SMART HEALTHCARE DATA TO IMPROVE THE EFFICIENCY USING CLOUD COMPUTING FRAMEWORK

Abstract

Cloud computing technologies have developed the healthcare sector in recent years. It consists of on-demand services for storage, computing power, servers, networking, applications, and various other IT resources that are based on the Internet. A number of privacy and security issues, such as authentication, authorization, inference manage, controls over access, confidentiality of information, cloud-based medical data abuse, and integrity, are brought up by the transition from offline to online computing as medical technology progresses. A trustworthy and effective security and data protection solution is therefore needed for a cloud-based e-healthcare system. As a result, the data's trustworthiness and secrecy are maintained by this structure of protection. It also makes sure that only those who have been given permission can view their individual medical records. In addition, privacy issues are resolved and a safe healthcare system is maintained. This system protects against inference attacks on the sensitive data. The system also speeds up response times, stores patient profiles, and helps patients make the best medical decisions.

Keywords: Cloud Computing, E-Healthcare management system, Electronic Health Records.

Authors

Dr. D. Naga Ravikiran
Professor
Department of ECE
Chalapathi Institute of Technology
Guntur, Andhra Pradesh, India.

Dr. Neelima Guntupalli,
Assistant Professor
Department of CSE
Acharya Nagarjuna University
Guntur, Andhra Pradesh, India.

Dr. Vasantha Rudramalla,
Faculty
Department of CSE
Acharya Nagarjuna University
Guntur, Andhra Pradesh, India.

Sai Srinivasvellela
Assistant Professor
Department of CSE-Data Science
Chalapathi Institute of Technology
Guntur, AP, India.

I. INTRODUCTION

The greatest approaches to improve the standard, performance, and responsiveness of healthcare systems are always being searched for by health ministry's all over the world. To communicate social organization to patients and administrators over the worldwide, the protection of social organization goes through a substantial improvement.

In daily life, the importance of information and communication technologies (ICT) has increased, and changing from conventional to innovative methods of healthcare would speed up response times, permit users to manage their own health care needs, and decrease the burden on healthcare facilities [1].

Healthcare information systems enable healthcare providers and patients to gain new insights from and use healthcare data [2].The use of health care information system addresses many current medical issues. It is predicted to decrease costs and improve service levels by allowing health care providers to share information, identify faster diagnosis and treatments, and eliminate unneeded testing and doctor visits by allowing "self-service" appointments or medication instances.

The demand in cloud computing has recently developed quickly to provide healthcare organizations with alternatives for achieving a combination between high operational improvement potential and inexpensive IT systems [3]. The two main components of health services are MHRs (Medical Health Records) and EHRs (Electronic Health Records) [4]. However, the main benefit of EHR is that it maintains patient health data electronically. Several security and privacy mechanisms, including password security, request setsize limits, interpretation control techniques, privacy-preserving techniques, and others, are created to secure the information. However, because of a number of security needs, current security solutions are not appropriate for electronic medical care services, data sensitivity and limited control over remotely information stored. To protect the confidentiality of information, the healthcare organization does not publish any of its data in the cloud with any identifiers still present, such as address, SSN, and name, etc. However, removing all characteristics from the data alone does not guarantee complete privacy.

Data storage is secured and protected to some extent by Data Base Management Systems (DBMS). However, DBMS by themselves cannot ensure personal privacy. It mainly offers ways to secure data through access control. Network attacks and inference threats on cloud-based healthcare data can damage individual privacy. In these kind of attacks, the attacker acts as a legitimate user and sends several authorization questions to infer sensitive information beyond its privileges. Recent advancements in e-health can be characterised as the use of information and communication technology in healthcare organisations. It is an undeniable fact that using the internet to store, access, and modify healthcare data as well as automate many processes and operations that are essential stages to achieving e-health. The advantages of e-health in this context include an increase in service quality in elderly societies, a decrease in cost and medical errors, and convenience of shifting data to the appropriate area. However, lack of adequate technology for preventative care, difficulty collecting and storing medical data, and difficulty transforming paper-based records are all potential challenges.

A wide range of applications and services, such as patient monitoring and emergency response, are predicted to be supported by mobile health care technologies, following the emergence of a pervasive computer architecture. However, they concurrently provide a number of difficulties, including problems with data management and storage, interoperability, resource availability, and universal access. The term "pervasive cloud healthcare" refers to an emerging model in the medical field that uses computing in the cloud to treat, manage, and monitoring patients [5]. Algorithms, cloud infrastructures, smart houses, products, and sensors all contribute to the systems in different ways, and they launch various service kinds based on the context and surroundings in which they are utilized. Currently, many hospitals and healthcare systems still save their records on paper copies, which can lead to information loss and make it difficult for doctors and patients to manage. To minimize this effect, a new movement known as cloud computing is quickly growing rapidly in healthcare [6]. With the help of this trend, users can store large amounts of data secure in the cloud. By allowing users to access their data from any location and at any time, it also improves user productivity and eases the pressure on patients and doctors who must perform data analysis. In order to confirm the user's identity and improve the privacy of the patient's information, the user authentication method is used.

The analyses remaining sections are organised as follows: In Section II, a review of the literature is provided, In Section III introduces the designing of Smart healthcare system based on cloud computing. Section IV discusses the result analysis. Finally, Section V introduces the analysis and future works to a conclusion.

II. LITERATURE SURVEY

Quazi Mamun and Muhammad Rana et al. [7] the current authentication issues with healthcare data are addressed by a strong authentication paradigm utilising cryptographic approaches. The right of patients to control their health information is accorded significant attention.

Vincent Micheal Kiberu et. al. [8] The E-health readiness assessment frameworks (EHRAFs) for developing nations are the result of an analysis of previous research, with the EHRAFs being modified for local use, and The major objectives of this study were to assess E-Health security in relation to the implementation of telemedicine services in health services provided by public organisations in Uganda. A systematic search of conference proceedings and peer reviewed literature was carried out. For the purpose of gathering data, qualitative and quantitative approaches will be utilized. Screenshots of EpiData will be used to record and export quantitative data to Stata13. Nvivo software will be used to transcribed qualitative data.

Tania Basso, Regina Moraes, Roberta Matsunaga, and Nuno Antunes et. al. [9] utilized a data perturbation model to provide random noise to the physical data to decrease the risk of connection and inference attacks.

Muhamed Turkanovic, and Tatjana Welzer Druzovec, Marko Holbl et al.[10] addressed many forms of inference attacks and their defences to protect the confidentiality of statistics databases. The explored strategy in this approach demonstrates that access control mechanisms alone are insufficient to protect data against indirect access.

Yingjuan Shi, Hui Wang, Gejian Ding, H. Eduardo Roman, Si Lu et. al. [11] explains fog computing's properties, potential applications in the healthcare system, and services it can provide. Fog computing, which is based on edge servers, is thought to having a sophisticated design that divides insufficient computing, storing, and a standard cloud computing data center's end-to-end networking capabilities. It gives end devices logical intelligence and filters data for data centres. In latency-sensitive Internet of Things (IoT) applications, such as healthcare, low and constant latency is a key goal in fog computing.

A Basem, K DAEHAN and B Manaf et. al. [12] While having given providers of telemedicine access to the smart ambulance system model known as the E-Ambulance, which monitors patients health, the work has a security limitation. The solution advised that data be stored in databases and maintained on dedicated servers, an MCCEH approach that might be problematic for sensitive data that can be compromised or exploited because dedicated servers have physical access to it rather than physical hardware. Address the challenges associated with a "virtual" cloud environment maintained by a cloud dedicated server.

Lamia Chaari Fourati et. al. [13] focus on the healthcare monitoring system (HMS) design, the development of wireless technologies (supporting infrastructure and technology), and the wireless body area network (WBAN), and the PHY, MAC, and routing layers as well as security, mobility, and patient location) (services) design difficulties related to WBAN. This method may also be seen as a complete technical review of the most current advancements in WBAN and HMS state-of-the-art.

Y Kumar Jain and Santosh Kumar Bhandare et. al. [14] analyzed the data mining approach's need for data privacy protection. After analysis, they discovered that perturbation is the most effective privacy protection method for preventing data leaking. Therefore, they suggested a perturbation strategy based on min-max normalization to randomize the data.

Jie Wang and Jun Zhang et al. [15] In order to overcome the privacy concerns with data mining techniques, matrix factorization was taken into consideration. The suggested adaptable and effective method for maintaining privacy in centralized datasets performs effectively.

III. SMART HEALTHCARE DATA TO IMPROVE THE EFFICIENCY OF CLOUD COMPUTING FRAMEWORK

The block diagram of Smart healthcare data for improve the efficiency of Cloud Computing Framework is represented in below Fig.1.

There is a communication flow at the administrative level of a healthcare provider where the administration gathers patient information to give the proper follow-up examination (such specialized medical services and examinations) and relevant papers for a variety of activities (such as billing).

The second portion specifies the generic rule-set. Customers of the framework can access a healthcare databases both registered and unregistered users, a data perturbation sections, an electronic health record manager, an electronic health record supplier, a rule-set providers, and query validates. Figure 1 shows the organization of all these elements. Users can be classified as either registered or unregistered. To login, registered users must enter their credentials. Users who are not registered can log in as guests without providing any credentials.

When a user accesses the healthcare cloud, the following actions are carried out.

1. The user is initially authenticated by the intermediate layer EHR provider.
2. Following successful authentication, the user can send the query to the EHR providers. The user's query is verified by the Query Validator before being sent to the EHR managers.
3. The data is sent from the EHR management to the data modification module after retrieving it from the EHR database in accordance with the requested information.
4. The data modification module randomly generates the outcomes from Algorithm 1's calculations.
5. The search query results are shown to the user in line with the rule sets that the rule-set manager has given. Whenever the query index (query number) is odd, the randomised query results in this technique equal the product of an orthonormal matrices and the initial result matrices.

This architecture provides several benefits due to the use of the cloud, including accessibility, flexibility, globalization, cost savings, etc. The main goal is to build a cloud-based patient management system that can be accessible at any time and from any location of utilizing cloud computing in our framework. Public cloud like GoogleApp-Engine as cloud infrastructure. The design now provides several benefits due to the utilization of the cloud, including cost savings, accessibility, flexibility, and globalization.

The electronic health records that patients referrals to medical facilities create. The necessary data, medical tests, and documentation are gathered and entered into computer programmes. At that particular centre, doctors, patients, and experts have access to health information. They added that the major and significant infrastructure is e-health records, which all health centres and hospitals can access when necessary. The information can be accessed to both patients as well as relatives. As the doctors can know about patient information in an emergency situation.

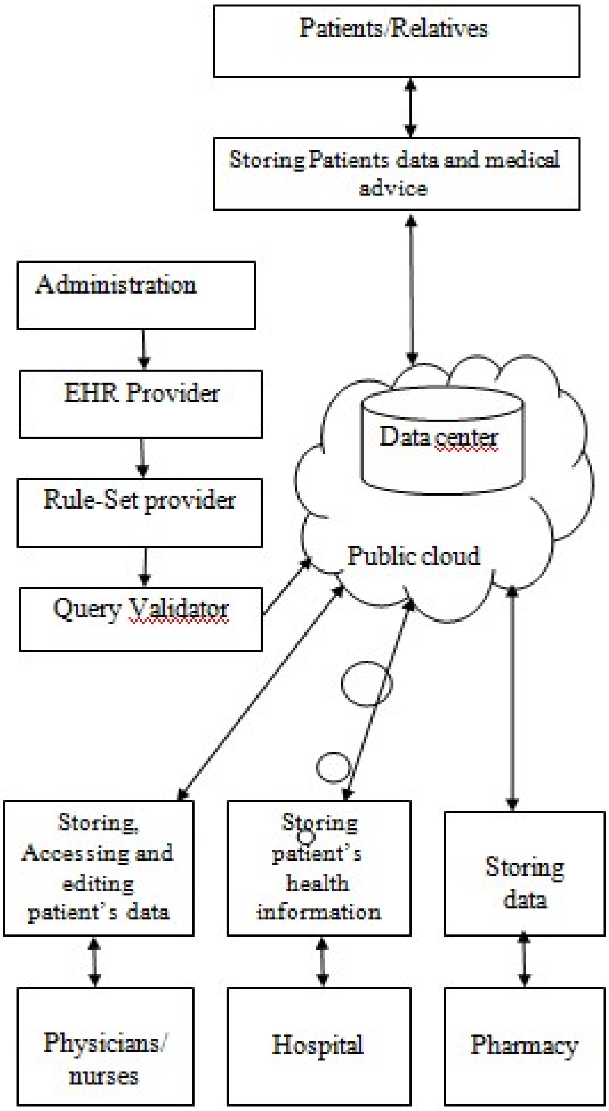

Figure 1: Block Diagram of Smart Healthcare Data to Improve the Efficiency Using Cloud Computing Framework

Whenever a physician or specialist needs to access any e-HR of a patient, it is assumed that the patient is in session. The doctor then downloads the matching encrypted file to his local computer from the server. Then he can decrypt locally only with the help of the key provided by the patient. The relevant portion of the profile is encrypted locally on the doctor's computer if the doctor needs to update the EHR at the end of the session. The most crucial role is for administrators to monitor, maintain, and maintain the complete E-Healthcare database, which is a difficult process.

The app displays the data that is gathered from the medical box. It's necessary to save the information in the cloud. The information from the mobile device is transmitted to the application server and stored in the cloud while being encrypted. All three components doctor, pharmacist, and clients access the patient information that is stored in the cloud. Utilizing GSM (Google Cloud Messaging) through HTTP before storing the actual servers. This message will be delivered to the GCM Application Server, which then forwards it to the Google Cloud Messaging Server.

The application provides a level of synchronization and updates for all of the above mentioned end users. The app is connected to the cloud and its data is taken. The local table is constructed and updated once the data has been collected. The local database has been updated. As a result, reading, updating, and deleting the data is simple. The patient, doctor, and pharmacy all utilize the same method to update and show information on their respective devices. To entirely device-independent the procedure, a common ID is given to all three. Each participant should enter their appropriate spaces: the doctor, the patient, and the pharmacist. When they first log in, they will be prompted to create an account using their email address, and further authorization will be provided by a recognized hospital.

The patient will get a list of the medications that are available. The medication that is available in limited amounts is highlighted. The patient can then request the medication from the pharmacy and have it filled if there aren’t sufficient resources. This approach provides the opportunity for the creation of supports that will help people follow their medical programs correctly and experience successful recovery. Additionally, since the medications will be taken on time, the recovery process will go more quickly. Additionally, the doctor, patient, and pharmacists can easily interact related to this approach, which makes the recovery process much simpler.

IV. RESULT ANALYSIS

In this analysis, the system’s implementation is explained. Health information and other data about the patient are extremely private. Due to the serious consequences of data tampering or leakage brought on by hacked infrastructure, security in mobile healthcare networks is of the greatest importance. After entering his username and password to log in, the administrator can access the E-health record management system’s home page. Security and resource provisioning are essential components of an E-healthcare service. Users must first register on the website with their information. The password for their authentication procedure needs to be created. After successfully registering, the user must login to view or access their information. After entering the password, a One Time Password (OTP) request was made and delivered to the user’s email address. The customer can access their specific module by logging in with the help of OTP.

The admin will be in charge of the securely stored medical data on the cloud. Different security levels are used when outsourcing secure information to the cloud. The security and management stage is continuously under the admin’s watch. In the security stage, user authentication was put into place. Whereas data can be requested and accessed from the user side. Security and resource provisioning are critical elements of an e-healthcare service. Monitoring, organising, and managing the complete E-Healthcare database is the most important responsibility, and the administrator is in charge of this tedious task.

Service Oriented Architecture is used in the current framework to create multiple services that people can use to store and access their information. However, security is a major problem. This framework uses the cloud to provide a range of services that improve user productivity and security.

The platform utilizes Advanced Encryption Standard (AES) based e-health technologies and retrieves the result to each query. In the largest table, 31 different questions were run on lab observations. Each query produced a unique set of fields, each with a varied number and size. This allows us to evaluate the performance of the methods on the cloud platform by monitoring the computation time of the methods for each field retrieved from the database. In regards to security and the outcomes of all the questions below, cloud-based healthcare performs better than traditional healthcare.

Fig. 2 shows security Comparison standard health care and cloud based health care with various thresholds. X-axis shows classification and Y-axis represents percentage (%). The cloud based health care has a high efficiency.

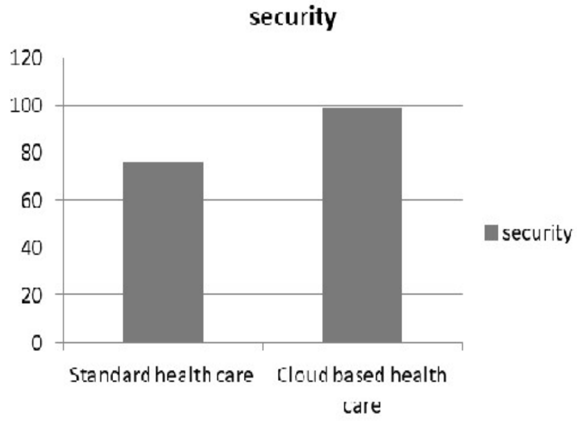

Figure 2: Security Comparison Graph

The Fig. 3 shows the time comparison of standard health care and cloud based health care. The cloud based health care takes less time for query compared to standard health care data. The Y-axis represents the time in ms (milliseconds) and X-axis represents the health care.

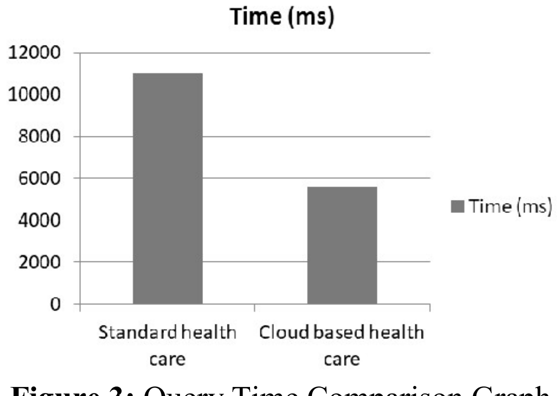

Figure 3: Query Time Comparison Graph

Consequently, based on the findings, the framework may address various problems related to remote patient monitoring, routine checkups, offering a suitable individual plan, and providing access to patient information for specific individuals such as doctors, nurses, and family members.

V. CONCLUSION

In this analysis, smart health care data for improve the efficiency of cloud computing framework is described and analyzed. This is essential to develop a robust healthcare system that can handle emergencies and support medical care. This evaluation concentrated on the structure of Secure EHealthcare and Security; entire patient information has to be maintained on a centralized database server. A framework that provided all the patient-specific information to the documents and themselves is made possible by the distributed computing configuration, which can be used anytime, anywhere. To organise the development of E-Healthcare services for outsourcing enormous data to the cloud environment, the government provides a number of benefits. A user-based authentication system has been implemented to improve the accuracy of data creation for the division of medical services and to provide security to various clients. Smart health care data has a faster response time than AES encryption. A user-based authentication system has been implemented to improve the accuracy of data creation for the division of medical services.

REFERENCES

[1] Rima Sermontyte-Baniule, Asta Pundzien, “Value-capture capabilities in value-based digital healthcare performance”, 2021 IEEE International Conference on Technology and Entrepreneurship (ICTE), Year: 2021

[2] Hudiarto Sukarman, Fathan Yunicha Rizkiyana, Apriyanto, Muhammad Farhan Al Farizi, “The Design of information system and Technology Strategy for Improving Performance of healthcare Service With EA3 Framework: (Case Study: Summit)”, 2020 International Conference on information Management and Technology (ICIMTech), Year: 2020

[3] Wei Li, Bonnie M. Liu, Dongxi Liu, Ren Ping Liu, Peishun Wang, Shoushan Luo, Wei Ni, “Unified Fine-Grained Access Control for Personal health records in cloud computing ”, IEEE Journal of Biomedical and health Informatics, Volume: 23, Issue: 3, Year: 2019

[4] Varun Shukla, Arpit Mishra, Anchal Yadav, “An Authenticated and Secure Electronic Health Record System”, 2019 IEEE Conference on Information and Communication Technology, Year: 2019

[5] Sagar Sharma, Keke Chen, Amit Sheth, “Toward Practical Privacy-Preserving Analytics for IoT and cloud based healthcare system”, IEEE Internet Computing, Volume: 22, Issue: 2, Year: 2018

[6] Chang L. Kim, “Managing Environments for healthcare Information systems Using Enterprise Application Integration”, 2017 IEEE International Conference on healthcare Informatics (ICHI), Year: 2017

[7] Quazi Mamun and Muhammad Rana. “A robust authentication model using multi-channel communication for ehealth systems to enhance privacy and security”. In Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2017 8th IEEE Annual, pages 255–260. IEEE, 2017.

[8] [8] Vincent Micheal Kiberu, “E-Health Readiness Assessment in Uganda: Integration of Telemedicine Services into Public Healthcare System”, 2016 IEEE International Conference on Healthcare Informatics (ICHI), Year: 2016

[9] Tania Basso, Roberta Matsunaga, Regina Moraes, and Nuno Antunes. “Challenges on anonymity, privacy, and big data”. In Dependable Computing (LADC), 2016 Seventh Latin-American Symposium on, pages 164– 171. IEEE, 2016.

[10] Muhamed Turkanovic, Tatjana Welzer Druzovec, and Marko Holbl. ¨ Inference attacks and control on database structures. TEM Journal, 4(1):3, 2015.

[11] Yingjuan Shi, Gejian Ding, Hui Wang, H. Eduardo Roman;Si Lu, “The fog computing service for healthcare”, 2015 2nd International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech), Year: 2015

[12] Basem A ,DAEHAN K and Manaf B , “E-AMBULANCE: Real-Time Integration Platform for Heterogeneous Medical Telemetry System” , Procedia Computer Science ,Volume 63, 2015.

[13] Lamia Chaari Fourati, “Wireless Body Area Network and Healthcare Monitoring System”, 2014 IEEE International Conference on Healthcare Informatics, Year: 2014

[14] Y Kumar Jain and Santosh Kumar Bhandare. “Min max normalization based data perturbation method for privacy protection”. International Journal of Computer & Communication Technology, 2(8):45–50, 2011.

[15] Jie Wang and Jun Zhang. “Addressing accuracy issues in privacy preserving data mining through matrix factorization”. In Intelligence and Security Informatics, 2007 IEEE, pages 217–220. IEEE, 2007.