IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

TRUST BASED MONTORING AND AUDITING SYSTEM FOR M-HEALTHCARE IN CLOUD COMPUTING: A Review

[1]Praveen S. Challagidad, [2]Ashwini S. Kale

[1]Professor, [2]PG Student,

[1]Department of Computer Science and Engineering Basaveshwar Engineering College Bagalkot - 587103, India.

[2] Department of Computer Science and Engineering Basaveshwar Engineering College Bagalkot - 587103, India.

Abstract: M-Healthcare is a sub-segment of e-health and stands for mobile healthcare. It faces many challenges such as data integrity attacks, service availability, reliability, data security, and trust management. Some research works have been published to resolve the challenges associated with it. But, there are only a few research works on data integrity, data security, and trust management. Data security and trust management in M-Healthcare is a critical issue because it is quite essential in securing the system and building trust among the entities in the healthcare system and cloud. Hence, data security and trust evaluation and management in the M-Healthcare system are a big challenge. This abstract aims to design and develop of trustworthy M-Healthcare System (TMHS) which monitors and audits patients' health records and doctor's information by building trust among all entities. The THMS uses the Technique for Order of Preference by Similarity to the Ideal Solution (TOPSIS) method to build and evaluate the trust and the Performance Monitoring and Auditing System (PMAS) is used to manage the trust among all entities. It is planned to use Machine Learning Techniques such as Support Vector Machine (SVM) and Artificial Neural Network (ANN) to resolve the mentioned challenge. The proposed system also is expected to achieve data integrity, availability, and reliability.

Index Terms **- Trust evaluating, Monitoring, Auditing M-Healthcare.**

I. INTRODUCTION

The term cloud computing "refers to the much-needed availability of computer system resources, including data storage (cloud storage) and processing power, without the user's constant control [1]". Cloud computing focuses on sharing resources to achieve compliance and is often based on a "pay-as-you-go" approach, which can help reduce significant costs but may also result in unexpected operating costs for inexperienced users."Art applications, business apps, data storage and backup applications, educational applications, and entertainment applications are all examples of cloud computing applications [4]."

The combination of cloud computing with health monitoring is known as cloud-based healthcare. The computer equipment permits the dissemination of accurate medical information through the internet at any time and from any location.

"Mobile health is the practice of medical and healthcare using mobile devices, tablets, and portable computers (or M-healthcare) [20]". M-Health has developed tremendously in recent years, owing to extensive use in developing countries and more widely available mobile technology. In poor nations, M-Health focuses on getting information quickly in order to diagnose symptoms, track diseases, and deliver timely information to the public.

One of the most important aspects of healthcare is trust. It is essential for new health-related services to be accepted and required. In order to assess trust in healthcare, patients must have had prior interactions with healthcare service providers. Trust in M-healthcare, which includes entities such as patient information, Doctor Information, specialized information for the specific treatment, and receptionist information, as well as the provision of medicine to each patient. Patient_id is an M-healthcare option for tracking the patient. Every healthcare entity must work together and coordinate well in order to have a secure and reliable M-Health cloud technology. The proposed system focuses on monitoring and auditing M-Healthcare entities to evaluate trust among them. Checking is a procedure for laying out trust and assessing it progressively.

"The Monitoring Approach assessment system is as per the following:

1. Inactivity: A help's inertness or organization dormancy time.
2. Execution Time: The time it takes an assistance to perform and deal with its succession of activities is alludes to as its execution time.
3. Reaction Time: A help's reaction time is the time it takes to process and execute an assistance demand; the reaction time contains the execution time and inactivity.
4. Throughput: The quantity of solicitations a help can process for every unit of time is alluded to as its throughput" [20].

Audit is a protective effort that ensures the security of the medical services framework. It basically means keeping client services of medical services in chronological order, for example, keeping log-in logs and information differences.

II. RELATED WORK

This section introduces a comprehensive book review in the cloud computing testing platform and introduces Trust based Monitoring and Auditing system for M-healthcare in cloud computing also presents qualitative of parameters, Dynamic trust evaluation, reputation based trust in healthcare System model (i.e., TBMAS-MH)

Table 1: Overview of Literature survey

Author and publication year	Description	Advantages	Limitations
In 2020 the study of Salah T Alshammari et,al;[1]	Introduction Role-based access control (TRBAC) techniques can be used for cryptographic tasks to ensure privacy. This method protects data from unauthorized users while allowing authorized users to access it.	Allows the reliability model to be integrated with the cryptographic T-RBAC-based system to decrease the number of unscrupulous clients among TRBAC	Trust is one of main issue
In 2020 the study of Praveen S. Challagidad et,al;[2]	MDTES assists CCs in choosing a dependable CSP that offers the suitable QoS, in addition to CSPs in choosing appropriate and prison CCs. In evaluation to current agree with models, the experimental consequences display that the MDTES is self-motivated, resourceful, and constant in figuring out honest and untrustworthy CSPs and CCs.	MDTES is self-motivated, effective and stable in distinguishing between reliable and reliable CSPs and CCs.	MDTES include to deal with Qualitative head to head comparisons between accessible works.
In 2015 the study of Hanen Jemal,et ,al;[3]	The study describes an integrated system that includes Multi-Agent System (MAS), Web Service and MCC. This document describes the MCC and web health care services.	Collaboration, Performance, safety, Modernization, Portability	It only uses the mgmt home care system to monitor high blood pressure and diabetics.
In 2018 the study of Farhana Jabeen,et,al;[4]	The following are the main contributions to this paper: Sections of soft trust in healthcare systems, (ii) reference model to evaluate concert and description of TRS, and (iii) expectations research topics of soft trust in health care.	Improve data communication privacy and security.	The fact that these TRSs they have not been tested in real world conditions within a particular legal framework is one of their limitations.
In 2011 the study of Hoang T. Dinh,et,al;[5]	This paper provides an MCC survey, which helps ordinary readers to get an overall view of the MCC including definitions, structures, and applications. Issues such as, battery life, storage, and bandwidth introduced.	Mobile applications benefit from job transfer and remote processing, Dynamic Offering, Scalability, Multitenancy, Easy integration	Bandwidth is one of the major problems for MCC because the radio service for wireless networks is not easily accessible compared to conventional wireless networks; Availability of service becomes a very important issue..
In 2018 the study of Wided Ben Daoud et,al;[6]	The suggested scheme's major features are the integration of the trust concept with the monitoring process in order to provide greater access control security. The suggested approach's methodology is supported by adequate assessment findings, and it enhances system security and performance by reducing the time spent obtaining permits to access services and improving total system resource use.	This enhances system security and speed by reducing the amount of time it takes to get permits to access services. Exceptional security and privacy.	Less data storage
In 2018 the study of Matin Chiregi et,al;[7]	The article outlines a systematic review (SLR) in a cloud-based reliability test. By Introducing high-level knowledge and challenge, this study will directly support scholars, researchers and staff in their understanding of changes in cloud reliability testing.	Encourage ideas of trust value and trust behaviour in the CC environment.	Issues such as integrity, honesty, trustworthiness, flexibility and balance.
In 2016 the study of Zainab M. Aljazzaf et,al;[8]	This paper provides a SOA-based solution based on the definition of trust and guidelines for choosing services based on their reliability. In particular, SOA is being developed, and the original component, the support of trust , is being introduced into the construction of structures, which is responsible for the process of trust..	Trust is changing, trust depends on who you are, and trust is based on knowledge.	Privacy, security, trust.
In 2018 the study of Lilei Lu, Yuyu Yuan et,al;[9]	The purpose of cloud services is explored with two ideas in this paper. For one reason, there is concern about the reliability of QoS data sources, which is why QoS branded monuments, are used instead of user feedback ratings. Another goal is to reduce the impact of inaccurate or fake parameter information by specifying the entropy weight of different QoS attributes. Second, trust selection is introduced, which reflects the humility of trust.	One is the cycle of assessing trustworthiness.	Inaccuracy between things, which makes it difficult to compare them properly.
In 2018 the study of Fayez Alqahtani et,al;[10]	To deal with the issue in the management of trust in multi-cloud systems, this study uses a series of TSPs distributed across all Service Providers (TSPs) cloud-based applications	Improving the security.	In making decisions about a more accurate signal, the nearness of

	that collect raw trust data from a variety of sources and formats. Data about a CSP's compliance with a cloud-based service's Service Level Agreement (SLA) as well as CSU feedback make up this proof. Using this information, assess the objective and subjective trustworthiness of CSPs.		two or more devices with a slight coldness difference fail.
In 2018 the study of Wenjuan Fan et,al;[11]	This study uses a series of Trusted Service Providers deployed to manage trust management complexity in multi-cloud systems (TSPs) TSP are dispersed more than the cloud and collect raw trust data beginning a number of sources and formats. This evidence comprises data on a CSP's compliance with a cloud-based service's Service Level Agreement (SLA) as well as CSU input. Assess the objective and subjective trustworthiness of CSPs using this data.	Good performance observed.	Total related errors occur in unreliable estimates.
In 2021 the study of Rong Jiang et,al;[12]	To measure the reliability of the role factor in the size of the physician's personal qualifications, this study provides a T-RBAC (reliable access control) model based on two-dimensional integrity tests using AHP and Gray theory. Using Euler's rating and calculation of probability, the basis for trust law is based on the legitimacy of a category based on the full value of the standard, which assesses doctors' reliance on ethics at the previous level. The access control system offers better flexibility and improved security due to the reliability of many features in testing.	The model has smooth access and high security.	Sensitivity, dynamics, and bleaching resistance.
In 2021 the study of Z. Faizal khan et,al;[13]	With a focus on the particular issues in m-health, this article investigates the use AI and data analytics to provide users with information and help them organize, and introduce AI and a m-health model based on big data analytics. The findings of this study will contribute to the development of effective m-health data management strategies using a grouping of AI and big data as a basis.	The proposed method enhances the m-health process by processing each question, and allows for real differences.	Population, the system will never be very accurate, should rely entirely on technology, as well as various privacy and security concerns.
In 2020 the study of Muhammad Imran Saleemet,al;[14]	The Smart E health monitoring system is cutting-edge technology that attempts to keep us safe in our surroundings. The underlying causes of health problems must be addressed first in order to make living risk-free. The Internet of Things (IoT) is transforming health care in both technological and socially positive ways. This intelligent health system is built on cutting-edge network topologies and IoT-based health-care applications.	It is easy, dependable, and low-cost, with complete data security.	Battery failure, Signal failure due to any reason such as distortion or power failure. Server response delay.
In 2020 the study of Mohamed Firdhous,,al;[15]	The authors of this work are investigating what is trusted and how it is used on a distributed computer. The following section provides a summary of the recommended models for the various distributed systems. The capabilities, functionality of the actual cloud system, and the ability to use trusted cloud computing systems have been tested. Finally, the proposed models / systems are compared using others using a set of cloud computing terms.	The fundamental benefit of this strategy is that it integrates cloud computing to a watermark-aware operating environment.	One of the most important problems is cloud security.
In 2015 the study of Praveen S. Challagidad,al; [16]	To address limits such as power, storage, scaling, management, and computing, wireless network (WBAN) systems use cloud computing technology (CC). The distributed location with CI S presents additional risks to patient data solitude and security. Methods of confidentiality of patient data and security in S-CI are discussed in this study. According to their workplaces, Multi-biometric key generating, smart key creation, hash functionality, attribute-based encryption, mixed maps, mixed encryption, Numerical Research Unit, Tri-Mode Algorithm, Marking Dynamic Probability Pack, and Basic Data Transfer Strategies. they are all examples of existing strategies.	Conventional security measures cannot solve all kinds of security problems due to its complex structures that combine a combination of various modules and technologies.	Security is considered as one of the most critical issue, decrease in the confidence of cloud technology
In 2017 the study of Praveen S. Challagidad,al; [17]	This study raises a reputable model based on reputation that assesses service provider reputation using a reliability test that considers customer feedback, server downtime, and server load. Results are valid.	From a distant data centre, cloud computing provides businesses with cost-effective dynamic, scalable, and shared services..	The issue of cloud computing trust is a major one.
In 2018 the study of Isma Masood,al;[18]	Wireless network (WBAN) systems have used cloud computing technology (CC) to overcome limitations such as power, storage, measurement, management, and processing. Total S-distributed CI poses additional risks to patient data privacy and security. In this work, methods of patient data privacy and security in the S-CI are considered. Available strategies can be categorized as the creation of multiple biometric keys, intelligent key creation, hash functionality, attribute-based encryption, complex maps, mixed encryption, Numerical Total Search Unit, Tri-Mode Algorithm, Picketing and Important Priorities Data Forwarding, depending on their	Special thinking about understandable applications, unwieldy applications, effective admission control, network security, real-time usage, and better quality of cool data access.	Restrictions such as authority, storage, rating, running, and computer.

	search terms.		
In 2020 the study of Roman Lewandowski,al; [19]	Assesses the crash of remedial information on patient trust in physician, health check practitioner, hospital, and payer levels. The COVID-19 outbreak in Poland appears to be having a significant impact on patient confidence in medical settings. Patient trust increases medical treatment results, improves perceptions of healthcare presentation, and enhances the efficiency of healthcare systems.	Reliability enhances treatment outcomes, elevates the perception of health care performance, and facilitates the overall functioning of health care systems.	Increases in trust in hospitals and payers, contrasting losses in physician trust, may be connected to trust levels.
In 2020 the study of H.Y. Lam,al;[20]	The aim of this project is to discuss the propose of an intelligent M-Healthcare System (ImHS) to reduce the need for staff to go to higher service providers by reducing the level of technology and simplifying the guidance process for staff. Face recognition technology is used to enable adults to access and track their medical records using the FaceAPI service. Future IMHS provides consumers with faster access to health care information, reducing the frequency of unpleasant drug reactions (ADE) and reducing the length of the pill delivery process.	To monitor and protect the health status of the elderly who provide the highest level of care for the mature, it is important to use mobile applications and EHR to progress efficiency.	Complaint due to human mistakes

III. ISSUES AND CHALLENGES

Nowadays, healthcare organizations want to be able to access medical records at any time and from any location. In a health-care centre, the cloud paradigm is being used. Medical files are shared and integrated. There are numerous cloud computing uses to boost confidence in this relatively young technology. There are various safety criteria that must be met. The problems and obstacles that follow are listed below.

1. Data Integrity Attacks: In M-Healthcare, if data isn't expected after transmission or storage in the cloud, it can have serious security consequences. When it comes to Mobile Cloud Computing (MCC) security, data integrity is critical since data is stored and processed on cloud services.
2. Service Availability, Security Risks, and Mechanisms: For users and cloud service providers, MCC Availability and Reliability are critical.
3. Data saved and processed in numerous places poses a risk: Data stored on mobile devices is frequently transported and stored in the cloud. Because it is heavily loaded and run on the cloud, the data code is susceptible on mobile devices.
4. Trust: In terms of the healthcare system and the cloud, trust is a crucial problem since it plays a significant role in safeguarding the system and developing trust among the entities. The fact that these Trust and Reputation Systems (TRS) have not been experienced in real-world circumstances inside a specific legal framework is one of its limitations.
5. Due to the offline natural connection between all involved, it is not possible to maintain continuous communication between the patient and the health care system (e.g., in an emergency while mobile, it is difficult for the patient to get immediate help)
6. Early development of global healthcare computing standards is a crucial objective for the health informatics community. Interoperability between systems will never be accomplished without standards.
7. Data integration and interoperability technologies are employed.
8. Battery life is a major factor in the adoption of mobile health apps. Clinicians demand a gadget that is operational for the duration of their shift.

IV. PROBLEM DEFINATION

Over the years, the health care community has seen significant improvements in the methods and technologies used in health care delivery, including M-health as a rising area of healthcare application to get better the accesses to heath services. The area of healthcare is involved with treatment of patient's sensitive data. The security and privacy of this data is of paramount importance. The main goal of the crisis statement is to develop an M-Healthcare application that will enable safe, reliable and trustworthy communication between patients and health care providers. This can be resolved by designing trust evaluation mechanism which includes Trust building, Trust evaluation, Trust update, Monitoring and Auditing phases.

V. OBJECTIVES

Design and development of trustworthy M-Healthcare System (TMHS) which monitors and audits patient's health record and doctor's information based on trust by building the trust among all entities.

The TMHS aims at:

1. Design of adequate, qualitative and preventive trustworthy healthcare system.
2. To enable health professionals to store and access information related to patient health records at any time anywhere.
3. Improve communication of patient information in a readable format that anyone can use. And they treat their patients very easily even from a distance.
4. Using digital health, and especially M-health to increase access to health services through effective and timely sharing of health data, especially for people who are hard to reach.

VI. PROPOSED SYSTEM

This paper proposes TBMAS-MH which precedes using 5 steps:

1. Healthcare information,
2. Information collected by cloud service provider and cloud entities
3. Trust evaluation process(TOPSISs)
4. Trust Mechanism process
5. Delivering and secured data to mobile phones via Healthcare Administrative.

Figure 1 illustrates the architecture of the proposed system (i.e. TBMAS-MH). Following steps describes TBMAS-MH:

1. M-Healthcare Entities Module: M-Healthcare cloud entities which extracts detailed information about the patient, Doctor, Nurse, Specialist.
2. Compliance information (CI) from all cloud organizations to CA. The incoming CI is referred to PMAS to monitor and generate a CI report based on Qos parameters
3. The CI report was received by PMAS or CA. The developed TOPSIS method is used in the reliability rating process. The audited trust is delivered in a trustworthy test method to assess the final reliability of Patients, physicians, specialists, physicians, nurses, CCs and CSPs and reviews the assessed reliability of the system.
4. The evaluated trustworthiness is submitted to CA for auditing purpose. If any entity wants know their trustworthiness then a request is to be submitted to CA.
5. For Pre Evaluation data being sent to SOA for the trustworthiness of information.
6. Reports submitted to Health Data Layer analyze cloud-based healthcare data to support individual clinical decisions.

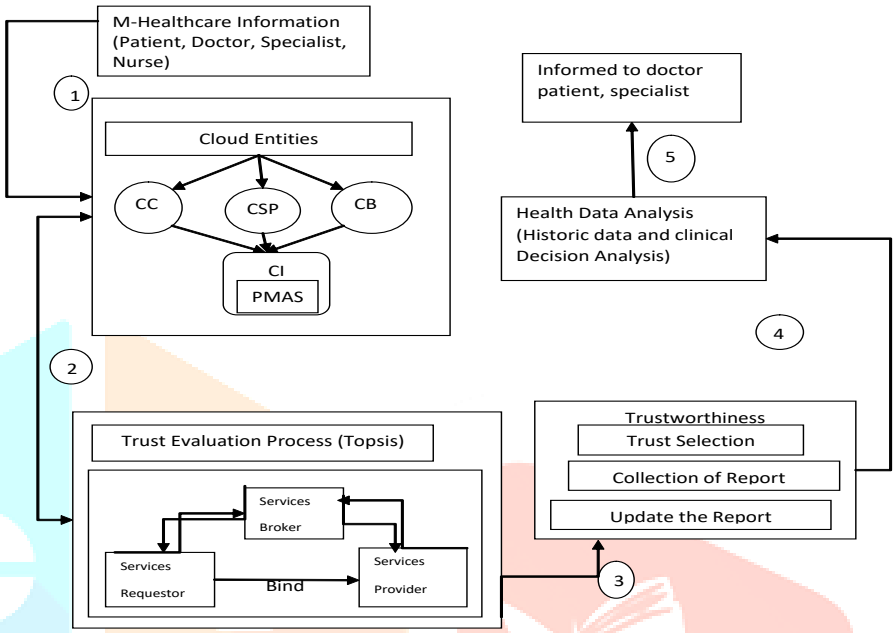

Figure 1: Architecture of TBMAS-MH

7. Tested reliability is sent to CA for research purposes. If any business wants to know its reliability the application should be submitted to the CA.
8. For Pre Evaluation data being sent to SOA for the trustworthiness of information.
9. Reports submitted to Health Data Layer analyze cloud-based healthcare data to support personal clinical decisions.
10. In support of clinical decisions, similar historical backgrounds are a useful experience in choosing a treatment plan.
11. The resemblance calculation formula is planned to compare patient's healthcare data to choose similar patients from Cloud Storage and Multiple Tenants Access Control Sphygmomanometer Blood-glucose Meter Electrocardiograph Clinic Path Mining Tenant Database Shared Database is Standard Clinic Path Support Systems.
12. Clinic Decision Support Systems Diagnosis and Treats the patients of Semi-structured Data, Structured Data, Personal Healthcare Data, Open Life Data Instance Mapping Healthcare Data Annotation Healthcare Data Analysis Hospitals and Healthcare Agencies Similar Historic Cases of Cloud-MHMS.
13. Through the previous data mobile use to informs the doctor or patients about his prescriptions, and also alerts about the upcoming problems.
14. If incorrect data is found, patients can be notified to take appropriate action, with the services of a medical service, such as ambulances or specialized care.

SUMMARY

It is proposed to develop an M-healthcare system that monitors and audits patient and doctor data based on trust. A thorough literature research is discussed in order to determine the current condition of domain and existing system. The disadvantages of the current system are briefly discussed in this paper. To develop, assess, and update trust, a trust evaluation method and mechanism is used. The patient can use the mobile phone to access his/her at any time any location. All entities' trustworthiness is audited using the PMAS module. The proposed system will improves efficiency and accuracy of mobile healthcare system. It also makes a communication between patient and doctors effectively. In future authors would like implement the proposed system to prove its efficiency and accuracy.

REFERENCES

[1] Salah T Alshammari, Aiiad Albeshri and Khalid Alsubhi, "A High-Reliability Trust Management System in Cloud Computing", [A Textbook] **2021**

[2] H Y Lam Y.M Tang Valeria Tang C H Wu, "An Intelligent M-Healthcare System for Improving the Service Quality in Domestic Care Industry", *International Federation of Automatic Control* ,2021. Science Direct 2020 Volume 53, Issue 2, doi: 10.1016/j.ifacol.2020.12.2113

[3] Praveen S Challagidad, Mahantesh N.Birje, "Multi-dimensional dynamic trust evaluation scheme for cloud environment", Journal of Computers and Security, Elsevier.2020 Volume 91 doi:10.1016/j.cose.2020.101722

[4] Zara Hamid , Adnan Akhunzada; Wadood Abdul, Sanaa Ghouzali ,"Trust and Reputation Management in Healthcare Systems: Taxonomy, Requirements and Open Issues*", IEEE Translations and content mining are permitted for academic research,* IEEE XPlore **2018** 17246 – 17263 doi:10.1109/ACCESS.2018.2810337

[5**]** Fayez Alqahtani Zafer Al-Makhadmeh Amr Tolba, "TBM: A Trust-based monitoring security scheme to improve the service authentication in the Internet of Things communications", *Journal of Computer Communication* (2020) Science Direct **2020 Volume** 25 , 216-225 Doi: 10.1016/j.comcom.2019.11.030

[6] Rong Jiang, Yang Xin, Huiping Cheng, and Wenxuan Wu, "T-RBAC Model Based on Two-Dimensional Dynamic Trust Evaluation under Medical Big Data", *Journal of Wireless Communications and Mobile Computing*. Hindawi **2021** Volume 2021 Article ID 9957214 Doi:10.1155/2021/9957214

[7] Z. Faizal khan and Sultan Refa Alotaibi "Applications of Artificial Intelligence and Big Data Analytics in m-Health: A Healthcare System Perspective", Journal of Healthcare Engineering Hindwi 2020 Volume 2020 Article ID https://doi.org/10.1155/2020/8894694

[8] Roman Lewandowski, Anatoliy G. Goncharuk & Giuseppe T. Cirella, "Restoring patient trust in healthcare: medical information impact case study in Poland", *National center of Biotechnology institution* **2021** 21(1):865 doi:10.1186/s12913-021-06879-2

[9] Mohamed Firdhous, Osman Ghazali, Suhaidi Hassan", Trust Management in Cloud Computing: A Critical Review" , *International Journal on Advances in ICT for Emerging Regions (ICTer)* **2018** vol. 04, no. 02, pp. 24-36

[10] Isma Masood, Yongli Wang,Ali Daud,Naif Radi Aljohani, and Hassan Dawood,"Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure" *Wireless Communications and Mobile Computing* .Hindawi **2018** Volume 2018 Article ID 2143897 doi:10.1155/2018/2143897

[11] WenjuanFan ,HarryPerros ,"A novel trust management framework for multi-cloud environments based on trust service providers", *Journal of Knowledge Based system* ScienceDirect **2018** Volume 70, Pages 392-406 Doi:10.1016/j.knosys.2014.07.018

[12] Lileilu Yuyu Yuan, "A novel TOPSIS evaluation scheme for cloud service trustworthiness combining objective and subjective aspects", *The Journal of System Software* Science Direct **2018** Volume 143, Pages 71-86 doi:10.1016/j.jss.2018.05.004

[13] Wided Ben Daoud, Amel Meddeb-Makhlouf, Faouzi Zarai, "Trust based Access control Scheme for e-health cloud",[A TextBook] 2018 doi: 10.1109/AICCSA.2018.8612786

[14] Zainab M. Aljazzaf , Miriam A.M. Capretz , Mark Perry, "Trust Based Services Oriented Architecture", *Journal of King Saud University – Computer and Information Sciences.* ScienceDirect **2018 ,** 470–480 Doi:10.1016/j.jksuci.2015.12.003

[15] Muhammad Imran Saleem , Abdul Moid Khan, Shaheena Noor , and Muhammad Aamir, "Framework Smart E-Health Monitoring System", *Indian Journal of Science and Technology*. Google Scholar 2017, Vol 10(29), DOI: 10.17485/ijst/2017/v10i29/117323

[16] M. N. Birje, P. S. Challagidad, M. T. Tapale, R. H. Goudar" , Security Issue and Countermeasures in Cloud Computing", *International journal of scientific & technology research volume 4, issue 11,*2017 ISSN 2277-8616.

[17] Matin Chiregi, Nima Jafari Navimipou, "Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms", *Journal of Electrical Systems and Information Technology* 2018 Elsevier Volume 5, issue 3Pages 608-622 Doi: https://doi.org/10.1016/j.jesit.2017.09.001

[18] Hoang T. Dinh, Chonho Lee, Dusit Niyato and Ping Wang, "A Survey of MCC Architecture, Application, and Approaches",*Wireless communication and mobile computing* **2011** Doi: 1002/wcw.1203

[19] Hanen Jemal, Zied Kechaou, Mounir Ben Ayed, Adel M. Alimi, "Cloud computing and mobile devices system for healthcare application", *International Symposium on Technology and Society (ISTAS),* IEEE Xplore **2015** doi: 10.1109/ISTAS.2015.7439407 ISBN: 978-1-4799-8283-7

[20] Praveen S. Challagidad, Vani S. Reshmi , Mahantesh N. Birje ,"Reputation based Trust in Cloud Computing", *Internet of s and Cloud Computing,* vol. 5(5-1), pp. 5-12, **2017.** doi: 10.11648/j.iotcc.s.2017050501.12