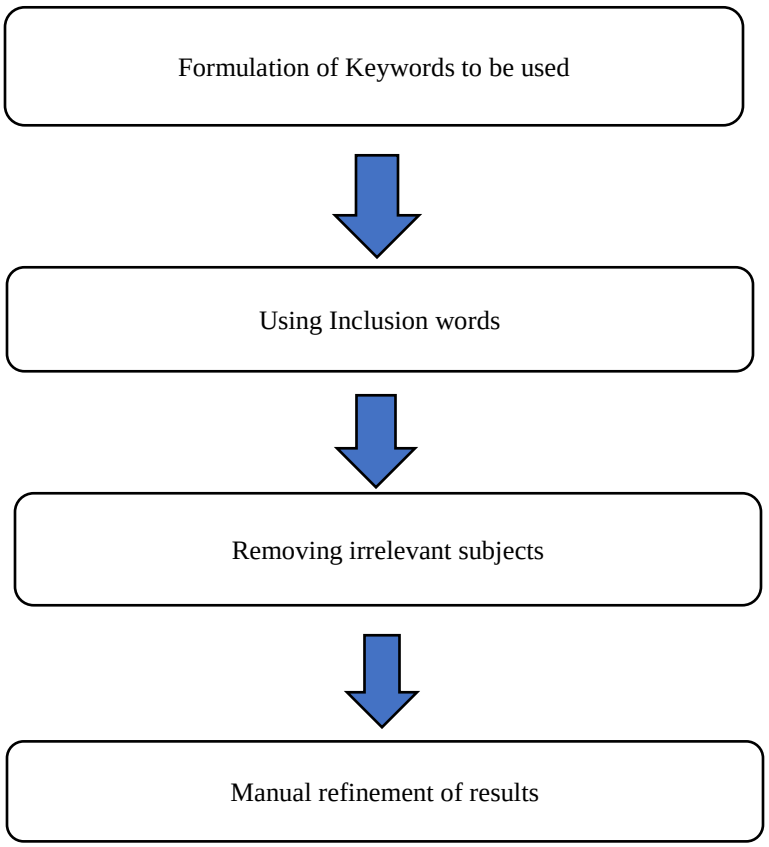

Chart 1. The Steps of The Methodology

The keywords that were used in the first step include ‘digital healthcare and privacy’, ‘advancements in healthcare delivery privacy and confidentiality of data’, ‘instances of data breaches in the healthcare industry’, ‘challenges in maintaining confidentiality and privacy of patient data in healthcare sector’, and ‘measures for ensuring healthcare privacy and confidentiality’. The databases and online libraries that were used for finding the sources include SAGE Journals, Google Scholar, and EBSCO Host. The researcher only needed peer-reviewed sources to be used for the review.

The researcher then used conjunctions like ‘AND’ and ‘OR’ to combine the keywords in unique words to yield search results that were more specific for the study. ‘AND’ and ‘OR’ are inclusion words that helped to widen the scope of the search results. The researcher shifted between the different online libraries and databases. The researcher then selected the best 20 sources to be used for the study.

Table 1. The steps of obtaining sources for the study

Steps	Search Keywords	Average Search Results
Step 1	1. Digital healthcare and privacy 2. Advancements in healthcare delivery privacy and confidentiality of data 3. Instances of data breaches in the healthcare industry 4. Challenges in maintaining confidentiality and privacy of patient data in the health care sector	40, 918
Step 2	Inclusion Words: 'AND' and 'OR' Example: Instances of data breaches in the healthcare industry AND challenges in maintaining confidentiality and privacy of patient data in the health care sector	5, 013
Step 3	Removing irrelevant subjects	895
Step 4	Manual Refinement of Search results	47

RESULTS/FINDINGS

It was found that even after considering the benefits of cloud computing, the disadvantages cannot be ignored. The major issue of the shift in the healthcare industry to the cloud computing system is that they experienced great exposure to the outside environment giving rise to security challenges and security threats (Medhekar & Nguyen (2020). The information stored on clouds can be accessed by unauthorized users by hacking the servers. It was challenging for both the users and the cloud computing service providers to protect data privacy. Algorithms were used and proposed for securing the data and overcoming these obstacles. The AES and pailier cryptosystem algorithm, which is a probabilistic asymmetric algorithm for public cryptography was used for storing and transmitting the text and image in the encryption form. Another algorithm that was used was the Homomorphic encryption algorithm that can be defined as a kind of encryption that allows computation on ciphertexts to develop encrypted results after decryption, and it must be exactly the same as of the operations which are performed on the plaintext. This algorithm was used to protect the data from unauthorized access. Based on the healthcare organization and the confidentiality of the data, many algorithms are used for the security of authorized access (Arunkumar, 2017).

Implementation of cloud computing reduced the time, operations cost, and enhanced the delivery of the services with different service models (Hathaliya & Tanwar, 2020). The patient's data can be more secure as the access is provided only via the unique identification number given to the individuals. Also, the hospitals can only access the patient's data stored on the clouds if they have a license and have registered themselves to the database access registrar. The patient's complete medical records are obtained and stored in a uniform manner that reduces the wait time by making the reports available remotely. This results in accuracy in reports and fast delivery. For example, an individual was able to contact a doctor available mile away from his location for the diagnosis and start the treatment all in a duration of a few hours that has saved his life. EHR enables the healthcare organizations and the insurance companies to manage the patient's information and store them securely. The main objective of the organization is obtained to increase the number of services in healthcare, enhancing the quality of services and managing the data efficiently (Hathaliya & Tanwar, 2020).

The implementation of cloud computing also plays an important role in digital health as it removes the geographical barriers providing a system that allows universal access (Medhekar & Nguyen (2020). The doctors, physicians, researchers, and statisticians, all can access the report simultaneously even if they are miles apart to provide a better, secure, and faster service. In the case of the second reference, the patient does not need to personally visit the doctor and take his appointment to review the reports. The doctor needs only the access code from the healthcare organization

or the patient to access the reposts stored on clouds. These services have minimized the risk of false reports, misplacements of reports, change in the patient's reports, or alteration of reports.

The results of this research could be very beneficial as the future healthcare industry will surely overcome all the complexities in EHR by making it flexible and remotely accessible. The EHR will be saved on the cloud by the healthcare organization, and a better EHR would help the patient in an emergency by providing access to the records remotely.

Fig. 3 given below describes the cloud computing usage in medical image display. The cloud computing architecture, which includes the cloud service, the cloud platform, and the cloud storage facilities, is used to store the medical image from the EHR. A web service API is used to transfer the image to the clouds, which can be accessed via an active internet and mobile device. The image is stored in the encrypted form to prevent it from attacks. This is explained in Fig. 4.

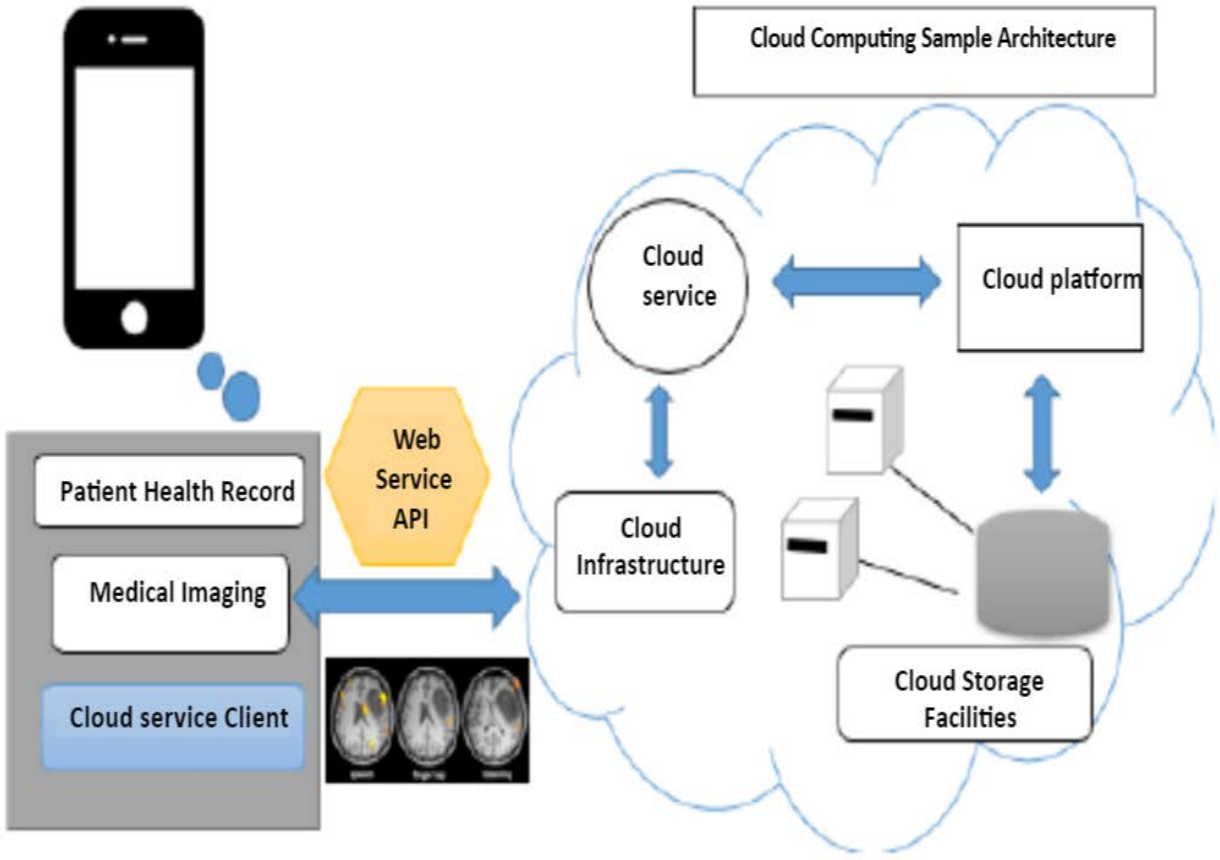

Figure 3. Cloud computing usage in medical image display (Aziz, 2016)

In the Fig. 4 given below, the data stored is in encryption form and different from what it looks in the original EHR. The AES algorithm is applied frequently for encryption, which converts the data into an unreadable form. Based on several permutation and linear transformations, the data is executed on blocks transferring the plain text into encrypted text. This algorithm is used as there are no possible attacks against the AES algorithm. It is also a standard for government standards and a high-security system (Arunkumar, 2017).

Figure 4. Original Health Record VS Encrypted Health Record (Arunkumar, 2017)

LIMITATIONS

This study has several limitations that can be considered as the hurdles of digital health. When considering the safety and security of the patient's data while implementing the cloud computing system in the organizations, the organization's management faces issues like network dependency, security, and privacy; the data becomes vulnerable to attacks, and also at times faces the limitation of control and flexibility. These limitations affect the organizations and must be considered to excel and achieve the aimed objectives of the organization. Key limitations of cloud computing that needs to be considered are:

1. Network Connection Dependency: To gain the total benefits of cloud computing, the system of business must have an internet connection. You cannot neglect this fact. A network is an essential gateway to send or retrieve the files. As in stormy conditions, you may face a problem while transferring the data.
2. Security and privacy of cloud computing: Although the cloud computing service providers enforce the best security standards and industry certification, data storing and important files on external service providers are always opened up to risks. The service must ensure the security and privacy of the data, especially when it is related to manage sensitive data. No doubt, any cloud computing service provider is able to execute and watch over the underlying hardware infrastructure of an organization. However, the responsibility is in the control of user access management, and up to you attentively analyze all the risk scenarios.
3. Vulnerability to attack: In cloud computing, all the components are online, thus it may disclose potential vulnerabilities. No matter how best the team is, even they experience severe attacks or security breaches at regular intervals. Cloud computing was built considering it as a public service. You only need to have a credit card generally to get started with cloud computing.
4. Limited control and flexibility to the cloud: As cloud infrastructure is totally owned, handled, and observed by the service providers. It allows minimum control over to the customer. Cloud computing users may find that they have limitations over the function and to cut off the services within a cloud-hosted infrastructure. The license agreement of a cloud computing provider's end-user management policies has the right to establish the limits on what a customer can do with their organization. The customer may have the authority

of their applications, data, and services, but they do not have an equal level of control as the backend infrastructure.

5. Customer lock-in: Customer lock-in is also known as Vendor lock-in and another recognized limitation of cloud computing. The service that did not yet completely emerge is the easy switching between cloud computing services, and the organization may find it challenging to shift their services from one vendor to another. The difference in the vendor platforms creates difficulty in shifting from one cloud platform to another (Andrew, 2019).
6. One of the biggest limitations of cloud computing in digital health is to handle such a big data flood with intensive security and with highly skilled hands because the risk becomes higher with the ease of technology.
7. Privacy and security of the sensitive data of the patient is an utmost priority and a highly secure connection costs a lot of expense to any healthcare organization.
8. The awareness regarding digital healthcare is low when compared to other technologies.
9. Technological problems can cease the on-going process, which may result in huge problems in times of emergency cases.
10. Minor concerns like power cuts, power outages, loss of internet connectivity resulting in disconnection with the cloud can also occur in such cases.

CONTRIBUTION TO THEORY

This paper contributes to the understanding of how cloud computing can be proofed to circumvent all manner of cyber-attacks that would cause damage to patient data. The paper discusses the challenges in attaining digital privacy and the measures that can be implemented to proof cloud computing, thus protecting patients' data.

CONCLUSION

While challenges such as the threat of malicious hackers gaining access to patient data persist, there are still numerous opportunities for circumventing unauthorized access. The ever-increasing technology with highly enabled data-generating technologies in the field of healthcare and biomedical is the need for any organization as it becomes the biggest support by handling the data flood. Even though the digitalization of the healthcare industry promises to deliver many benefits, on the contrary, it also raises some barriers and challenges. Indeed the question of securing sensitive information is still an ideal thought. Hence the data security and privacy are considered to be a huge barrier in this field. There have been successful works accomplished across the world, but it can be counted on along with the advantages and disadvantages of the technologies in context with the digital health care industry. One example from the various methods used to prevent patient's privacy in healthcare is Attribute-based encryption Access Control, AES, and also Homomorphic encryption. Here on the perspective for the future is to provide effective solutions to the problem in digital health care and data security.

Cloud computing can be used as a personalized network used as per demand. It has the ability to control the resources and provide the services accordingly. The public, private, and hybrid clouds are available in the environment to be used as per the requirement of the organization. The healthcare needs to implement new innovations and technologies to handle the ample of data created by them every day and preserve it securely. Hence cloud computing is the best idea to combine it with the EHR and find a solution to the big data challenges. This implementation can resolve the storage issue, security, privacy, flexibility, reliability, and availability of data between the patients and the healthcare organization. With the web service or API, the medical records are transferred on the clouds using the homomorphic encryption or AES algorithm, which can later be accessed remotely on mobile devices via an active internet connection.

REFERENCES

Ahmed, S. M., & Rajput, A. (2020). Threats to patients' privacy in smart healthcare environment. In *Innovation in Health Informatics* (pp. 375-393). Academic Press.

Andrew, L. (2019). Disadvantages of cloud computing. Retrieved from https://cloudacademy.com/blog/disadvantages-of-cloud-computing/

Arunkumar, R. J. & Anbuselvi. (2017). Enhancement of cloud computing security in health care sector. IJCSMC, Vol. 6, Issue. 8, August 2017, pg.23 – 31. Retrieved from https://www.ijcsmc.com/docs/papers/August2017/V6I8201705.pdf

Aziz H.A, Guled A (2016). Cloud Computing and Healthcare Services. *J Biosens Bioelectron 7: 220.* doi:10.4172/2155-6210.1000220

Banerjee, S., Hemphill, T., & Longstreet, P. (2018). Wearable devices and healthcare: Data sharing and privacy. *The Information Society*, *34*(1), 49-57.

Bartoletti, I. (2019, June). AI in healthcare: Ethical and privacy challenges. In *Conference on Artificial Intelligence in Medicine in Europe* (pp. 7-10). Springer, Cham.

Beaulieu-Jones, B. K., Wu, Z. S., Williams, C., Lee, R., Bhavnani, S. P., Byrd, J. B., & Greene, C. S. (2019). Privacy-preserving generative deep neural networks support clinical data sharing. *Circulation: Cardiovascular Quality and Outcomes*, *12*(7), e005122.

Devi, S. A., & Manju, A. (2014). Enhancing security features in cloud computing for healthcare using cipher and inter cloud. *Int J Res Eng Technol (IJRET)*, *3*(3), 200-203.

Divya, R. & Jangale, S. (2016). Cloud based information security and privacy in healthcare. *International Journal of Computer Applications (0975 – 8887) Volume 150 – No.4, September 2016.*

Doman, M. (2020). Preserving privacy in healthcare data through anonymization.

Duggal, R., Brindle, I., & Bagenal, J. (2018). Digital healthcare: regulating the revolution.

Glasper, A. (2019). A long-term plan for embracing digital healthcare technology. *British Journal of Nursing*, *28*(3), 204-205.

Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, *153*, 311-335.

Jonah, C. (2018). Why healthcare data may be more secure with cloud computing. Retrieved from https://www.mobihealthnews.com/content/why-healthcare-data-may-be-more-secure-cloud-computing

Joni, G. & Murillo, C. S. (2020). Data protection laws of the world. *DLA Piper*. Retrieved from https://www.dlapiperdataprotection.com/index.html?t=law&c=CA

Kingsford, K. M., Fengli, Z., & Komlam, G. (2017). Patient knowledge and data privacy in healthcare records system. *Published in: 2017 2nd International Conference on Communication Systems, Computing and IT Applications (CSCITA).* DOI: 10.1109/CSCITA.2017.8066543

Liebler, J. G., & McConnell, C. R. (2020). *Management principles for health professionals*. Jones & Bartlett Learning.

Lina, A. A., Wa'ed, S. Ahmed, A. (2016). Privacy preserving data mining on published data in healthcare: A survey. *Published in: 2016 7th International Conference on Computer Science and Information Technology (CSIT).* Retrieved from https://ieeexplore.ieee.org/document/7549444?arnumber=7549444

Lustgarten, S. D., Garrison, Y. L., Sinnard, M. T., & Flynn, A. W. (2020). Digital privacy in mental healthcare: current issues and recommendations for technology use. *Current Opinion in Psychology*.

Maria, L. (2019). eHealth cloud security challenges: a survey. Retrieved from https://new.hindawi.com/journals/jhe/2019/7516035/

Medhekar, A., & Nguyen, J. (2020). My Digital Healthcare Record: Innovation, Challenge, and Patient Empowerment. In *Opportunities and Challenges in Digital Healthcare Innovation* (pp. 131-150). IGI Global.

Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature medicine*, *25*(1), 37-43.

Semantha, F. H., Azam, S., Yeo, K. C., & Shanmugam, B. (2020). A Systematic Literature Review on Privacy by Design in the Healthcare Sector. *Electronics*, *9*(3), 452.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333-339.