IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Analytical Survey on Cloud Medical Infrastructure Using Blockchain

[1]Shruti Chaudhari, [2]Piyush Rawool, [3]Shreyas Gawade, [4]Shreya Aralimar, [5]Snehal Thorave

[1]Student, [2] Student, [3] Student, [4] Student, [5] Guide

[1]Computer Department,
[1]Dhole Patil College of Engineering, Pune, India

Abstract: Having started particularly recently in the medical industry, the information era there has moved somewhat slowly in comparison to other sectors. As technology, invention, and entrepreneurship have moved quickly, health care has become one of the main topics of personal, political, and even economic significance. The traditional healthcare model has drawbacks, particularly challenges in seeing a doctor, excessive hospital charges, and the concealment of health information. However, the IoT deployment segment has indeed been incorporated into every aspect of the current Internet of Everything era with the intentional introduction of the internet of Things paradigm. The center of the digital age in healthcare is the Internet of Medical Things, which is the cohesive expression of IoT interconnectivity in the medical environment. To protect people's safety and confidentiality, the information captured from this equipment must be properly maintained. The public cloud has emerged as one of foremost cutting-edge technologies that could be excellent supplement with the rise in patient numbers and acceptance of the remote diagnostic strategy. In order to protect the collection of medical IoT information in the cloud and provide an information retrieval operation on the encrypted information, a system must be put in place. This methodology will be even more refined in the forthcoming versions of this research.

Index Terms - Internet of Medical Things, Public Cloud, Medical Health Records, Cryptography, Search over encrypted data.

I. INTRODUCTION

The rapid advancements in technology have improved the accuracy of human body assessment procedures. This is crucial for maintaining our health and stopping the spread of many diseases. The emergence of technological solutions to the medical industry has also brought forth a number of technical issues. It should be given priority to keeping personal patient data in a way and location that reduces the risk of theft or destruction [1]. In addition, medical professionals should have access to data so they can analyze it as needed, while anyone without the right credentials should be denied access.

Consequently, the sole adoption of digital health information transmission will have no positive impact on data transparency and will instead make medication and diagnoses more difficult. For certain research, getting the statistics and doing the evaluation can take several months. There isn't anything accessible to the naked eye when it relates to assessment. To this purpose, artificial intelligence approaches can be applied to assist healthcare providers. Especially now that equipment that perform particular examinations could communicate information and analyze it remotely thanks to the Internet of Medical Things. Healthcare systems of the future ought to be wireless, remotely approachable, and higher efficiency while also having low delay.

Reinforcement learning, machine learning, and artificial intelligence frameworks must still be able to help wireless devices make judgments even if their Internet connection is lost. Nevertheless, training these algorithms in the fields of deep learning, machine learning, and artificial intelligence on an IoT device necessitates more data samples than are typically accessible at each device in addition to the requirement to interchange data with other devices [2]. This makes it possible for an increased and improved diagnosis, which can be highly beneficial.

The relationship between a doctor and his patient has never been as fraught as it is right now. The doctor wasn't really interested in the patient's medical history and was more focused on the illness. Of course, when a family only ever sees the same doctors, linkages are made, allowing the doctor to recognize the characteristics of his patient and afterwards remember his various treatments, allowing him to avoid committing the relatively similar mistakes repeatedly.

Since almost every doctor has a different working method and they would not possess a clear memory, he would have to sit out and record down his consultations. But if the patient changes doctors, they will be required to start over, and the doctor won't be capable of accumulating information to identify the illness the patient is going through, particularly if the person has many diseases getting addressed by various specialists. In other words, the doctor's impressions were never routinely recorded during a consultation, even though they had already been, they simply couldn't be shared. However, worries about honesty, transparency, and accountability amongst patients and hospital personnel have grown as a result of the quick development of medical investigation. Transparency in visitation is now necessary, and this problem is now reflected in the keeping of a patient history.

The medical history has developed into an important tool for clinicians. Several countries presently include it in their medical ecosystems, and it is governed by very strict legal restrictions. It makes headlines in particular because it addresses protracted treatment interventions, neurological diseases, thorough examinations, and occasionally even surgical procedures. It is essential in hospitals because it is intended to provide medical professionals who are unfamiliar with the patient with a description of both his

intimate condition and the illnesses to that he is predisposed [3]. This saves time and stops the prescription of the wrong therapies. The health history is a resource that doctors can utilize to learn more about their patients' conditions and then use that knowledge to their care.

This literature review paper divides section 2 into an assessment of prior work in the form of a review of literature along with the glimpse of our model in section 3, and section 4 concludes with recommendations for future research.

II. RELATED WORKS

Bhaskara S. Egala outlines a cutting-edge technique for maintaining privacy in a sizable data warehouse. The number of significant companies gathering data to better understand patterns has increased as a result [4]. The authors developed a technique that protects the privacy of the data while also helps in its evaluation for retrieval and searching since a lot of this material may comprise sensitive user information that may be damaging if released. This approach has a comparatively high level of temporal complexity, which is a drawback.

P. Sreekumari explicates on a method for quickly and secretly accessing and obtaining information from an encrypted cloud. To obtain sensitive information without jeopardising security, the authors use a fuzzy searching technique [5]. The lack of essential components that define the condition of cloud environment, such as authenticity, confidentiality, and effectiveness, constitutes another of the system's primary weaknesses.

Chenchu Xu et al. offer an innovative approach to security management and assessment in the setting of big data. Log records, Pcap documents, DNS reports, as well as other varieties of information are produced in large quantities by large enterprises and are frequently housed in a storage facility. Massive amounts of data are produced every day, which increase in storage volume and size [6]. The authors develop a plan centered on Apache Spark enabling information evaluation and management because this enormous amount of information can indeed be managed, creating a serious security risk to the business.

Users of the mobile platform developed by Sihem Souiki et al. can enhance their health records by uploading paper documentation compiled by healthcare professionals. Due to the fact that only the patient will have access to it, maintaining the medical file is made simpler. Furthermore, this mobile application will guarantee the protection of both the patient's medical data. In actuality, the Cloud, a relatively new concept, is what this security depends on [7]. It offers on-demand IT services that may be accessed through an Internet connection. This security in the program is mirrored by the concept that every individual has a storage facility that only they can access using their Google account.

In their study of traditional IoMT, virtualized IoMT, and edge-based IoMT, Lanfang Sun et al. placed special attention on the development of telemedicine and peripheral healthcare cloud data analysis. They first discussed the standard IoMT architecture and the key technologies concerned, subsequently they talked about the usage of IoT innovation in the healthcare field and the concerns that occur, and ultimately they offered optimization advice [8]. On the basis of this, they examined the drawbacks of conventional IoMT and the advantages of adopting cloud computing for IoMT, evaluated the key technologies of cloud computing, and focused on healthcare cloud information protection. The authors then contrasted edge computing with cloud computing, looked at mobile cloud improvement, and suggested that cloud and edge collaboration could be most effective in the medical sector.

Two very secure dynamic searchable encryption techniques are recommended by Fan Yang and others. The first can provide both forward and reverse anonymity as well as collaboration resilience among the remote server and searching consumers. The second one deals with the common key allocation problem in the kNN-based accessible symmetric encryption. Performance evaluation reveals that the suggested methods perform better than the existing works in aspects of the storage, retrieval, and modification complexities [9]. The suggested methodologies are effective in regards of memory overhead, trapdoor creation, index creation, and query, according to numerous research.

Yi Ding and colleagues suggested an enhanced mutual authentication technique for something like the Telecare Medical Information System using the cloud environment. The authors acknowledged that they face dangers from customer confidentiality, wellbeing Disclosure, medical Falsification, report Transparency, and non-repudiation. An upgraded authentication system has undergone a rigorous evaluation to ensure the long-term viability of the security architecture [10]. The outcomes of the tests show that the suggested protocol not only guarantees security from a range of threats but also lowers the processing expenses of a virtualized healthcare data architecture.

Tri-Storage Failure Recovery System, a multi-cloud backup architecture for the medical IoT, is presented by Ronghui Cao et al. as an OpenStack-based design. In addition to offering native Open-Stack storage space and memory FR functions, it is needed to engage the services and features of numerous medical cloud instances. To address the issue of management systems across various medical cloud applications, the authors develop a native infrastructure multi-cloud waterfall approach. Additionally, they offer an interoperability process model for our multi-cloud healthcare system that complies with OpenStack community requirements [11]. With the advent of the testing framework, the OpenStack organization can enable it ever simpler to include these features in the official explanation.

Huang Nana et al. created an organized and thorough contracted dependent solution for the personal health record. Private domain and public's interest are the logical divisions of PHR users. Key-Aggregate Encryption is used by the authors to obtain publish access permissions. The users employ the outsource-able technique to significantly lessen the computational strain both on the PHR proprietor and customers, as well as to grant access or publish rights according to different regions in the PUD [12]. Based on the vulnerability examination of the public and private domains, the suggested solution on the healthcare virtualized environment can achieve privacy preservation.

In order to address the issue of data security throughout the retention and transmission of large volumes of medical information in 5G, cloud computing, and the Internet of Medical Things, Jing Liu [13] proposes a unique resilient watermarking algorithm. The robust medical volume data feature extraction function was created by combining human visual features and perceptual hashes with the three-dimensional double-tree discrete wavelet transform transform's strong directional discrimination and interpretation invariance. Zero steganographic and blind retrieval were made possible by applying encrypted communications and the 3rd - party idea without altering the healthcare measurements, ensuring the accuracy of clinical diagnosis and enhancing diagnostic effectiveness.

In order to protect EHRs, uphold user privacy, and reduce key abuse in systems, Peng Zeng [14] presented a partly regulation and transparent system for controlling access. The fundamental building element of the proposed cypher text policy that enables us to implement partially obscured access policy, vast universe, decoding testing, and accountability is attribute-based cryptography. In this method, the vulnerable individual elements are concealed in the cypher text while only the names of the attributes inside an access control mechanism are made public. The number of right to be provided is constant, and the attribute universe isn't necessarily constrained. This technique incorporates a cryptographic test before the final decryption in order to enable a more effective decryption procedure. Last but not least, the suggested method enables traceability by incorporating the user's identifying data within the decryptor.

In order to use the Internet of Medical Things, Dawid Poap [15] present an architecture for fusing blockchain benefits with artificial intelligence methodologies only within confidentiality collaborative training approach. The suggested concept was built on providing new means of giving artificial intelligence techniques available from which machine learning can acquire data for training and securing strength and conditioning information in the blockchain. This provides both safety for the data itself and a continuous learning and improvement mode for classifiers.

III. PROPOSED MODEL

After careful and effective analysis of the previous researches on this topic, a framework is achieved as shown in the figure given below. The approach starts through the key evaluation, if the key isn't evaluated the system reaches the stop state. Once the key is evaluated, the sensor data is collected and encrypted using RCC encryption. The Encrypted data is then used to create a blockchain which is then stored on the cloud storage. The stored data needs to be evaluated for its integrity, which is done through the use of Bit Mapping. If the integrity of the agreement is compromised then a report is generated and it reaches the stop state. On the other hand, if the agreement is not compromised, then the system reaches the stop state directly. This model is shown in the below depicted figure 1.

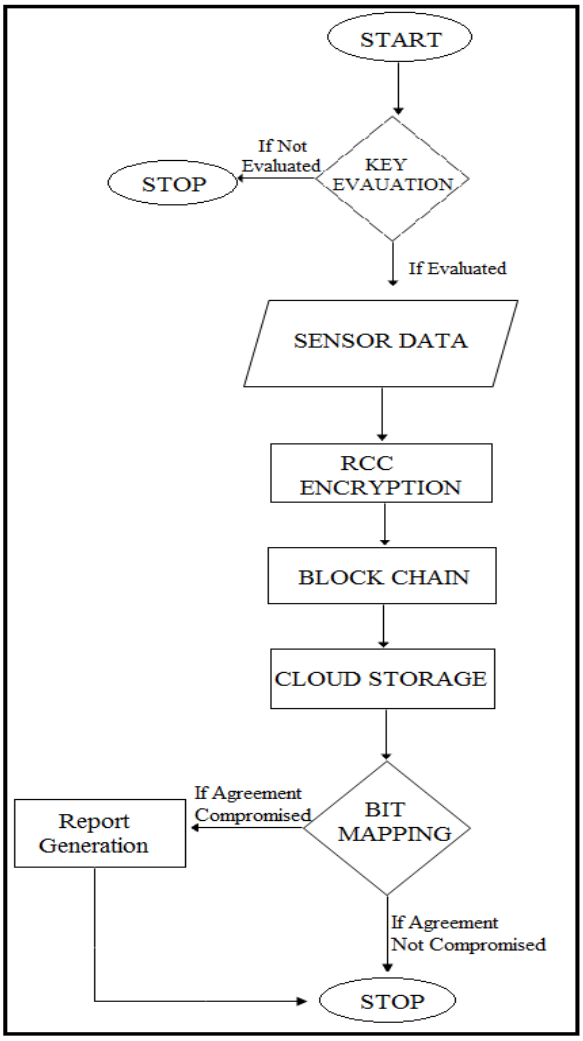

Figure 1: Proposed model

IV. CONCLUSION AND FUTURE SCOPE

While starting comparatively prior than in other industries, transformation in medicine has progressed more slowly than in others. Pharmacological treatments has become one of the main areas of psychiatric, occupational, and even societal developments as research, innovation, and corporatization have advanced quickly. Conventional medical practices have drawbacks such trouble locating a physician, expensive expenses for treatment, and the concealment of health data. Nevertheless, the IoT application sector has recently been merged into all facets of today's Internet of Everything period with the explicit establishment of the internet of things philosophy. The heart of medical IoT connectivity and the source of medical science's greatest advances is the Internet of Medical Things (IoMT). The data collected from these devices must be carefully preserved in order to guarantee consumer confidentiality and security. As the number of patients rises and the prevalence of remote diagnosis increases, one of the newest technological breakthroughs that might be of assistance is the cloud platform. In order to provide a suitable searching strategy on the encrypted data, a reliable method for providing adequate online storage of healthcare IoT data is needed. This approach will be developed furthermore in subsequent iterations of the research.

REFERENCES

[1] M. Masud et al., "A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care," in IEEE Internet of Things Journal, vol. 8, no. 21, pp. 15694-15703, 1 Nov.1, 2021, doi: 10.1109/JIOT.2020.3047662.

[2] X. Liu, X. Yang, Y. Luo and Q. Zhang, "Verifiable Multi-keyword Search Encryption Scheme with Anonymous Key Generation for Medical Internet of Things," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3056116.

[3] R. Cao, Z. Tang, C. Liu and B. Veeravalli, "A Scalable Multicloud Storage Architecture for Cloud-Supported Medical Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 3, pp. 1641-1654, March 2020, doi: 10.1109/JIOT.2019.2946296.

[4] B. S. Egala, A. K. Pradhan, V. Badarla and S. P. Mohanty, "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control," in IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11717-11731, 15 July15, 2021, doi: 10.1109/JIOT.2021.3058946.

[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] C. Xu, Z. Gao, D. Zhang, J. Zhang, L. Xu and S. Li, "Applying Cross-Modality Data Processing for Infarction Learning in Medical Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 23, pp. 16902-16910, 1 Dec.1, 2021, doi: 10.1109/JIOT.2021.3068775.

[7] Sihem Souiki 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] F. Yang et al., "Internet-of-Things-Enabled Data Fusion Method for Sleep Healthcare Applications," in IEEE Internet of Things Journal, vol. 8, no. 21, pp. 15892-15905, 1 Nov.1, 2021, doi: 10.1109/JIOT.2021.3067905.

[10] Y. Ding et al., "DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things," in IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1504-1518, 1 Feb.1, 2021, doi: 10.1109/JIOT.2020.3012452.

[11] Ronghui Cao, Zhuo Tang, Chubo Liu, Bharadwaj Veeravalli, "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.

[13] J. Liu, J. Ma, J. Li, M. Huang, N. Sadiq and Y. Ai, "Robust Watermarking Algorithm for Medical Volume Data in Internet of Medical Things," in IEEE Access, vol. 8, pp. 93939-93961, 2020, doi: 10.1109/ACCESS.2020.2995015.

[14] P. Zeng, Z. Zhang, R. Lu and K. -K. R. Choo, "Efficient Policy-Hiding and Large Universe Attribute-Based Encryption With Public Traceability for Internet of Medical Things," in IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10963-10972, 1 July1, 2021, doi: 10.1109/JIOT.2021.3051362.

[15] D. Połap, G. Srivastava, A. Jolfaei and R. M. Parizi, "Blockchain Technology and Neural Networks for the Internet of Medical Things," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020, pp. 508-513, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162735.