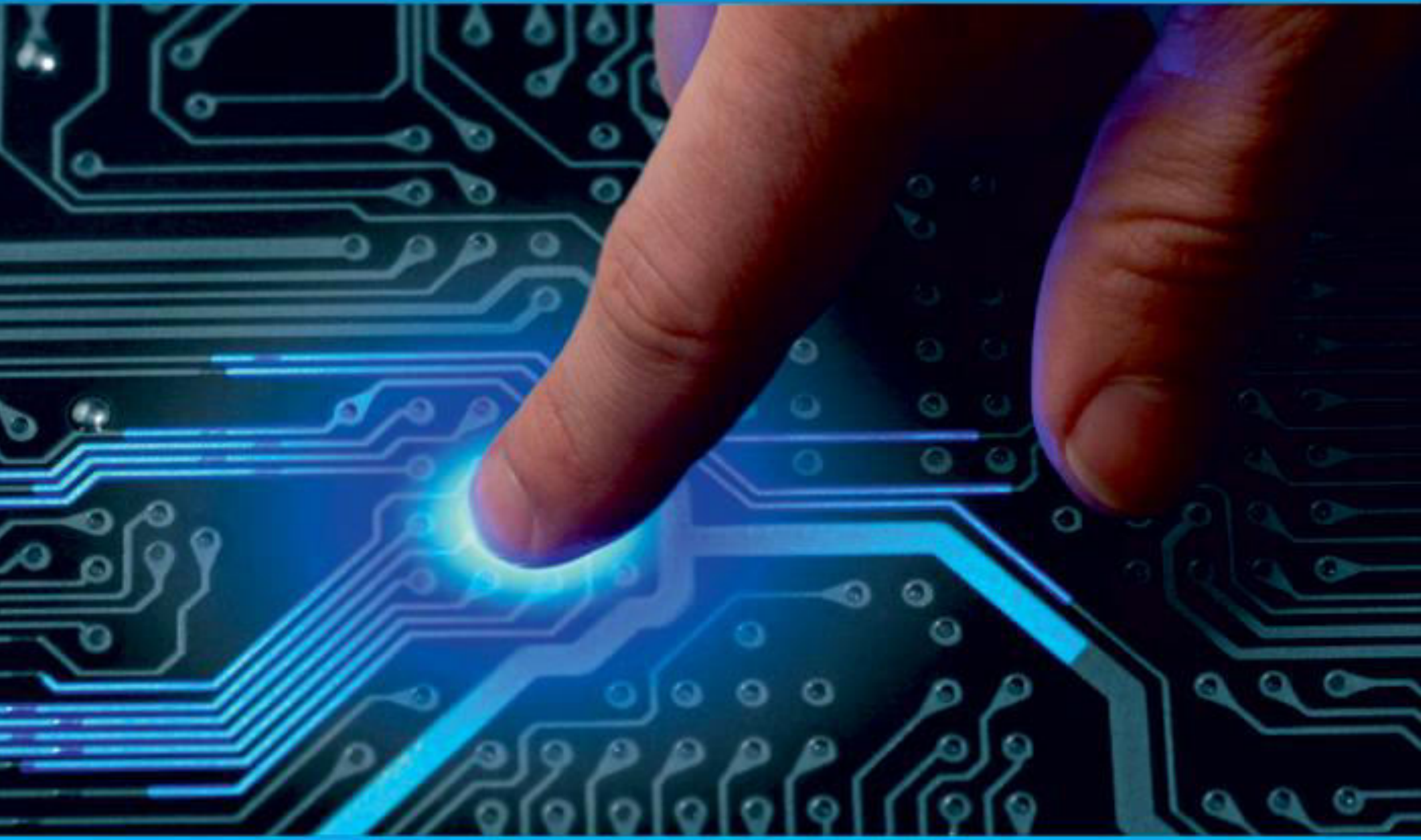
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 12, December 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

☐ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com @ www.ijircce.com

| DOI: 10.15680/IJIRCCE.2021.0912034 |

Secure Searching of Medical IOT Data over Cloud Platform

Taware Priti[1], Shendage Monika[2], Shinde Dhanashree[3], Jaheda Parveen[4], Prof. S.K. Shinde[5]

B.E Student, Department of Computer Engineering, K J College of Engineering & Management Research, Pune, Maharashtra, India [1,2,3,4]

Professor, Department of Computer Engineering, K J College of Engineering & Management Research, Pune, Maharashtra, India[5]

ABSTRACT: Although the digital revolution in the healthcare industry began relativelyearly, it has progressed more sluggishly than in other industries. Medical care becameamong of the centres of individual, economic, and even societal concern as research,innovation, and the commerce have advanced rapidly. The conventional healthcare approach includes flaws including such difficulties in visiting a physician, high cost oftreatment, and the obfuscation of health data. Nevertheless, with the explicit advent ofinternet of Things notion, the IoT implementation sector has already been integrated inall facets of today's Internet of Everything period. The Internet of Medical Things is the consolidated manifestation of IoT connectivity in the hospital context, as well as the heartof healthcare technological revolution. The data being collected from these devicesneeds to be stored securely to achieve privacy and security for the individuals. With theincreased number of patients and the popularization of the remote diagnosis approach, the cloud platform has been one of the most innovative paradigms that can be a valuable addition. Therefore, an effective mechanism for the purpose of achieving secure storageof medical IoT data on the cloud and providing an effective searching mechanism on theencrypted data. This approach will be further elaborated in the upcoming editions of this research

KEYWORDS: Internet of Medical Things, Public Cloud, Medical Health Records, Cryptography, Search over encrypted data

I. INTRODUCTION

A physician's connection with his customer has not been as strained as it is now. The physician was essentially concerned with the ailment and was uninterested in the person's medical background. After all course, whenever a family is only ever seen by the very same doctors, connections are formed, enabling the doctor to recognize the nature of his affected person and therefore recall his numerous therapies, permitting him to skip repeating the same things over and over. More or less every physician worked with his own style, and since he did not have a vivid recollection, he had to sit down and write his appointments. However, if the customer switches doctors, he will have to commence again, and the doctor will be unable to avoid gathering information in order to determine the condition through which the patient is experiencing, particularly if the patient has multiple ailments being treated by various experts. In alternative terms, during every consultation, the physician's impressions were not routinely documented, and even if they had been, these just cannot be disclosed. However, the rapid advancement of medical research has exacerbated concerns of integrity, openness, and responsibility between patients and healthcare professionals. Visitation transparency has now become a need, and this issue is now represented in the maintaining of a medical record. The health history has evolved into a significant instrument for doctors. It is currently part of the medical ecosystem in several nations and is controlled by quite tight legislative regulations. It piques people's attention even more because it deals with lengthy therapeutic interventions, neurodegenerative conditions, in-depth exams, and sometimes even surgical operations. It is critical in the hospitals since it is designed to give professionals who do not recognize the patients a description of his intimate condition as well as the diseases to which he has been susceptible. This preserves time and prevents incorrect therapies from being prescribed. The health history is a working resource for physicians that enables them to obtain information about their patients' condition and then use it throughout their treatment. The knowledge included in the medical record has progressively proved vital, and all specialists who tend to a client have automatically incorporated it into the healthcare service. As a result, the gathering of data and the regulations for its transfer had to be formalized. Health data must be differentiated from the channel via which it is delivered, i.e. the organization and contents. Medical data is gathered from a multitude of outlets, including test findings, interviews, and supplementary assessment results, such as a Computed tomography report and illustrations. The most common channel for providing data is still a printed page. However, it is becoming increasingly and lesser widespread, and it is increasingly being replaced by information systems. Although it is evident that the physical document materializes health information and provides for its accountability, technology advances and the rapid expansion of the Internet have rendered it feasible to be independent of the physical archive without compromising the information or its record keeping. The tendency is increasing digitalization, and the file format varies according on the specific medical interaction, such as hospitalization, counselling, and so on. The abandoning of the paper medium, which is rapidlybeing replaced by the computer medium, has influenced public health policy in many developed nations, which support the transfer of medical data to smartphones. In truth, today's cell phone is utilized for more than only conversation and brief message exchange. Videos, music, Internet surfing, email, and other new applications have emerged. The widespread availability of smartphones with big interactive displays has sparked fresh curiosity, particularly in a larger perspective of the health record. The growth of networking has resulted in a profusion of smartphones and tablets services, several of which enables users to create their own health records and deliver information to the clinician of their choosing. Whenever necessary, the clinician might add to it and try sharing it. The client may then encourage everyone involved to participate by, for instance, enhancing it throughout medical appointments. The use of modern IT solutions has accelerated the growth of the healthcare business. Conventional equipment is being phased out in favour of sophisticated technology in order to change healthcare institutions. Medical records, IoT devices, sensor systems, novel machinery, and smart gadgets are all being used to modernize healthcare providers. All of major changes in the healthcare industry create a massive amount of data. These statistics are extremely beneficial to the healthcare business. By keeping and analysing collected information, the healthcare sector may avoid some serious diseases, improve patient health monitoring, and deliver cost-effective services. Sophisticated imaging systems such as single-photon emission computed tomography, positron emission tomography, radioactive medicine functional imaging, thermography, tactile imaging, 3D imaging magnetic resonance imaging, and others are extremely important in providing healthcare. The inclusion of a variety of different sensors for IoT medical data and the combination of the cloud service is a useful improvement. This literature survey paper segregates the section 2 for the evaluation of the past work in the configuration of a literature survey, and finally, section 3 provides the conclusion and the future work

II. RELATED WORK

D. Jutla et al. express worries about the condition of the cloud environment, which has been developing at an exponential rate, raising issues about the privacy of data held on the cloud. The researchers devised a method for maintaining the cloud's and data's privacy, as well as providing master management to the cloud to aid in the maintenance of appropriate data in a Big Data environment. This system has seven components that work together to keep the system's privacy safe. The increased spatial and temporal complexity of this method is one disadvantage. According to S. Wang, there has been tremendous growth in the industry of big data and data mining over the last several years. Because most individuals congregate in groups in a specific area, the authors offer a method for utilizing huge location data as a way of delivering detection of illegal behaviours and targeted marketing. Therefore, the authors created a mechanism for analysing large amounts of location data while also protecting the user's privacy. As more enterprises and people utilize this very handy service, X. Shi elaborates on the expanding popularity of the cloud computing sector. However, when they relinquish control of their data, the cloud's security becomes increasingly critical. The most frequent method for keeping data safe is to encrypt it, however, this renders the data unsearchable [3]. As a result, the authors created a fuzzy-based searching strategy that protects the data's privacy. One of the technique's flaws appears to be its inability to handle unencrypted search operations'. Navuluri describes an innovative method for preserving privacy in a huge data warehouse. Therefore, there has been a rise in the number of major organizations collecting data to gain a better.understanding of trends [4]. Because much of this data might contain personal data about users, which could be harmful if leaked, the authors devised a mechanism that safeguards the data's privacy while simultaneously assisting in its analysis for search and retrieval. The temporal complexity of this procedure is relatively significant, which is a disadvantage. P. Sreekumari elaborates on an approach for searching and retrieving data from an encrypted cloud in an efficient and privacy-preserving manner. The authors create a fuzzy technique for searching to get sensitive data without compromising security [5]. One of the system's major flaws is the absence of key factors that characterize the status of cloud data, such as verifiability, security, and efficiency. In a Big Data context, S. Lighari et al. provide a revolutionary way to security analysis and management. Large organizations create a huge amount of data in the form of log files, Pac files, DNS logs, and other types of data, which are often kept in a data warehouse. Every day, a vast quantity of data is created, which builds up in storage and becomes massive in size [6]. Because this vast quantity of data cannot be handled, posing a significant security risk to the company, the authors devise a strategy based on Apache Spark for data analysis and management. The mobile application presented by SihemSouiki et al. allows users to improve their medical records by adding documents gathered on paper from healthcare experts. It simplifies the maintenance of the medical file because it will only be accessed by the patient.

Furthermore, the security of the patient's medical record will be ensured by this mobile application. This security is, in fact, dependent on the Cloud, which is a relatively new notion [7]. It provides IT services as an on-demand service that may be accessed via an Internet connection. In the presented software, this security is reflected by the fact that each user has a storage space that he is the only one who can control thanks to his Google accountLanfang Sun et al. examined classical IoMT, cloud-based IoMT, and edge-based IoMT, with an emphasis on edge medical cloud data processing and telemedicine development. First, they covered the architecture of traditional IoMT and the major technologies involved, then they addressed the use of IoT technology in the medical profession and the issues that arise, and finally, provided optimization guidance [8]. On this foundation, they explored the issues with traditional IoMT and the benefits of using cloud computing to IoMT, assessed cloud computing's core technologies, and concentrated on medical cloud data security. Then, in comparison to cloud computing, the authors examined the benefits of edge computing, explored edge computing optimization, and recommended that edge cloud cooperation may reach maximum usefulness in the medical industry. Hongwei Li, Yi Yang et al. suggest two high-security dynamic searchable encryption systems. The first can accomplish not only collusion resistance between the cloud server and search users but also forward and backward confidentiality. The second one addresses the key allocation issue that is prevalent in the kNN-based searchable encryption technique. In terms of the repository, search, and update complexity, performance assessment shows that the suggested methods outperform the current works [9]. Extensive studies show that the introduced approaches are efficient in terms of storage overhead, trapdoor generation, index construction, and query. Using the Cloud Environment, B D Deebak et al. proposed an improved mutual authentication strategy for the Telecare Medical Information System (TMIS) (CE). Patient Anonymity, Health-Report Revelation, Health-Report Forgery, Report Confidentiality, and Non-Repudiation are all threats that the writers disclosed they are subject to. To maintain the security architecture's long-term sustainability, and improved authentication system has been thoroughly evaluated [10]. The experimental results reveal that the proposed protocol not only ensures security against a variety of threats but also reduces the processing costs of a cloud-based medical information infrastructure. Ronghui Cao et al. present Tri-Storage Failure Recovery System (Tri-SFRS) as an OpenStack-based architecture for constructing a multi-cloud storage infrastructure for medical IoT. It's made to connect the resources and services of many medical cloud instances, as well as provide native Open-Stack data storage and storage FR functionalities. The authors create a native resource multicloud cascading solution to solve the challenge of resource management across several medical cloud platforms. In addition, they provide an integration testing framework that fits the OpenStack community's standards for testing new storage capabilities in our multi-cloud medical system [11]. The OpenStack community can make it easier and easier to incorporate these functionalities into the official version with the introduction of the testing framework. In the personal health record, a systematic and comprehensive outsourced CP-ABE depend solution was developed by Huang Nana et al. The PHR users are logically split into two domains: personal domain (PSD) and public domain (PUD1 and PUD2). To get read access authorization in the PSD, the authors use Key-Aggregate Encryption (KAE). The outsource-able ABE approach is utilized by PUD PHR users to greatly reduce the calculative burden on both the PHR owner and users, and can also provide read or write rights depending on various domains in the PUD [12]. The proposed method on the medical cloud platform can accomplish privacy preservation, according to the security analysis of public and personal domains.

III. PROPOSED ALGORITHM

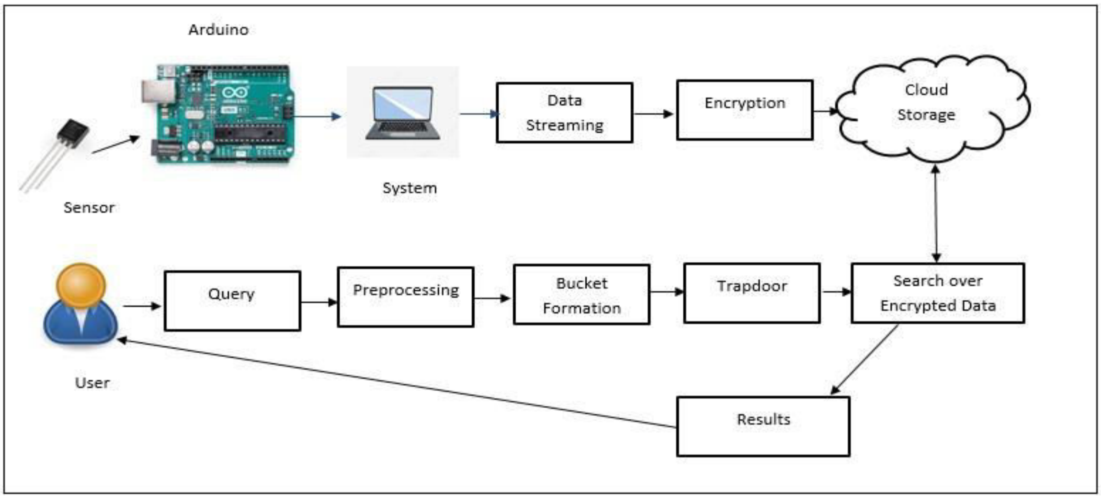


Fig 1 Proposed System

IV. CONCLUSION & FUTURE SCOPE

Despite the fact that the digitalization in medicine commenced comparatively earlier, it has moved relatively slowly than in other areas. As science, technology, and commercialization have evolved fast, medical treatment has become one of the focal points of psychological, professional, and even sociological phenomena. The traditional healthcare strategy has issues such as difficulty finding a doctor, exorbitant treatment costs, and the obscuring of health information. However, with the clear introduction of the internet of things concept, the IoT application industry has already been incorporated into all aspects of today's Internet of Everything time. The Internet of Medical Things (IoMT) is the culmination of IoT connection in the medical environment, and also the epicentre of the healthcare scientific breakthrough. To ensure safety and confidentiality for consumers, the data acquired from these gadgets must be properly maintained. The public cloud has become one of the foremost revolutionary technologies that may be a useful contribution as the percentage of patients grows and the remote diagnosing technique becomes more widespread. As a result, an efficient technique for ensuring secure cloud storage of medical. IoT data and offering an appropriate searching mechanism on the encrypted data is required. In future versions of this study, this technique will be expanded further.

REFERENCES

[1] Dawn N. Jutla and Peter Bodorik, “PAUSE: A Privacy Architecture for Heterogeneous Big Data Environments”, IEEE International Conference on Big Data (Big Data), 2015.

[2] S. Wang and R. Sinnott, “Privacy-protected Place of Activity Mining on Big Location Data”, IEEE International Conference on Big Data (BIGDATA), 2017.

[3] X. Shi and S. Hu, “Fuzzy Multi-Keyword Query on Encrypted Data in the Cloud”, 4th Intl Conf on Applied Computing and Information Technology/3rd Intl Conf on Computational.

[4] K. Navuluri, R. Mukkamala, and A. Ahmed, “Privacy-aware Big Data Warehouse Architecture”, IEEE International Congress on Big Data, 2016.

[5] P. Sreekumari, “Privacy-Preserving Keyword Search Schemes over Encrypted Cloud Data: An Extensive Analysis”, 4th IEEE International Conference on Big Data Security on Cloud, 2018.

[6] S. Lighari and D. Hussain, “Hybrid model of rule-based and clustering analysis for big data security”, First International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT), 2017.

[7] SihemSouiki et al., “M-Health Application for Managing a Patient's Medical Record based on the Cloud: Design and Implementation”, 2020 2nd International Workshop on Human-Centric Smart Environments for Health and Well-being (IHSH), DOI: 10.1109/IHSH51661.2021.9378744.

[8] Lanfang Sun, Xin Jiang, Huixia Ren, Yi Guo., “Edge-Cloud Computing and Artificial Intelligence in the Internet of Medical Things: Architecture, Technology, and Application”, DOI 10.1109/ACCESS.2020.2997831, IEEE Access.

[9] Hongwei Li, Yi Yang, Yuanshun Dai, Shui Yu, and Yong Xiang “Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data”, 2168-7161 (c) 2017 IEEE, DOI 10.1109/TCC.2017.2769645, IEEE.

[10] B D Deebak and Fadi Al-Turjman “Smart Mutual Authentication Protocol for Cloud-Based Medical Healthcare Systems Using Internet of Medical Things”, 2168-7161 (c) 2017 IEEE, DOI 10.1109/TCC.2017.2769645, IEEE.

[11] Ronghui Cao, Zhou Tang, Chubo Liu, Bharadwaj Veera Valli, “A Scalable Multi-Cloud Storage Architecture for Cloud-Supported Medical Internet of Things”, DOI 10.1109/JIOT.2019.2946296, IEEE Internet of Things Journal.

[12] Huang Nana and Yang Yuanyuan, “An Integrative and Privacy Preserving-Based Medical Cloud Platform”, 2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics, DOI: 10.1109/ICCCBDA51879.2021.9442534

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ✆ 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com