International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.9756/INTJECSE/V14I5.333 ISSN: 1308-5581 Vol 14, Issue 05 2022

Potential Sustainability in Storing Cloud Data with Privacy Preservation Scheme over E-Records in HealthCare Systems

Ms G.Manjula
manjulacse@rmkcet.ac.in
Assistant Professor, Department of Computer Science and Engineering, RMK College of Engineering and Technology, Chennai.

Mrs N.Kalyani
kalyanicse@rmkcet.ac.in
Assistant Professor, Department of Computer Science and Engineering, RMK College of Engineering and Technology, Chennai.

Mrs S.Vijitha
vijithas.se@velsuniv.ac.in
Assistant Professor, Department of Computer Science and Engineering, Vels Institute of Science Technology and Advanced studies, Chennai.

Dr A.Packialatha
packialatha.se@velsuniv.ac.in
Assistant Professor, Department of Computer Science and Engineering, Vels Institute of Science Technology and Advanced studies, Chennai.

Ms J.Preethi
preethi.j@rajalakshmi.edu.in
Assistant Professor, Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai.

Abstract - Researchers suggest incorporating security within portable medical systems with use of the cloud infrastructure in response to user privacy, barriers towards the application of e-healthcare systems, and the astronomical performance of cloud platforms. The structure integrates notable characteristics such as effective key generation, secure data access, particularly for emergency collection, and greater transparency for unauthorised use of healthcare data.The majority of data is sent to the cloud for storage and analysis in IoT devices that use cloud services. Because obtaining data in the cloud poses a danger of private revelation owing to the cloud's accessibility, security and privacy are major considerations. Data security is ensured in that fashion because an intruder needs access to both peripheral and storage server copies of the information. Thorough testing as well as a comprehensive performance evaluation have shown how well the system functions to protect user data.An adaptive authentication protocol for a sophisticated IoT-based e-health cloud storage device is suggested. So, in order to protect patient health records, implement user access both for emergency medical situations and to provide space in internet database systems, those requirements must all be met. All health records created by the health network infrastructure are protected before being transported to the backup system. Through the use of a cross-domain policy, various medical staff across numerous health zones may safely exchange this data with one another.

Keywords: User Privacy, Data Security, E-health, Healthcare,Cloud Technology

I. INTRODUCTION

Patients' past medical files could be restored via an encryption key method in an incident. Together, in a typical system, only medical practitioners with appropriate characteristic private keys could retrieve the cloud. A safe reduction approach is created to remove redundant patient records containing similar data that might be secured using various restrictions, in order to reduce overall memory consumption as in cloud storage of data. This fact that over data traffic permitted by various initial user credentials can view the residual health record after reduction is among the technique's key features. A sophisticated medical massive storage solution has been explicitly demonstrated to be safe, and a thorough analysis and set of models show that this is effective.The confidentiality of data in such systems is very important since innovations might come with threats. Despite its expanding popularity and greater efficacy, many privacy concerns that could develop were not given any thought. Proper protection of anonymity must be examined in light of evolving security laws and regulations pertaining to personal data or information. Several of the main uses for cloud computing technology are cloud infrastructure. Many users are drawn towards cloud servers because of their enormous storage capability. This outsourced strategy means that cloud users have no control of their data. Confidential or sensitive information will be seriously threatened once it is seized, disclosed, or altered while in recovery.The advancement of IoT technologies enables healthcare institutions to offer top-notch, practical, and all-encompassing medical care. This patient could have a set of small Wsn inserted to track their health and gather vital biological data useful in both diagnosing infectious conditions as well as making critical medical choices. The elderly can receive contemporary health treatment anywhere at any time to pursue a better life by using wearable or implantable embedded sensors. This clinical IoT platform gathers biomedical signals, which are then sent to a health data centre for archival and illness diagnostics.

The suggested system tackles the possible dangers to e-healthcare through giving users a safe interface as well as preventing intruders from entering cloud services. Technological health services have replaced traditional medical care, allowing the ability to treat illnesses from a distance. Many parties, including physicians, customers, and others, now have simple access to a patient's

health information owing to the public cloud, which significantly contributes to this transformation. Internet services provide flexible, economical, and portable solutions related to healthcare information systems. Given the massive advantages of the cloud, such as authenticated access to data, patients' EHR confidentiality is a top priority. The suggested technique is the best option for ensuring the security of data in cloud E-healthcare solutions because of its flexibility and resilience.A patient with unclear ailments may be identified and treated at many institutions, and various health files could be kept, according to the current health industry. As a result, developing a merged safe information exchange process is crucial to facilitating clinical outcomes at various institutions. These cloud resources are used to store and provide ubiquitous data access for protected medical information created by various institutions. The inter-authentication mechanism for a patient's safeguarded medical records is determined by the user. Every member of medical personnel must connect with the treatment centre in order to obtain the unique private key needed to decode the physician's cypher text.

It makes it simple for all parties involved, including health providers, physicians, and users, to create, save, and retrieve health data, regardless of the limitations imposed by time or place.Cloud providers offer advantages in terms of the efficient and effective handling, upgrading, and storing of data. The fact that information is stored on a diverse set of cloud computers that are connected to each other and maintained in a centralized fashion that can be viewed by several people from various regions puts both safety and confidentiality at risk. Because the vast majority of patient records are also extremely private and sensitive, storing them on data held by third parties inevitably increases those risks.The current private information tools are insufficient to guarantee strong encryption, mostly in e-health infrastructure.

Despite popular opinion, malicious insiders involving personnel having authorized data access within firms, whereby database management systems or top management are indeed the assailants, pose a much greater danger to health information kept on cloud storage than foreign assaults. This research tries to give a thorough analysis of the benefits and shortcomings of user privacy protections now in place in e-healthcare settings, which leave users exposed to attacks throughout the cloud system.Including its capacity, flexible capabilities, simple and quick installation, and lower prices, the public cloud has experienced remarkable development and transformed the entire computing platform, inspiring many enterprises to migrate their information there. Although cloud services offer significant advantages, they are nonetheless vulnerable to a number of potential threats. Users might not be conscious of enormous quantities of information saved by the service provider, such as this illustration. Lack of clarity makes it challenging to understand how, where, or how information is handled. This makes it tricky to respect any provider, which may be to blame for significant losses in data. Numerous plans and innovations have been made in this field of clouds.Inadequate knowledge may result in their therapy being delayed. That might be deadly. However, if the patient previously had data with gadgets that are cloud-accessible, retrieving it will just take a few moments, allowing the new medical personnel to initiate the therapy as quickly as feasible. If a storage server has connected web access, then the healthcare insurance sector could hold information there in encoded format using robust security cryptographic procedures, restricting access to only authorized users. This "cloud" consists of servers that are connected to the internet that host a variety of programmers or information.Many of the cutting-edge private information cloud security precautions cannot be used for e-health. A centralized mainframe processing model known as cloud services, which is controlled by cloud vendors as well as fewer physicians and open to hacker attacks, renders medical files more insecure. Another of the main drawbacks of cloud technology would be this. Despite the fact that cloud services approaches follow adequate protection guidelines, their security vulnerabilities prevent them from providing a reliable e-health service.These medical files may be secured and saved mostly in the cloud using this method. It ensures such a level of data security for effective information storage mostly in the e-health sector. This plan is less secure due to the fact that healthcare data is still kept private, as well as the fact that the data administrator may access the information. Additionally, this approach is unsuitable for health records since it is not physician-driven and is virtually impossible for concerns of any significant magnitude. The clinical Iot gathers biomedical signals, which are then sent to a health data centre for archival and illness diagnostics. During distribution, the clinical file must be encoded to preserve patients' privacy and stop monitoring.This healthcare data must be secured upon distribution in order to preserve patients' confidentiality and stop third parties from listening in on private communications. For sensitive information, this patient applies an authentication scheme to specify the permissible characteristics and interactions.

Content information is protected throughout this fashion because an intruder needs access to both peripheral and cloud servers' copies of data. Additional testing as well as a thorough evaluation of the metrics has shown how well the device works to protect user information. This architect's ability to safely and effectively access data stored whilst lowering computing costs via operations reduction has been sorely tested. Whenever the number of users is significantly small, this product's operational cost is much lower than the standard internet-secured storing approach.Every time an authorized user requests access to the EHR, the health system gathers the relevant data across fragmented cloud storage and reconstructs its electronic health record. Through outsourcing all patient records that can be recreated via cloud computing, the strategy boosts the EHR's effectiveness.According to conceptual and empirical analyses, the approach is a very effective and secure way to handle health records remotely. The architecture is insufficient to prevent intrusions and illegal availability.

II. LITERATURE REVIEW

T. Wang [1] the author, investigated the majority of transmitting data towards the web for storing and analysis as in Iot devices with cloud assistance. Because obtaining data poses a danger of private revelation owing to cloud's accessibility, data security remains major considerations. To such aim, the paper suggests PERT, a retrieving method with security enhancements for virtualized IoT. Such technology's implied indexing, which is kept up to date by end nodes, its hierarchy retrieving mechanism, which conceals the details underlying information transit between internet as well as the peripheral virtual machines, protect private information. In order to split the information for hierarchy detection algorithm, we developed an approach.

Y. Bao, [2] introduced a paper in building a sophisticated health system using IoT devices with the cloud is still a growing concept in healthcare technology. This physician may keep track of the patient's condition with the help of an IoT-focused and platform health service and react to symptomatic disorders instantaneously. Given the seriousness of patients' confidentiality, it's indeed essential to secure the health information cloud storage to avoid undesirable individuals and moderately cloudy individuals from obtaining it. Nevertheless, the recipient of information experiences difficulties retrieving the secured medical data contained in the cloud. The resource-constrained gadgets upon which patients' and physicians' perspectives are challenged by the high computation usage.In this article, we describe a simple essential element encryption algorithm arrangement that realises fine-grained network access and keywords whilst also lowering the computational complexity for resource-constrained equipment in order to endorse effective cypher-text collection and address the achievement challenge. In order to meet the security requirements mostly in the field of services, researchers systematically demonstrate the conceptual safety of the suggested LABSE system and examine enhanced security aspects. Researchers then create a detailed methodology for LABSE inside the health service. Researchers additionally assess LABSE's usefulness and sophistication in relation to other cutting-edge similar methods. Lastly, we use the research to show how usability and effectiveness benefit.

According to Z. Yang [3], the Iot has subsequently had a significant impact on the medical industry. Nevertheless, the fast expansion of medical technology has generated a large number of large datasets, the majority of which are visually. Both computation, caching, and the movement of information are severely hampered. The advancement of IoT healthcare systems is hampered by network dynamism and regional distribution. To increase the effectiveness of future methods or approaches to health, we suggest a smart terminal design for visually Internet-of-things health services in this paper. We begin by providing a systematic analysis of the aspects of the human from the point of view of information processing, after which we identify the ultimate intellect and address the issue of measuring the cognition of embedded systems.To offer a conceptual underpinning for dynamic management of network edges, we also present an efficient awareness measurement instrument for edges or cloud sides. Consequently, we offer a round that maximises the effectiveness of node density as well as data analysis. The HIoT is made as sophisticated as possible, and smart node monitoring is used. We conducted research on several techniques to confirm their effectiveness. The simulation findings show that smart V-HIoT works much better than current ways since the proposed technique can achieve the highest levels of knowledge both in a circumstance involving numerous diverse gadgets as well as an emergency health need.

W. Zhang[4] introduced a paperthe e-healthcare cloud environment had demonstrated its capacity to raise both quality of patient care and quality care. However, confidentiality concerns prevent its broad adoption and use. The confidentiality of information in electronic health records is the subject of many research studies. Such efforts do, nevertheless, possess several significant drawbacks. Individuals also experience the assumption assault. In this research, we propose an e-healthcare public cloud featuring fine-grained network access that is immune to inferences attacks for first period. We start by suggesting a two-layer encryption technology.Researchers methodically created the 2nd cryptography to respect the privacy of role characteristics and availability requirements utilised in the first cryptography. We suggest allowing its cloud service to carry out operationally heavy tasks on sample data from a larger user while understanding certain confidential material in order to fully utilise the cloud service. In addition, researchers created a blind information retrieval procedure to maintain overall retrieval of data characteristics in the Ehealth. We additionally show that adding exploration ability to the system is a simple process. Last but not least, we carry out in-depth safety studies and performance reviews that validate the efficiency and effectiveness of their methods.

Kanwal [5] introduced a paperEHRs are used more often to retain, preserve, and communicate various sorts of health information. Additionally, this information may be used for any variety of scientific projects, including medical studies and methods for controlling epidemics. Health businesses feel secure contracting such activities to cloud-based EHRs due to the high cost and unavailability underlying health care. Although its expanding popularity and greater efficacy, the privacy concerns that may develop were not given any thought.The wireless carriers or internet provider organisations in charge of managing an EHR are indeed the data controllers, establishing the guidelines by which others must abide while processing information. A primary goal of EHR is to assist in the treatment and recovery of individuals. There are several further applications, including those in analytics, scientific diagnostics, and population health. Our efforts are concentrated on the EHR's additional usage.

According to Mamta, B[6],since it enhances accessible reliability, the idea of exchanging health data via cloud services in a medical physical phenomenon has gained popularity recently. The only way to maintain the overall privacy of health information is to keep it classified, but doing so reduces its usefulness and greater flexibility of efficient searching. Nevertheless, since a conventional ABSE includes mathematical operations, it is not viable to take the right steps to devices with low and huge storage.

This information is constantly gathered by sensors with capacity constraints in a healthy cyber-physical system, so we are unable to effectively implement ABSE strategies here yet. The systems are increasingly operations of a conventional ABSE system are carried out over the blockchain system in the proposed technique to minimise the intrinsic computationally of the ABSE system. This suggested method provides two important advantages when compared with using a block chain. This is truly decentralised and independent from a system failure since it is firstly independent from a reliable source. Since the computing load is already shared throughout the Ethereum channel's consensus nodes, it is highly scalable. In particular, these consensus nodes are in charge of initialization of the system, which is thought to become the most difficult to solve, and the duty of generating and examining the various tokens, which is thought to become the most common activity.

S. Ali [7] suggested an approach in order to speed up treatment effectiveness, lower complications, and support ongoing setup in changing circumstances. Users select cloud computing solutions from web apps on a variety of platforms. Medical insurance biosensor monitors are frequently utilised for diagnostic testing and ongoing clinical services during medical services. Regression testing is therefore used by enterprises to verify the effectiveness and dependability of system-based modifications. Nevertheless, element computer validation becomes tough and demanding for a big system having limited funds and regularly changing part management within cloud servers because of inappropriate and duplicated test scenarios and failures.In order to boost the overall efficiency of detecting defects, a layout pattern-based methodology for testing choice and prioritising was proposed in this research. Utilizing an observation pattern, we simply select test scenarios for commonly used parts, and then we provide priority to test instances that use certain approaches. An investigation has been used to verify the increased organizational, and it has been contrasted to alternative methods. Therefore, the test findings demonstrate that the conceptual approach effectively validated modifications. This conceptual approach improves its fault detection rate when compared to the earlier fault conditions and randomized prioritizing systems.

According toR. Ranchal[8],In several ways, cloud technology is superior to conventional systems. Health organisations are beginning to use it. Given the growing amount, speed, and diversity of health records as well as the requirement to assist in data linkage and extensive analysis, this became necessary. Big data analysis, effective data linkage, and constant data collection from many diverse sources are all capabilities of cloud-based solutions. At the same moment, important reasons supporting cloud adoption include safety, scalability, and recovery procedures. Because of the ambiguous nature of healthcare information protocols, the diversity and related concepts of health records, and the numerous restrictions that govern their use, effective transfer of care operations to the cloud is not even a simple process.

III. PROPOSED METHODOLOGY

3.1 Electronic Health Records

Electronic health records (EHRs) were more often advocated in e-health networks for the collection and storage of numerous types of client records, including private data about patients' demographics, private details including current weight, and prescription data. EHR is indeed a legal contract, and both its contents and usage are subject to rules. An EHR's contents could ever be altered. The EHR is a conceptual database as well. The EHR platform, a group of parts that together create the process wherein the EHR is produced, maintained, stored, and retrieved, operates the EHRs. The module includes users, health records, instructions and methods, apps, and modern technologies.Technological medical services have replaced traditional health services, allowing the ability to treat diseases from a distance. Various participants, including physicians, nurses, clients, life insurance brokers, etc., may simply avail patients' medical info thanks to cloud applications, which is a key factor in this transformation. Internet services provide for flexible, affordable, and wide-ranging mobile sharing of patient health records. Patients' EHR confidentiality is a top priority. Given the massive advantages of the internet, such as real-time accessing data, communicating extremely critical and valuable patient data via an unprotected wifi network presents several potential risks, including espionage and data tampering.These have been put into practise, employing and altering the most effective encryption process techniques appropriate for cloud EHR systems. This suggested plan avoids using conventional cryptographic techniques since they are inappropriate for cloud systems.

They achieved the capacity to govern and increase computer assets in accordance with necessary healthcare. An EHR can accommodate massive data transfers. When compared with typical client computers, moving and adapting patient information via network computers already present in care settings to the cloud offers various benefits. The capacity to scale is a huge benefit of this move. The cloud EHR process utilises fewer IT assets, which lowers operational costs, increases access and communication, guarantees a faster deployment process, offers support resources, and ensures superior flexibility.

3.2 Sensors to Detect EHR

A behaviour analysis element which collects sensory and visual information, analyses predictable outcomes, and produces notifications for possible issues. A database for activities that stores sensory data and may be used to create alerting circumstances.Investigators, physicians, families, and individuals will see the information through private internet portals having adjustable accessibility.The behavior data, that houses all sensor information, as well as the EHR dataset are strongly connected by system design. With help of such a link, major medical occurrences may be added here to sensor information, and alarms that are created by information could be recorded in the EHR.

To effectively use technological data that supports great selection, but to do so inside the EHR, physicians must be able to access and use it with ease. Additionally, any standardised tests that medical personnel want to employ have to be fully functional. Accurate risk evaluations for rashes, accidents, as well as other post-traumatic stress require standardised testing. Physicians must be able to quickly evaluate and understand the findings of assessments in order to implement danger measures during patient care. Technology is constantly being used to evaluate healthcare coverage, so all health practitioners will then have complete EHRs.

IV. DESIGN AND IMPLEMENTATION

4.1 Privacy Preservation Scheme for Data Sustainability

The purpose of this proposed scheme is to implement an eHealth functionality, ensuring all data can be accessed by authorised parties while still being properly safeguarded. For example, if a patient requires immediate help, this platform makes sure to ensure that it receives fast and adequate treatment, yet additional measures prevent security breaches or enable fraudsters to compromise the platform's integrity. Even while the technology is used for interaction among patients and healthcare professionals, commercialised components, such as the dispatching centers, are unable to see the data going through.In this article, we provide a series of privacy-preserving procedures made available by either a for-profit community eHealth that protects elderly patients and patients who are confined to their homes and offers household assistance. The approach is considered a unique healthcare network infrastructure, as well as the standards created to promote it, outline permitted knowledge transfer between people with chronic conditions as well as a process of getting in touch with a patient's caretaker in such an event. This approach is premised on the idea that getting the eHealth support rendered by a business organisation is a crucial step toward widespread implementation of such technologies. There is an integral aspect to ultrasensitive patient records, and users will only have confidence in the government if their data is safe.

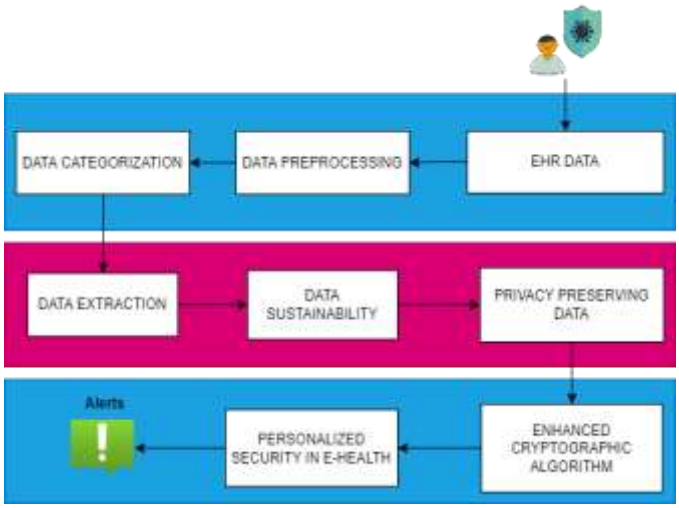

Figure 1. Data Sustainability for E-health Recording Database

Individual e-health devices are built for use by individuals, such as patient populations or community members, in terms of maintaining their health and preventing illness, primarily beyond the setting of a hospital or other health provider. This encourages health literacy, disease prevention, integrated care, and self-management. Personalized e-health platforms could also make use of data from patients' environment, their internet usage, as well as other well-being applications in addition to typical health-related private information, including medical files and biological sensor readings.

V. CONCLUSION

Data sustainability relates to legal provisions of secrecy regarding the gathering and sharing of personal information. Anywhere personal information is gathered and maintained, whether digitally or otherwise, privacy implications are raised. Data protection, which pertains to safeguarding data from danger of loss or modification, including from unauthorised usage, is connected to confidentiality but should not be confused with this. A personalised e-health system could also rely on data from the patient's environment, their internet communications, as well as other wellbeing applications in addition to typical safety personal information, including medical files and biological sensor readings. Several strategies that calculate consolidated findings could be used to ensure privacy protection while transferring private information for analysis and information sharing. The majority of patients used in an integrated determines privacy issues; too few individuals may still potentially expose people's data. Hiding

personal details from processing elements is yet another type of security purpose. Thus, the position of storing as well as the specific type of data pre-processing determine the selection of good approaches.

VI. REFERENCES

1. T. Wang, Q. Yang, X. Shen, T. R. Gadekallu, W. Wang and K. Dev, "A Privacy-Enhanced Retrieval Technology for the Cloud-Assisted Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 18, no. 7, pp. 4981-4989, July 2022, doi: 10.1109/TII.2021.3103547.
2. Y. Bao, W. Qiu and X. Cheng, "Secure and Lightweight Fine-Grained Searchable Data Sharing for IoT-Oriented and Cloud-Assisted Smart Healthcare System," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2513-2526, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3063846.
3. Z. Yang, B. Liang and W. Ji, "An Intelligent End–Edge–Cloud Architecture for Visual IoT-Assisted Healthcare Systems," in IEEE Internet of Things Journal, vol. 8, no. 23, pp. 16779-16786, 1 Dec.1, 2021, doi: 10.1109/JIOT.2021.3052778.
4. W. Zhang, Y. Lin, J. Wu and T. Zhou, "Inference Attack-Resistant E-Healthcare Cloud System with Fine-Grained Access Control," in IEEE Transactions on Services Computing, vol. 14, no. 1, pp. 167-178, 1 Jan.-Feb. 2021, doi: 10.1109/TSC.2018.2790943.
5. Kanwal, Tehsin & Anjum, Adeel & Khan, Abid. (2021). Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities. Cluster Computing. 24. 10.1007/s10586-020-03106-1.
6. Mamta, B. B. Gupta, K. -C. Li, V. C. M. Leung, K. E. Psannis and S. Yamaguchi, "Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System," in IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 12, pp. 1877-1890, December 2021, doi: 10.1109/JAS.2021.1004003.
7. Shobharani Pacha, Suresh Ramalingam Murugan, R.Sethukarasin,'Semantic annotation of summarized sensor data stream for effective query processing', The Journal of Supercomputing,volume 6,issue 6,pages 4017-4039,Springer US,2018,DOI: 10.1007/S11227-017-2183-7
8. S. Ali et al., "Towards Pattern-Based Change Verification Framework for Cloud-Enabled Healthcare Component-Based," in IEEE Access, vol. 8, pp. 148007-148020, 2020, doi: 10.1109/ACCESS.2020.3014671.
9. R. Ranchal et al., "Disrupting Healthcare Silos: Addressing Data Volume, Velocity and Variety with a Cloud-Native Healthcare Data Ingestion Service," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 11, pp. 3182-3188, Nov. 2020, doi: 10.1109/JBHI.2020.3001518.
10. G. Yang et al., "Homecare Robotic Systems for Healthcare 4.0: Visions and Enabling Technologies," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 9, pp. 2535-2549, Sept. 2020, doi: 10.1109/JBHI.2020.2990529.
11. X. Wang and Z. Jin, "An Overview of Mobile Cloud Computing for Pervasive Healthcare," in IEEE Access, vol. 7, pp. 66774-66791, 2019, doi: 10.1109/ACCESS.2019.2917701.
12. ES Madhan, KS Kannan, P Shobha Rani, J Vakula Rani, Dinesh Kumar Anguraj,'A distributed submerged object detection and classification enhancement with deep learning', Distributed and Parallel Databases, Springer US, DOI: 10.1007/S10619-021-07342-1,May 2021
13. S. Sharaf and N. F. Shilbayeh, "A Secure G-Cloud-Based Framework for Government Healthcare Services," in IEEE Access, vol. 7, pp. 37876-37882, 2019, doi: 10.1109/ACCESS.2019.2906131.
14. C. Xu, N. Wang, L. Zhu, K. Sharif and C. Zhang, "Achieving Searchable and Privacy-Preserving Data Sharing for Cloud-Assisted E-Healthcare System," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8345-8356, Oct. 2019, doi: 10.1109/JIOT.2019.2917186.
15. R. Zhang, R. Xue and L. Liu, "Searchable Encryption for Healthcare Clouds: A Survey," in IEEE Transactions on Services Computing, vol. 11, no. 6, pp. 978-996, 1 Nov.-Dec. 2018, doi: 10.1109/TSC.2017.2762296.
16. Abbas, Assad. (2016). e-Health Cloud: Privacy Concerns and Mitigation Strategies. 10.1007/978-3-319-23633-9_15.
17. C. He, X. Fan and Y. Li, "Toward Ubiquitous Healthcare Services with a Novel Efficient Cloud Platform," in IEEE Transactions on Biomedical Engineering, vol. 60, no. 1, pp. 230-234, Jan. 2013, doi: 10.1109/TBME.2012.2222404.