International Journal of Engineering & Technology, 7 (3.27) (2018) 220-222

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Mobile Cloud-Privacy and Data Security in Healthcare Environment Using Cloudsim Simulator

R. Parameswari[1*], K.Vani[2]

[1]*Associate Professor, Department of Computer Science, School of Computing Sciences, Vels Institute of Science, Technology & Advanced Studies, Chennai, India.*
[2]*Assistant Professor, Department of Computer Applications, Shri Shankarlal Sundaribai Shansun Jain College for Women, Chennai, India.*
E-mail:vani_kani@hotmail.com
**Corresponding author E-mail:dr.r.parameswari16@gmail.com*

Abstract

The advancement of telecommunication in the medical field makes the diagnosis and treatment of patients in a faster manner because the patient information are stored and maintained in an electronic storage device. But there are some issues related to physical data storage, privacy by accessing user data and security etc. With the help of the cloud computing these issues are reduced now. The mobile health care system can improve the quality of patient care and reduce a medical cost for both patients and hospitals. The simulation tool CloudSim is used to generate the data center details, provider's details and processing time. For the analysis, the cloud analyst tool can simulate the data center and others. The patient information in the Healthcare Information System (HIS) and Electronic Medical Records (EMRs) is stored in a data center or cloud platform in a secure manner.

Keywords: *Cloud computing, cloudsim, data center, cloud analyst, cloud data security.*

1. Introduction

Cloud Computing is a one of the Information /Business application benefits that some organizations offer for a 'pay-as-you-go' model. Cloud computing dealswith on-demand premise for storage, server, infrastructure and applications. Therefore, securing hardware, programming and applications can essentially be executed in, dislike the conventional methodologies of establishing a data center before onecanfocus on building an business solutions[1].

Cloud Computing gets rid of the necessity for spending more amount for the data center, because the Cloud merchant provides, manages and monitors the health and usage of the framework.

The expression "cloud" has its establishment from the web which has its schematic representation as a cloud. It refers to the various particular sorts of services and applications have been conveyed in the internet cloud, and the way that, on numerous occasions, the devices used to get to these offerings and now applications do not require any extraordinary applications.

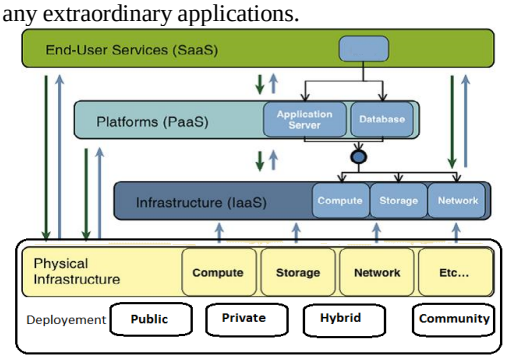

Fig. 1: Cloud computing systems

2. Mobile Cloud Computing

Mobile and Cloud computing is a center core part of healthcare's data transformation. Mobile cloud computing offers a new lead-ins to individual users of healthcare services. Wireless devices are interconnect to service platform of mobile healthcare related data, usage of data and communicate those data.

Fig 2.mobile cloud computing systems termed as follows:

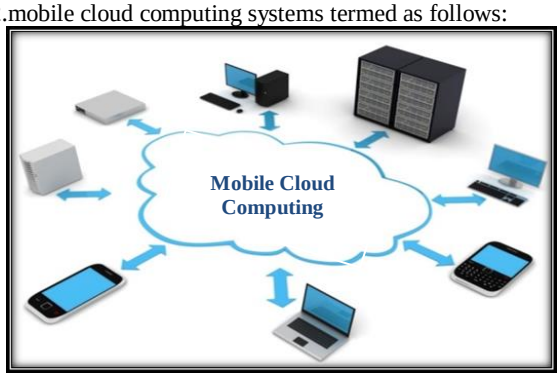

Fig. 2: Mobile cloud computing systems

3. Mobile Cloud Security in Healthcare

Many healthcare companies organizations are grasping cloud computing to improve data, performance and minimize managerial expenses The cloud lets healthcare professional access patient information from any Wi-Fi enabled tool at any location.

This straightforward entry makes it simpler for healthcare specialists, healthcare centers, and protection corporations to rapidly

share patient records. Crisis responders can give patient care faster by the method for having entry to fundamental healthcare data off-site. Doctors can assess new patients' entire medical histories online without sitting tight for physical records to be exchanged. Patients could have direct get entry to their healthcare records on the web. The sharing of data through the cloud reduces authoritative costs as a result of the decreased requirement for paper information.
Those points of interest and more have prompted the developing prominence of cloud computing in the healthcare industry. In any case, cloud computing must be successful if the cloud is secure and patient security is ensured[6].

4. Challenges of Cloud Security

Effective cloud security must handle with key challenges in the following areas:[12]

- **Preventing unauthorized access:** It is fundamental that only authorized client's get right of entry to record in a healthcare cloud. This can be troublesome in a virtual domain with such a great deal of remote clients and different remote devices.
- **Accessing data safely from mobile devices:** Health professionals and patients need to be able to access information securely from mobile devices like cell phones, tablets, or laptops. If network protection isn't always ultimate, susceptible data can be misplaced or stolen whilst accessed via an unsecured mobile device.
- **Protecting databases from malware and attacks:** A cloud needs to have a secure database that effectively protects opposition to cyber-attacks and malware. It is vital to have an incident restore and response system in place to reply fast to block any attacks or breaches[9].
- **Preventing data loss:** A cloud has to have a terrific device to prevent data loss and a manner to retrieve lost information while feasible. A cyber-attack, an encryption error, or natural disasters are some of the ways records can be lost[10].

5. Overcoming Cloud Security Challenges

Cloud computing is used in most of the healthcare technologies. This makes the healthcare organizations trustworthy to save, share data and deliver expert services using cloud.
The key challenges to cloud network security can be overcome with encryption, two-key factor identification, and security intelligence[8].

- ***Encryption:***Encrytption changes the information to another format which can only be accessed by the authorized user with the applicable key. Data must be encrypted even when it is put in storage, usage or during transmission to make sure that the data cannot be readable even when it is misplased or hacked. Based on the network security, split-key encryption technique provides a encryption key to both healthcare corporation and the cloud service provider.Each key ought to be used that allows you to get entry to facts[5].
- ***Two-key factor identification:*** Unique usernames and passwords aren't sufficient to identify authorized users. Requiring an additional method of identification like a fingerprint or specialized software token provides an additional layer of security to make sure simplest authorized users access the cloud data.
- **Security Intelligence System:** A security intelligence system that monitors the logs of all of the cloud servers and firewalls for any unusual activities can discover and block cyber-attacks and malware and prevent capability information breaches or record loss.

By analyzing these three methods, the security intelligence system taken for this research work because it provides more security and reliable data communication in the cloud computing.[14][15]

6. Cloud Simulation in Healthcare

CloudSim: A CloudSim highlight for displaying server farms is utilized as a part of Cloud Analyst. Cloud user can set up the large scale utility over the real cloud without taking any responsibility for useful resource control and resource provisioning. CloudSim toolkit affords demonstrating and re-enactment of cloud computing and resource utility provisioning strategy usage. The cloud component model can be using this simulation toolkit. The main resource data center in the cloud can be modelled and configured throughout the distinct time sector. Internet programs are accessed via customers around the arena.
This Simulation tool affords the repeatable and managed the environment to set up our own virtual cloud computing environment with specific cloud component properties. Using CloudSim toolkit, evaluate the performance of the IaaS model on the idea of expected finish time like social networking application. The simulation results for Cloud Analyst running over the cloud environment implemented over the CloudSim at the user code level.
The overall response time of Cloud analyst runs to act as a performance evaluation parameter for cloud task or resource utilization. CloudSim Toolkit presents flexibility to the user to put in force his personal resource provisioning policy. To assemble the virtual cloud computing environment, it may use the layered structure of CloudSim and implement the virtual cloud environment the tool.

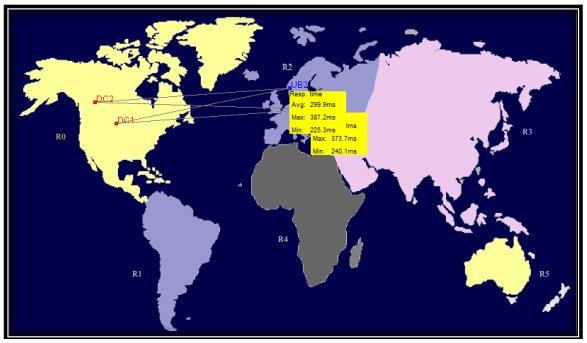

Fig. 3: Cloud analyst

Figure shows the simulation tool CloudSim is used to generate the data center details, provider's details and processing time. For the analysis, the cloud analyst tool can simulate the data center and others. The patient information in the HIS and EMRs is stored in a data center or cloud platform in a secure manner.

7. Simulation Report

The simulation results measured based on the preliminary model of the test system.

Response time of the renovated software

- The overall response time harmed down through buyer corporations, set inside geographical areas.
- The response time further separated when demonstrating the example of progress over the span of a day.
- The response time what's more harmed around the point showing the example of progress over the span of a day.

The use examples of utility

- A numerous clients utilize the application at what time from particular district, and the utilization on the data center web facilitating the applications.
- The time is taken by utilizing data center to provider a client demand
- The whole data center preparing recreation of time.

The response time variation test for the duration of the day as the sample throughout the day as the heap change.

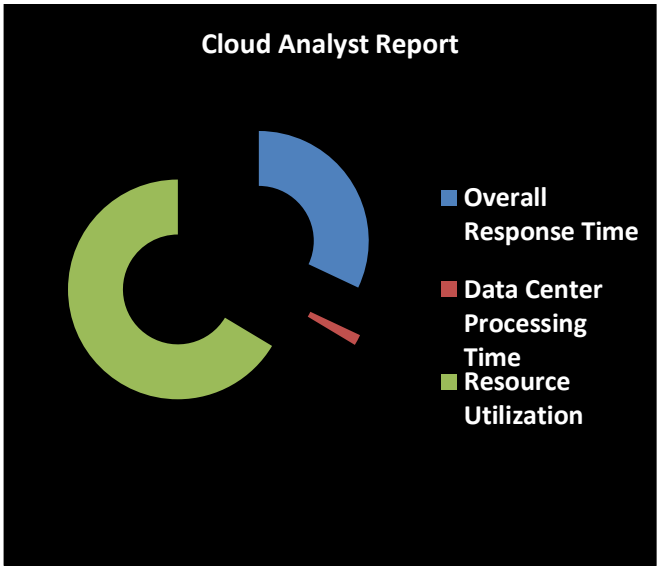

Fig. 4: Cloud analyst report

8. Conclusion

The mobile cloud security in the healthcare sector is a growing research area in the information security field. Cloud storage plays a major role in storing the healthcare record due to following reasons such as easy internet access, low-cost mobile devices, software availability, etc. To address the security challenges and policy for all patients and service providers who use mobile devices, the system is developed. In real time environment the healthcare data and medical images are protected and maintains confidentiality based on the simulation reports. Since this system is used in the distributed systems to protect the data from the hackers.

The future scope of this paper, transmission of data storing and sharing of data can be done with the help of the cloud in a much secured communication, which could be additionally to the present HIS system for implementing a VPN framework.The data generated in the big data analytics can be used to take the right decision at times of critical situation by the healthcare professionals. This will be done with increased speed and the huge size of health data and DICOM images.

References

[1] Mell P & Grance T, "NIST Definition of Cloud Computing", *USA: National Institute of Standards and Technology*, (2011).

[2] AbuKhousa E, Mohamed N & AlJaroodi J, "e-Health Cloud: Panchumarthi, G. P., & Surendar, S. M. A. (2017). A review article on Fin-FET based self-checking full adders. Journal of Advanced Research in Dynamical and Control Systems, 9(4).

[3] Armbrust M, Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I & Zaharia M, "A View of Cloud Computing", *Communication of the ACM*, Vol.53, No.4, (2010).

[4] Arora R & Anshu P, "Cloud Computing Is Transforming-Secure user data in cloud computing using encryption algorithms", *International Journal of Engineering Research and Applications*, (2013), pp.1922-1926.

[5] Berry LL & Bendapudi N, "Health care: a fertile field for service research", *Journal of Service Research*, Vol.10, No.2, (2007), pp.111–122.

[6] Boroujerdi M & Nazem S, "Cloud Computing: Changing Cogitation about Computing", *World Academy of Science, Engineering and Technology*, (2009).

[7] Varshney U, "Pervasive healthcare and wireless health monitoring, Mobile Networks and Applications", *Kluwer Academic Publishers*, Vol.12, (2007), pp.113–127.

[8] Cong W, Chow SSM, Qian W, Kui R & Wenjing L, "Privacy preserving public auditing for secure cloud storage", *IEEE Transactions on Computers*, Vol.62, (2013), No.2.

[9] Jeager PT, Lin J & Crimes JM, "Cloud Computing and information policy: Computing in a policy cloud", *Journal of Information Technology and Politics*, Vol.5, No.3, (2008), pp.269-283.

[10] Johan GB, "Electronic healthcare record; a way to empower the patient", *International Journal of Medical Informatics*, Vol.69, (2003), pp.191-196.

[11] Kim J, Beresford AR & Stajano F, "Towards a Security Policy for Ubiquitous Healthcare Systems", *Proc. 1st International Conference on Ubiquitous Convergence Technology*, (2006), pp. 263–272.

[12] Kuyuto SO, Ibikunle F & Awodele O, "Cloud computing security issues and challenges", *International Journal of Computer Networks (IJCN)*, Vol.3, No.5, (2011), pp.247-255.

[13] Lour H, Sadeghi AR & Winandy M, "Securing the E-Health Cloud", *Proc. First ACM International Health Informatics Symposium*, (2010), pp.220-229.

[14] Villalobos Antúnez, JV (2017). Karl R. Popper, Heráclito y la invención del logos. Un contexto para la Filosofía de las Ciencias Sociales. Opción Vol. 33, Núm. 84. 5-11

[15] M Pallarès Piquer and O Chiva Bartoll (2017). La teoría de la educación desde la filosofía de Xavier Zubiri. Opción, Año 33, No. 82 (2017): 91-113