November-December 2019
ISSN: 0193-4120 Page No. 2301 - 2306

# Authentication Based Cloud Computing Security Model for e-Healthcare System

[1]Rajesh Yadav, [2]Anand Sharma
*Research Scholar, SET-MUST, Lakshmangarh, yadav.rajesh27@gmail.com*
*Asst. Prof. CSE, SET-MUST, Lakshmangarh, anand_glee@yahoo.co.in*

***Article Info***
***Volume 81***
***Page Number:2301 - 2306***
***Publication Issue:***
***November-December 2019***

***Article History***
***Article Received:*** *5 March 2019*
***Revised:*** *18 May 2019*
***Accepted:*** *24 September 2019*
***Publication:*** *12 December 2019*

***Abstract:***
Providing medical services,for analyzing the information through collecting the patient's vital data, required lot of labor work. Thesemethods are usually slow and error-prone, using a potential that avoids real-time data accessibility. This set-upkeeps the clinical diagnostics and monitoring facilities. With this kind of situation, the sensors with medical equipment's and cloud servers are inter-connected to exchange the service [1]. The data available in cloud can be managed by expert systems and further distributed to medical staff. The problem with this solution is that there is no authentication from patient side as well as from medical staff/doctors side. From patient side there is no surety that, data which is stored on cloud will be right data or not and from medical staff/doctor side also not surety that they will not misuse the data. For this problem a solution as a model is proposed in this paper, in which authentication is mandatory for both-sides, patient side and staff/doctor side.

***Keywords:*** *Cloud Computing, Authentication, Medical-staff, MD5, TOTP, e-health, Token, 2 key authentication.*

## I. INTRODUCTION

Telemedicine permits remote analyses and monitoring of patients [2]. It provides protection, alertness and reliability in modern health-care institutions. There are many challenges related to automation in this environment [3].

Now day's computer systems are used widely in medical and healthcare systems. For the storage, documentation, analysis, processing, and presentation of patient'sdata storage devices and server systems are used.Healthcare systems are built on the basis that consists of paper handwritten test results, medical records, non-digitized images, handwritten notes and split IT systems. Sharing of information across providers is not portable and it's very inefficient and insecure.Doctors are depending on the medical staffs for patient's data [1]. All these processes are weighty and time consuming, so the collaboration and coordination between patients and doctors.

This problem is resolved to automate the process from information sharing, data collection and remotely access by healthcare service provider. For that sensors are connectedwith medical equipment's that are inter-connected to exchange services; these are joined to the healthcare computing network organization[1]. Themedical data is store in the "cloud", from where it can be managedand use by doctors/medical staff.

In the cloud, resources are shared by doctor's staff members, patients or other related persons. As a result patient's data in the cloud become open to all. Thus the records are more susceptible to attack. It is very easy for an intruder to harm the original patient's records [2]. So it is very

November-December 2019
ISSN: 0193-4120 Page No. 2301 - 2306

important for the cloud to be safe and secure. For security we need to restrict the user and only authorized user can access the data.

*A. E-Health*

E-Health there the interaction between patients and health service providers/health professionals. E-health should be efficient; thereby it decreases effort, cost and access accurate data. It also enhances the quality of care. It easily provides patient's to health services online from global providers. The technologies in E-health care are an important part of medical treatment and follow up procedures. Patient's medical records can be effectively shared with a wide range of users, including staff from health care providers, and other health professionals [4]. Electronic health record (EHR) is the essential source of information for future health care professionals.

*B. Cloud computing in healthcare*

Cloud computing change the concept how technology is manages and used. In cloud computing, the user can connect with resources and use the services without concerned how its work [5]. Like other services healthcare also use the cloud computing for information sharing between patient's and health professionals, data storage and access from anywhere through internet connection. Fast and efficient information exchange is necessary for quality healthcare [6].

Healthcare organizations can buildup cloud computing to well organize healthcare information system which provide effective and efficient medical data sharing and management. It's minimized the cost when accessing the information remotely. Cloud computing provide a perfect platform there hospitals can connect with each other and can share infrastructure and resources together hence cost reduction and increase of utilization [7].

Healthcare data is rising day by day. Therefore healthcare organizations outsource the storage services in the form of cloud computing and accordingly pay for that. Basically there are three main computing models (i.e. SaaS, PaaS and IaaS) are used in healthcare systems [8].

Cloud computing makes healthcare origination more efficient and advance. The followingadvantages of cloud computing in healthcare are.

- *Usability without taking into explanation and place*

Usability is related with the functionality of the application, system or product. It is the scope to which the product is easy to understand and use. The main important benefit of cloud computing is that user can access cloud service at anywhere, anytime through their laptop, personal computers, or mobile devices. Therefore, in cloud computing the information is exchange between healthcare users like hospitals, patients and doctors.

- *Equipment procurement is not required*

Cloud computing permits users to get the services or solutions so that Healthcare organizations don't need to purchase the hardware, technology or infrastructure [9]. With cloud technology hospitals can share their machine and equipment's for diagnosis and checkup. They share our health data for analysis and patients care [10].

- *Save money*:

Manual data collection is very costly and time consuming and error-prone. But through cloud computing data collection will be fast, simple and low costly. Through sensors attachment in equipment's automatically data storage in cloud make it possible to connect and exchange data between devices.Therefore, healthcare organization will save lot of money [11].

- *Minimum maintenance*

Cloud computing services will be available on the bases of on demand so that it's required minimum maintenance.

- *Quickly to take in use*

Cloud computing allow the healthcare staffs that have authorizations, to access the services from anywhere as long as they want [11].

November-December 2019
ISSN: 0193-4120 Page No. 2301 - 2306

- *Disaster recovery*

In healthcare using a Cloud computing is the good choice.Because they don't need to worry about the data lost or any harm. In cloud computing itprovides the backup or recovery a data of site as well as to fail the server [11].

### *C. Authentication*

While these new technologies promise to transform patient care, they also complicate the task of securing patient data. But patient data will continue to be a profitable target for cyber attackers. Healthcare providers need to recognize the evolving security challenges in this complex environment[12]. Authentication is the one of solution to safe and secures the patients and health organization data. Through authentication only authorized user can access the cloud for data storage and data sharing for patients care.

There different types of techniques are used for authentication: password or PIN, single sign-on, token, two-factorauthentication, three-factor authentication and biometrics etc.

We proposed a model through that first, before storing a patient's data into cloud equipment required to authentication first, so only authorized equipment's data will be store into cloud. Second when doctors, care taker and other related persons are trying to access the data they also first required authentication, through valid authentication they can access a data anywhere and anytime.

## II. RELATED WORK

After load the health data in cloud patient to lose the control of them so there chances to lose its sensitive data, which makes the requirement of authentication before access by other [13].

Bruno M.C. Silva *et.al* [14] the authors has suggested thatM-health is the new innovation in healthcare. M-health system and its mobility functionalities have a strong impact on healthcare monitoring and alerting system. It does not discuss about the user authenticity,who is using the cloud healthcare system for which purpose.

Richard Millham [15] proposes an enhanced model to share patient data with increased capacity but there is not concern about security of data.

Ming Li1 [16] It's beneficial for online personal healthcare records to transfer into cloud, its increase the elasticity of resources and reduce the operational cost. Storing personal healthcare data into cloud, the patients lose control to their data. In paper explain before storing data into cloud it's encrypt the data, it is challenging to know that which data is related to which patient because data is encrypted using different cryptographic keys, and there is no authentication so who is able to decrypt the data can access it. Its model is not providing more security.

RuoyuWu*et.al*[17] the author explain that in electronic medical record system access control is the major issue. In paper proposed a mechanism to systematic access control to care the composite e-health from different healthcare providers in cloud. There discuss about feasibility and efficiency but not about the security of accessing data.

Rui Zhang*et.al* [18] there author discuss about the concept of sharing and integration in healthcare cloud and analyzing the security and privacy issues in electronic health records. Author describes an electronic healthcare security model for managing security issues. This also can be improved through authentication techniques.

Kumar P. [19] surveyed the different techniques for authentication in health care system through wireless body area network.

Pradeep Kumar [20] proposed genetic algorithm for data security in healthcare data with respect to wireless body area network.

## III. METHODOLOGY

In this paper we have proposed a model with an aim to provide authentication for cloud services. It

November-December 2019
ISSN: 0193-4120 Page No. 2301 - 2306

will be helpful for various medical practitioners to store and access the data of the patients in a secured and effective manner.

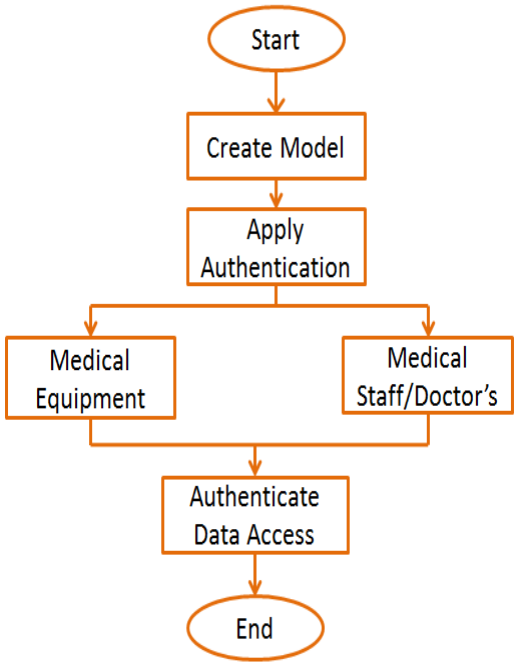


Fig.1 Flowchart for given methodology

Now in this paper we have applied authentication in following manner:

- When the sensors generate the data, it will first get authenticated before its storage to the cloud.
- Various stockholders of the medical field like doctors, caretakers, patients etc., can access the data through several devices, only when they have performed proper authentication for its access from cloud.

We apply authentication to the above approaches through our proposed model, which will turns advantageous in the following ways:

- Only authorized equipment's can able to store real-time data on cloud.
- It's eliminates anonymous data on cloud.
- Patient's data is safe and secure, so data misuses are reduced.
- Because of data authenticity, patient data analysis is perfect and takes right discussions for the treatment.

There are several ways to achieving the authentication:

- Passcode
- OTP
- Single sign-on
- 2 key authentication
- Token

## IV. PROPOSED SOLUTION

With the help of following model we proposed the solution.

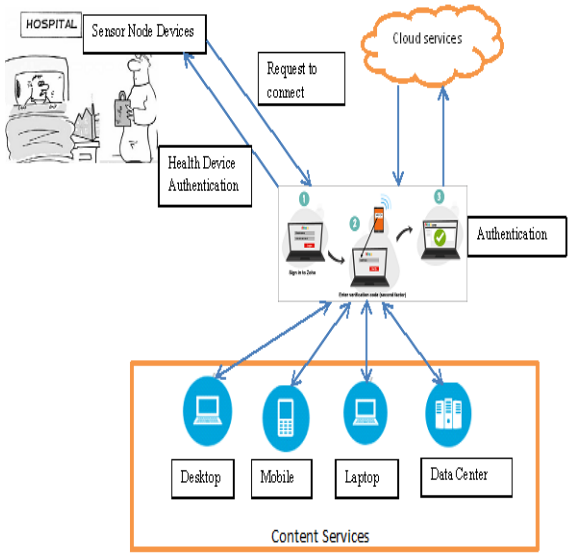


Fig.2 ProposedModel

In this model for authentication use the single sign-on and token authentication techniques on two different stages. When data is store on cloud machine through medical equipment's, use the token concept for authentication. In the respect of every patient first generate a unique token which is active till the equipment is connected to the patient's body. Data is store in the cloud with patient id. When treatment is done and removes the equipment from patient body, that token isfinish. For every patient generates a new token key.

When doctors or medical staffstrying to access patients data before they required to authentication. Forthat use the 2 key

authentication techniques. In this technique we use the login id and password and after successful login generate the OTP on their register mobile no. when both the authentication is successful that can able access the patient data for their treatment or other tasks.

We implement the proposed model through preparing the prototype in cloudsim simulator. Following authentication MD5 (Message Digest 5), TOTP (Time based one-time password)algorithms use for data safety.

## V. CONCLUSIONS AND FUTURE WORK

This paper discusses the model to automate the process of collecting data through number of sensing devices and further transmitting them to cloud for storage, processing and other related activities. Based on this model proposed the additional security mechanism to improve and provide the security to the collected and transmitted data. In the proposed model MD5 and TOTP algorithms has been used for authenticating the transmission sensing nodes and for accessing the gathered data at various interfaces respectively. The proposed model provides an efficient and secure way for data collection, accessing and processing required for various application areas using the benefits of clouds. As future work, we are planning to implement the whole system and to go through more to performance evaluation of authentication time.

## VI. REFERENCES:

[1] Kawser Wazed Nafi, Tonny Shekha Kar, Sayad Anisul Hoque, Dr, M.M. a Hashem, "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture",*IJACSA*,Vol. 3 issue 10, 2012.

[2] Debahis Saha, D. and Amitava Mukherjee, "A Pervasive computing: A paradigm for the 21st century", inIEEE Pervsive, Vol 36, issue 3, pp. 25-31, 2003.

[3] Carlos OberdanRolim, et.al, "A cloud Computing Solution for Patient's Collection in HealthCare Institutions", in Second International Confrence on eHealth, telemedicine, and Social Medicine, vol. 36, issue 3, March 2010.

[4] A. Antony Viswasa Rani, E. Baburaj, "An efficient secure authentication on cloud based e-health care system in WBAN", in Biomedical research, special issue S53-59, 2016.

[5] Aziz HA, Guled A, "Cloud Computing and Healthcare Services", Journal of Biosensors & Bioelectronics, p. 7:3, 2016.

[6] Sultan N, "Making use of cloud computing for healthcare provision: opportunities and challenges",International Journal of Information management, pp. 34:177-184, 2014.

[7] M. Li, S. Yu, K. Ren, and W. Lou, "Security personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner setting", in International Conference on Security and Privacy in Communication Systems, pp. 89-106. 2010.

[8] Aziz H, Madani A, "Evoluation of the web and its uses in healthcare", Clinical laboratory science: journal of the American Society for Medical Technology, pp. 28(4):245-249, Oct. 2015.

[9] Rahul Amin, et.al.,"A robust and anonymous patient monitoring system using wireless medical sensor networks", Future Generation Computer Systems, pp.80: 483–495, 2016.

[10] Carlos OberdanRolim, et.al., "A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions", in Second International Conference on eHealth, Telemedicine, and Social Medicine, Feb. 2010.

[11] Jing Jin, et.al., "Patient-centric authorization framework for electronic healthcare services". Computers & Security, pp. 30(2):116-127, 2011.

[12] Srivastava, P., Yadav, R and Razdan, P., "Cloud Computing in Indian Healthcare Sector",Proceedings of ASCNT 2011, CDAC, Noida, India, pp. 1-8, 2011.

[13] Li M, Yu S. Zheng Y. Ren K, Lou W. "scalable and secure Sharing of Personal Health records in Cloud Computing using Attribute-basedencryption",IEEE transactions on parallel and Distributed systems,pp. 24: 131-143, 2013.

[14] Bruno M.C. Silva, et.al., "Mobile-health: A review of current state in 2015",Journal of Biomedical Information, Elsevier, Vol. 56, pp. 265-272, 2015.

[15] Richard Millham, "An Enhanced Cloud Computing Model for Patient Record Management in South.Africa", in IEEE International Conference on Cloud Computing in Emerging Markets (CCEM),2015.

[16] Ming Li1, Shucheng Yu1, Kui Ren2, and Wenjing Lou1, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings", in International Conference on Security and Privacy in Communication Systems, Springer,pp. 89-106, 2010.

[17] RuoyuWul , Gail-JoonAhn , Hongxin Hu, "Secure Sharing of Electronic Health Records in Clouds", in 8th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing , CollaborateCom 2012 Pittsburgh, PA, United State, pp. 711-718, 2012.

[18] Rui Zhang, Ling Liu, "Security Models and Requirements for Healthcare Application Clouds", inIEEE 3rd International Conference on Cloud Computing, pp. 268-275, July 2010.

[19] Pradeep Kumar and Anand Sharma, "Survey on Authentication Process in Body Area Network" in International Journal of Electronics Engineering Research (IJEER)Volume 9, Number 6, pp. 913-921, 2017

[20] Kumar, Pradeep and Sharma, Anand, Data Security Using Genetic Algorithm in Wireless Body Area Network (2018). International Journal of Advanced Studies of Scientific Research, Volume 3, Issue 9, 2018.Available at SSRN: https://ssrn.com/abstract=3315423