

## A REVIEW ON CLOUD COMPUTING IN HEALTHCARE SECTORS

Ebtisam Ali Abdullah\*<sup>1</sup>, Anwar Saif ALshamiri\*<sup>2</sup>

\*<sup>1,2</sup>Department of Information Technology, Sana'a University, Yemen

### ABSTRACT

Nowdays, Cloud computing technology is one of the most important trends in information systems (IS). It is an important alternative that ensure high performance data processing, storing and exchange. Cloud computing is a new paradigm in the healthcare field, it facilitates the exchange of electronic medical records in hospitals and clinics as well as a storage and exchange center for medical records. Although there are many publications in the context of cloud computing in the healthcare sectors, there is no systematic review of the classification of current research to date. The purpose of this paper is to conduct a survey on adopting cloud computing in the healthcare sectors. It addresses the different adoption frameworks, case studies, as well as related security and privacy issues adopting cloud computing in the healthcare sectors.

**Keywords:** Cloud Computing, Healthcare, Frameworks, Case Studies, Security, Privacy Issues

### I. INTRODUCTION

organizations by offering a wide range of easily accessible virtual computer resources. Cloud computing also facilitates economic growth by providing cloud computing infrastructure with low investment capital [1]. Cloud computing also offers different advantages such as rapid flexibility, resource pooling, and access to an extensive network . This phenomenon has been developed from the idea of unifying and sharing resources in a central environment. Adopting cloud computing technology will help many organizations gain competitive advantage and become more efficient and productive . [1] Cloud computing in the health sector will provide easy access and storage for the patient's medical record anytime, anywhere, and this will improve the ability of physicians to provide better patient care [2] .

We discuss the different frameworks, case studies, as well as related security and privacy issues to adoption of cloud computing in hospitals. The paper is organized as follows, Section II Frameworks of cloud computing in healthcare, Section III case studies of cloud computing in healthcare, section IV Security and privacy of cloud computing in healthcare.

### II. FRAMEWORKS OF CLOUD COMPUTING IN HEALTHCARE

The work in [3] proposed the secure Health Information Systems ( HIS ) framework based on big data analytics in the mobile cloud computing environment, the framework can provide a high level of interoperability, integration and sharing of Electronic Health Records (HER) among patients , healthcare providers and practitioners.. The big data analytics helps analyze patients' data in order to provide right intervention to the right patient on time .The proposed framework also applies a set of security's constraints and access controls that ensure the confidentiality, integrity and privacy of health data. The main objective of this framework was to introduce a new generation of Electronic Health Records (EHR ) capable of providing low-cost , high-quality health services to patients using a combination of cloud computing , mobile cloud computing and big data.

The researchers in [4] proposed a cloud-based framework for information integration and informatics in health care application. The framework consists of Data Access, Data Analytics, Data Integration, Data Orchestration, Data Storage. The framework will allow the analysis, storage and integration of health care data in cloud. It also helps in rapid interaction between healthcare providers and patients. As well as the development of advanced healthcare application with integrated data in another database. The efficiency of the framework has been clarified with patient records and Health Mapper . The framework developed using the Aneka cloud platform.

The framework introduced in [5] for predicting health shocks based on a wide range of health informatics dataset. The proposed framework was developed using cloud services based on Amazon's web services integrated with geographical information systems (GIS) services to facilitate the collection, indexing and storage of big data, as well as the visualization of data by smart devices to various stakeholders. It will facilitates the collection of population based on the socio-economic level, cultural and geographical criteria of

Pakistan. These big amounts of data can be collected continuously for processing, storage and retrieval on the cloud. Thus, this framework will be able to help in understanding the various criteria such as socio-economic, cultural and environmental, which cause health shocks either directly or indirectly, But the researchers did not expand this study to form the first public available health information tool in Pakistan that can help health professionals and government to form health care policies and reforms

The researchers [6] introduced the cloud-based collaborative media service corresponding framework, where collaborative media are used to access various areas such as education, health care, defence, and other areas. Cloud computing has been used with this framework because of the need for an infrastructure that provides on-demand access to a shared set of computing resources such as networks, servers, stores, services, and applications.

This framework was provided to the cooperative service for effective cooperation between health care professionals and caregivers. This framework was used to detect voice diseases, and with the emergence of multimedia communication techniques such as (voice mail, video conferencing, web conferencing), the doctors, patients and caregivers were able to collaborate with each other. The proposed system is capable of providing adaptive collaborative services based on user's preferences, device's sensors capabilities and processing. The researchers used an external database Massachusetts Eye and Ear Infirmary (MEEI subset) to examine their own approach, giving their proposed framework features of agility, full scalability, flexibility and ubiquity, but their database was not deployed on the Amazon cloud.

The researchers in [7] discussed some of the difficult issues facing traditional healthcare services in Saudi Arabia, such as the complexity of e-health projects, the high cost, the lack of staff 'skills of information and communication technologies and the obstacles to electronic health. Due to, shortage of health professionals, and the increase of chronic diseases such as hypertension, diabetes and heart disease, the researchers presented a strategic framework for cloud computing for decision-making based on a Holistic Approach framework. The framework is comprehensive, and covers five main aspects that are "Organisation, Technology, Environment, Human and Business". There is still a need for further improvements in the near future to cover all factors affecting the adoption of cloud computing in the health sector in Saudi Arabia.

Critical health care patients in remote and rural areas and some urban health facilities do not have the same level of access to intensive specialist support as patients in higher care level urban critical care units (CCUs). The researchers in [8] presented a cloud computing framework for real-time urban, rural and remote service of critical care. Here, the researchers introduced Artemis Cloud, a cloud computing based Data-as-a-Service and Software-as-a-Service approach to provide remote real-time monitoring of patients, as well as support for clinical research. The research proved that support is great possible for patients within critical centers units (CCUs) in those areas, without the immediate need to transfer patients to urban centers. The researcher demonstrated this research through a case study within the neonatal intensive care unit (NICU). For this purpose, they were currently using the Cross Industry Standard Process for Temporal Data Mining (CRISP-TDM) and the Service based Multidimensional Temporal Data Mining (STDMn0) temporal data mining technique to support the clinical research study.

The researchers in [9] proposed a framework that contains the most important security processes associated with cloud computing technology in the health care, such as information security risk assessment, information security risk treatment, information security incident management, the control of outsourcing processes, and requirements management. All of these processes are key to ensuring the security of required information. Because of the limited resources, all an information security management system (ISMS) processes are not recommended to be established. And their interaction at an activity level to ensure an appropriate interaction of the ISMS processes. While not every ISMS process needs the same level of maturity, also an approach should be developed to identify the appropriate level of maturity using a proper maturity level model. So health care organizations have used cloud computing technology and focused on those processes mentioned above, since these processes needed at an adequate level of maturity. However, there is still a need to develop a detailed framework of (ISMS) (input, output, and interfaces) processes, and their interaction at an active level. Since all the processes of SMS do not need the same level of maturity, an approach should be developed to determine the desired level of maturity using a maturity level model.

In the research [10] the authors focused on the development of a new hybrid architectural framework, consisting of three frameworks (hybrid, mobile and multimedia frameworks). The researchers also proposed a novel evaluation model based on an analytical hierarchy process. This model includes criteria from multiple decision makers in the context of health care monitoring applications. Using this assessment they analyzed those frameworks for application in real health care environments. This hybrid framework is built on a mobile multimedia cloud that is cost efficient and scalable. This framework provides a cost efficient monitoring solution for a noncommunicable disease patient. The results of the evaluation attained from the multicriteria decision making (MCDM) technique showed that this framework is the most appropriate framework that can be used to build a health care monitoring system. But prototype of the cloud-centric health care system application was not implemented, and the performance of the proposed framework was not evaluated in terms of cost effectiveness and quality of services guarantee.

The researchers in [11] proposed a cloud-based health monitoring framework to identify speech and face to monitor the health of elderly patients with the help of the cloud. Where video cameras and handheld devices were used to collect the speech side by side with the images of the face and delivered to the cloud server for classification and analysis. In this case, the state of the elderly patient is identified, such as pain tensed, and so forth is recognized from his or her speech and face images. The state of patient recognition system is used to extract the Local features of speech and texture descriptors and fed them into two support vector machines (SVM) classifiers separately. Thereafter, the classifiers' scores are fused using Bayesian sum rule to get the final decision of the patient's condition. The recognized state is later sent to the remote care centre, healthcare professionals and providers for necessary services in order to provide seamless health monitoring. The tests carried out have proved the approach validity and evaluated the suitability of this framework in terms of requirements and accuracy. One of the advantages of this proposed system is that it can achieve greater accuracy more than 95% using five instances of the cloud server, and this server generates the response in three seconds, but there is still a need to consider more user related studies.

### **III. CASE STUDIES OF CLOUD COMPUTING IN HEALTHCARE**

The researchers [12] in introduced a cloud-based health care system. In this system, researchers integrated an informal care system (Microsoft HealthVault). With a formal care system called the Data Capture and Auto Identification Reference (DACAR). The advantages of this integrated system were to provide high levels of privacy and security within the cloud environment, also allowing sharing of both Health records and access rights. The researchers also identified a case study that helped assess and demonstrate the convenience of a cloud-based integrated health care system.

The researchers in [13] introduced the knowledge-as-a-service model, a new model of service in cloud computing technology. This model was designed as a framework for the knowledge cloud system. This system is characterized by facilitating interoperability among members of the knowledge network. The aim of this model was to develop cooperative networks in the medical services industry. This framework was applied in a case study in the field of medical radiotherapy Dynamic treatment service in China.

Researchers in [14] proposed a new solution for hybrid mobile cloud computing for the most effective personal medical monitoring. The researchers studied a case to demonstrate the efficacy and effectiveness of the proposed approach (mobile-cloud based electrocardiograph) by monitoring, analyzing and develop a mobile-cloud prototype.

The advantages of the proposed system, as shown by the results, are that the system significantly improves conventional mobile-based medical monitoring in terms monitoring, in terms of accuracy of diagnosis, energy efficiency and efficiency of implementation, and holds the potential in addressing future large-scale data analysis in personalized healthcare .

The researchers [15] discussed the strategic value of applying cloud computing solutions in the Saudi hospital based on The Balanced Scorecard(BSC) approach .In this research, the researchers presented the strategic map as well as the Key Performance Indicators( KPIs )used by the Saudi hospital. The expected results of this research were the possibility that the KPIs and strategy map were used by the Electronic Health Department (EHD).

#### IV. SECURITY AND PRIVACY

The researchers in [16] discussed the concepts related to EHR sharing and integration in clouds of healthcare and analyze the arising security and privacy issues in management and access to EHRs. The researchers provided an EHR security reference model for managing security issues in healthcare clouds, for protecting, accessing and sharing electronic medical records through a use-case scenario. As well as a description of corresponding security countermeasures and possible security techniques that can be applied as a primary guard of security.

The researchers [17] presented a study on the security issues included in data sharing and storage within the cloud. They also analyzed various security issues. The exchange of cloud-based medical images has unique features security and privacy, and challenges such as data security, privacy and recovery as well as legal issues such as regulatory compliance and auditing and key research areas such as the clients store their health data on the server without themselves possessing a copy of it. The researchers discussed solutions to these issues, such as ensuring the integrity of medical data in case the server is not fully trustworthy. Thus, will the encryption solve the problem of confidentiality of sensitive data?, and how it will effect the encryption on dynamic data operations such as query, modification, insertion, and deletion? Also, because medical data will be in the cloud in an environment along with other client data so data should be separated. Privacy preserving and data anonymization techniques will increasingly assume greater importance in cloud based medical image exchange and more main stream research are required in this area.

The researchers [18] suggested management system data health care based on the cloud(BAMHealthCloud), this model has two different parts, the first part takes care of the management side of huge data that are its establishment on a daily basis, and other part takes care of the security, and thus ensures that this work of safe access to the data Electronic Medical through behavioral biometric signature-based authentication, which guarantees the provision of a safe medical records in the system management health care.

The researchers in [19] suggested home healthcare system based on cloud computing, They introduced several use cases and draws an architecture based on the cloud to deal with the challenges of security and privacy. Researchers described a comprehensive methodology to integrate security and privacy engineering process into the software development lifecycle of the proposed system. Researchers then sketched out a plan of a functional infrastructure in order to integrate the proposed home healthcare application architecture into a commodity cloud. They also discussed the mitigation solution with a focus on facilitating patient- and data-centric protection for electronic health data, and highlighted its main components that allow patients to encrypt their own (health or physical activity) data prior to uploading the data to the cloud.

The researchers in [20] presented a review of the risks of hosting an E-health records(EHRs) on a third-party cloud service providers, to protect the confidentiality of patient information, facilitating process, and security issues that cloud service providers should address in their platforms. The results of this study indicate some of the security problems that must be seen by both cloud service providers and their healthcare customers in health care, such as, network security mechanisms, roles based access, digital signatures, data encryption, and access monitoring. To guarantee the safety of the information and adherence to privacy policies, the cloud provider must comply with different security management certifications. The researchers concluded that storing the sensitive information of the electronic health record should take precautions to ensure the safety and confidentiality of the data. A relationship built on trust with the Cloud service provider is essential to ensure a transparent process. Cloud service providers must ensure that all security mechanisms are in place to avoid unauthorized access and data breaches. Patients should be kept informed of how to manage their data.

The researchers in [21] suggested the using of Ciphertext-Policy Attribute-Based Encryption (CPABE) to encrypt an electronic health records(EHRs) based on the attributes of health care providers or credentials. To decrypt EHRs, they must possess the set of attributes needed for proper access. This approach provided effective solutions to some issues associated with standard encryption mechanisms. They conducted research investigated the feasibility of adopting CP-ABE in terms of storage overhead and performance. They conducted initial experiments to analyze the scalability and flexibility of the proposed approach. The results indicated that the proposed design would provide consumes negligible storage and reasonable performance. Therefore, this proposed approach can be used as an alternative to standard encryption mechanisms in cloud-based electronic



health records (EHRs) systems. This design is being implemented, which will be used to investigate the feasibility of this approach.

The researchers in [22] suggested a novel approach depends on the machine learning techniques in order to ensure data processing in an environment's cloud. The researchers used Hybrid approach is based on to Fuzzy C-means Clustering (FCM), Support Vector Machines (VFM) algorithms to divide the image to parts according to pixel's color. In addition, they incorporated a further level, the CloudSec module, into the conventional two layered architecture to reduce the risk of the potential disclosure of medical information.

## V. CONCLUSION

The purpose of this paper is to conduct a survey of previous research on cloud computing in the health sector. The research topics are both frameworks, case studies, security and privacy for adoption of cloud computing in hospitals.

## VI. REFERENCES

- [1] O. Harfoushi, A. H. Akhoshaidah, N. Aqqad, M. Al Janini, and R. Obiedat, "Factors affecting the intention of adopting cloud computing in Jordanian hospitals," *Communications and Network*, vol. 8, p. 88, 2016.
- [2] G. J. U. R. G.Nikhita Reddy, "Study of Cloud Computing in healthCare Industry," *International Journal of Scientific & Engineering Research*, vol. 4, September-2013
- [3] A. E. Youssef, "A framework for secure healthcare systems based on big data analytics in mobile cloud computing environments," *Int J Ambient Syst Appl*, vol. 2, pp. 1-11, 2014.
- [4] S. N. Sultana, G. Ramu, and B. E. Reddy, "Cloud-based development of smart and connected data in healthcare application," *International Journal of Distributed and Parallel Systems*, vol. 5, p. 1, 2014.
- [5] S. Mahmud, R. Iqbal, and F. Doctor, "Cloud enabled data analytics and visualization framework for health-shocks prediction," *Future Generation Computer Systems*, vol. 65, pp. 169-181, 2016.
- [6] M. S. Hossain and G. Muhammad, "Cloud-based collaborative media service framework for healthcare," *International Journal of Distributed Sensor Networks*, vol. 10, p. 858712, 2014.
- [7] F. Alharbi, A. Atkins, and C. Stanier, "Strategic framework for cloud computing decision-making in healthcare sector in Saudi Arabia," in *The seventh international conference on ehealth, telemedicine, and social medicine*, 2015, pp. 138-144.
- [8] C. McGregor, "A cloud computing framework for real-time rural and remote service of critical care," in *2011 24th International Symposium on Computer-Based Medical Systems (CBMS)*, 2011, pp. 1-6.
- [9] K. Haufe, S. Dzombeta, and K. Brandis, "Proposal for a security management in cloud computing for health care," *The Scientific World Journal*, vol. 2014, 2014.
- [10] M. Al-Qurishi, M. Al-Rakhami, F. Al-Qershi, M. M. Hassan, A. Alamri, H. U. Khan, *et al.*, "A framework for cloud-based healthcare services to monitor noncommunicable diseases patient," *International journal of distributed Sensor Networks*, vol. 11, p. 985629, 2015.
- [11] M. S. Hossain and G. Muhammad, "Cloud-assisted speech and face recognition framework for health monitoring," *Mobile Networks and Applications*, vol. 20, pp. 391-399, 2015.
- [12] E. Ekonomou, L. Fan, W. Buchanan, and C. Thümmler, "An integrated cloud-based healthcare infrastructure," in *2011 IEEE Third International Conference on Cloud Computing Technology and Science*, 2011, pp. 532-536.
- [13] I. K. Lai, S. K. Tam, and M. F. Chan, "Knowledge cloud system for network collaboration: A case study in medical service industry in China," *Expert Systems with applications*, vol. 39, pp. 12205-12212, 2012.
- [14] X. Wang, Q. Gui, B. Liu, Z. Jin, and Y. Chen, "Enabling smart personalized healthcare: a hybrid mobile-cloud approach for ECG telemonitoring," *IEEE journal of biomedical and health informatics*, vol. 18, pp. 739-745, 2014.
- [15] F. Alharbi, A. Atkins, C. Stanier, and H. A. Al-Buti, "Strategic value of cloud computing in healthcare organisations using the Balanced Scorecard approach: a case study from a Saudi hospital," *Procedia Computer Science*, vol. 98, pp. 332-339, 2016.
- [16] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in *2010 IEEE 3rd International Conference on cloud Computing*, 2010, pp. 268-275.
- [17] S. Shini, T. Thomas, and K. Chithraranjan, "Cloud based medical image exchange-security challenges," *Procedia Engineering*, vol. 38, pp. 3454-3461, 2012.

- 
- [18] K. A. Shakil, F. J. Zareen, M. Alam, and S. Jabin, "BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud," *Journal of King Saud University-Computer and Information Sciences*, 2017.
- [19] M. Deng, M. Petkovic, M. Nalin, and I. Baroni, "A Home Healthcare System in the Cloud--Addressing Security and Privacy Challenges," in *2011 IEEE 4th International Conference on Cloud Computing*, 2011, pp. 549-556.
- [20] J. J. Rodrigues, I. De La Torre, G. Fernández, and M. López-Coronado, "Analysis of the security and privacy requirements of cloud-based electronic health records systems," *Journal of medical Internet research*, vol. 15, p. e186, 2013.
- [21] S. Alshehri, S. P. Radziszowski, and R. K. Raj, "Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption," in *2012 IEEE 28th International Conference on Data Engineering Workshops*, 2012, pp. 143-146.
- [22] M. Marwan, A. Kartit, and H. Ouahmane, "Security Enhancement in Healthcare Cloud using Machine Learning," *Procedia Computer Science*, vol. 127, pp. 388-397, 2018.