International Journal of
Embedded Systems and
Emerging Technologies

ISSN: 2456-723X
Volume 11, Issue 2, 2025
July–December
DOI (Journal): 10.37628/IJESET

http://ecc.journalspub.info/index.php?journal=JESET&page=index

Review IJESET

Intensive Patient Care at Home Using IoT and Cloud

Lad T. Shivaji[1,*], Bhoite S. Vikas[1], Shingare V. Laxman[1], Pilane S. Ashok[1]

Abstract

All nations acknowledge that every individual has the right to maintain excellent health throughout their life and to take all necessary steps to keep improving. A person's productivity can be significantly impacted by their health. Everyone is happier and more productive when an employee is in good health, which benefits the company. Recent technological advancements have made a significant contribution to the healthcare sector. Internet of Things (IoT) sensors enable the idea of remote medicine, which has the potential to significantly reduce physicians' workloads in addition to enabling continuous patient monitoring. But in certain instances, these sensors have been used more frequently, increasing the risk of sensitive data being stolen or changed. Since most of this sensor data is being moved to cloud platforms, there is a higher level of vulnerability. However, there are serious issues with data security and privacy brought on by our growing reliance on IoT devices. Sensitive patient data is constantly being transferred to cloud platforms, putting it at risk for manipulation, illegal access, and data breaches. These flaws have the potential to jeopardize patient privacy, result in poor medical judgment, and even cause life-threatening circumstances. Therefore, it is crucial to protect medical data while preserving the advantages of IoT integration. There needs to be an alternative that safely safeguards the IoT's growing convenience. cloud platforms and IoT devices in the medical field. As a result, this technique outlines an effective way to send sensor data to the Thing Speak cloud using the cloud and the IoT. The server accesses this data concurrently for preprocessing and decision-making through WhatsApp Intimation to monitor the patient's vitals. Secure frameworks that combine cloud and IoT technologies have been created to address these issues. Sending sensor data to the Thing Speak cloud platform for preprocessing and safe storage is one method. Furthermore, WhatsApp real-time notifications give prompt information about patient vitals, enabling medical professionals to react quickly. These methods show how cloud and IoT system integration, when paired with strong security protocols, can enhance healthcare delivery, boost operational effectiveness, and protect private patient data.

Keywords: Medical health records, public clouds, internet of medical things, Internet of Things (IoT), Remote health monitoring system

***Author for Correspondence**
Lad Tejaswini Shivaji
E-mail: ladtejaswini48@gmail.com

[1]Students, Department of Computer Engineering, Rajgad Dnyanpeeth Technical Campus Polytechnic, Dhangawadi, Maharashtra, India

Received Date: April 06, 2025
Accepted Date: August 26, 2025
Published Date: December 31, 2025

Citation: Lad T. Shivaji, Bhoite S. Vikas, Shingare V. Laxman, Pilane S. Ashok. Intensive Patient Care at Home Using IoT and Cloud. International Journal of Embedded Systems and Emerging Technologies. 2025; 11(2): 28–35p.

INTRODUCTION

As the information age progresses, the amount of data produced by customers is also growing at an exponential rate. It is obvious that the user's local PC memory is insufficient. The use of cloud computing services for data processing, administration, and archiving is growing in popularity. Cloud-based apps offer numerous benefits, but they also present significant security and privacy threats to users. When data is uploaded to a distant server, the data owner no longer has control over it; instead, they must depend on the server to do any necessary actions. Since then, other issues with cloud data privacy have surfaced such as

how to ensure data privacy and the effectiveness of user-restricted access and authorization management [1, 2]. However, because most modern cloud storage systems are centralized, data administration is usually controlled by a single institution. In addition to distribution prices, using this method involves significant computing fees. Therefore, providing a reliable, safe, and efficient way to collaborate on cloud storage is essential. We provide a cloud ciphertext-based permission system to protect sensitive information. We utilize key encryption and store encrypted messages on the cloud since protecting sensitive data is our top priority. The owner also owns the keys and, implicitly, the access permissions. In conventional research, the function is put forth as a decryption criterion, supporting an encryption technique based on participation. One possible solution to this problem is to build an integrated cloud re-encryption data sharing architecture based on attribute cryptography. By using a creative and adaptable proxy re-encryption technique, the author makes it easier for data owners to handle their data and allows for more flexible ciphertext management of identities. By giving the authorized user the ability to decrypt any re-encrypted ciphertext using their component, the data owner can grant access to the plain text message. The inclusion of environment, credential, and individual components in a proxy encryption process was then proposed as potentially advantageous [3–5]. One common element of these techniques is moving user data to a distant cloud storage location for administration. Critical client data may be permanently compromised or erased by assaults against the management teams of third-party cloud services. The aforementioned security measures are sufficient to protect sensitive data, but they do not help users quickly obtain the accurate information and knowledge they need during the data sharing process. The authors present a unique proxy re-encryption technique based on cryptographically indexed phrases to improve access performance during data transmission. Nevertheless, this approach cannot be used to develop a workable ciphertext decryption algorithm. To improve keyword search, current research addresses this issue by confirming the effectiveness of a key-based characteristic proxy re-encryption procedure within a randomized oracle paradigm. Unfortunately, performance studies show that the approach is too computationally complex to be widely adopted.

A novel problem in cloud data integrity assessment is introduced by focusing on verifying whether files contain specific search terms while preserving file anonymity. To address this, a new labeling mechanism called RAL is proposed, which allows the generation of auditing evidence without disclosing the identity of the file. Experimental evaluations demonstrate both the security and the practical applicability of this method. A scheme called EPSM is proposed as a secure and efficient search method for encrypted medical cloud data in multi-owner scenarios. EPSM enables physicians to search for encrypted medical records in a privacy-preserving and cost-effective manner. While the cloud server cannot interpret semantic similarity, it can compute noisy values and return them for de-noising. This ensures secure and customizable search through trapdoors, while preventing link ability between trapdoors and indices containing shared terms. Designed specifically for multi-data-owner settings, EPSM minimizes computational and communication overhead while requiring only a small number of keys, making it well-suited for medical applications. A secure similarity search method is proposed for M/M (multi-owner/multiuser) environments. The approach guarantees asymptotically optimal comparison searching and query privacy even in the absence of similar data. To strengthen security, the method incorporates request, indexing, and file secrecy protections, achieving adaptive semantic security. Key innovations include ensuring both forward and backward privacy, which are essential for real-time data updates, and eliminating reliance on external trusted key services. These contributions make the protocol more practical and resilient for secure cloud-based similarity search.

LITERATURE SURVEY

A novel route-finding scheme based on searchable encryption has been proposed to support ranked results. The framework consists of three core components: route discovery, index construction, and chained list generation. Security analysis confirms compliance with adaptive translational security, while experimental results validate both the safety and efficiency of the system, demonstrating faster performance compared to existing approaches. An efficient search mechanism for encrypted cloud data introduces a feature-based method for joint word identification. By selecting a subset of unique terms

at random, a reduced-dimensional keyword dictionary is generated, which significantly decreases the size of keys, indexes, and trapdoors [6–8]. This optimization accelerates search operations while maintaining accuracy. Weighted scoring, derived from the comparison of query keywords with document attributes and dictionary terms, ensures precise query results. Traditional encrypted search techniques often fail when query keywords are slightly misspelled or when semantic variations occur, resulting in incomplete or inaccurate results. To address this issue, a cloud-compatible fuzzy semantic encryption model has been developed. This approach generates keyword fingerprints, applies distance measures, and matches them with query fingerprints to support multi-keyword fuzzy searching, thereby improving search tolerance to typographical errors and semantic diversity. An attribute-based keyword search strategy has been designed to prevent duplicate data storage while ensuring reliable keyword matching. The technique integrates access policy–based encryption for fine-grained control and employs outsourced decryption to reduce computational overhead. Integrity verification is supported through cryptographic hash functions and third-party auditing [9]. Furthermore, data labels enable the synchronization of locally stored and cloud data, minimizing redundancy and reducing communication costs. A lightweight multi-keyword search model employs simple multiplication operations for index construction, replacing heavier pairing and arithmetic techniques. This approach supports secure, fine-grained keyword searches while maintaining high efficiency. Security is established through formal analysis, and performance evaluations confirm reduced computational and transmission latency compared to earlier methods. A ranked search framework for encrypted cloud storage applies to a classification-based indexing structure. Documents are organized into groups, and group vectors are generated to reduce dimensionality and indexing time. This grouping also simplifies updates, as only affected vectors need to be rebuilt when documents are modified. Additionally, a focused feature-extraction method enhances search efficiency by restricting server computations to relevant group vectors rather than all possible combinations. A privacy-preserving substring search mechanism has been designed for cloud-stored genetic data. The system supports multiple users and accommodates variable-length queries to locate substrings within gene sequences. Strong security measures preserve the confidentiality of both data and queries. Communication efficiency and session optimization further improve usability, making the method practical for real-world medical research applications [10].

A ranked multi-keyword search model incorporates TF-IDF and vector space modeling to provide precise search engine rankings over encrypted data. The scheme leverages secure kNN computations to resist known attacks and adopts a BC-tree indexing structure to enhance efficiency. By clustering documents prior to encryption, the approach reduces search complexity and improves retrieval accuracy. Existing ranked search solutions are predominantly limited to public cloud environments. To extend support for hybrid cloud infrastructures, an authenticated multi-keyword ranked search algorithm has been introduced. This scheme employs partitioned keyword segmentation based on k-means clustering, ensuring balanced vocabulary distribution and improving both ranking effectiveness and search efficiency. A feature-scoring–based ranked search mechanism is proposed to optimize secure query processing [11–13]. Indexes are constructed so that each recovered term contributes to a ranking dimension, leading to reduced index size compared to traditional keyword indexing. A customized matching score algorithm in the trapdoor generator assigns scores according to similarity type and number of matches, thereby aligning query results more closely with user intent.

METHODOLOGY

The system overview in Figure 1 illustrates the approach that has been recommended to set up a patient's IOT remote health monitoring system.

The implementation of the steps listed below served as a foundation for the proposed approach.

Step 1

Sensor Data Collection

The patient is lying in bed at home while the order is affixed to a board, and their temperature sensor is calibrated. However, the microcontroller board already has the API built in, so connecting it to the

laptop does this. The ESP32 board attaches to the sensor to provide power and gather input values. The sensor's inputs can be used to turn it on and provide data to the board. The board has Python installed with the intention of gathering sensor data, after which it is connected. Data collection from the sensors begins immediately when the Python code is uploaded to the board.

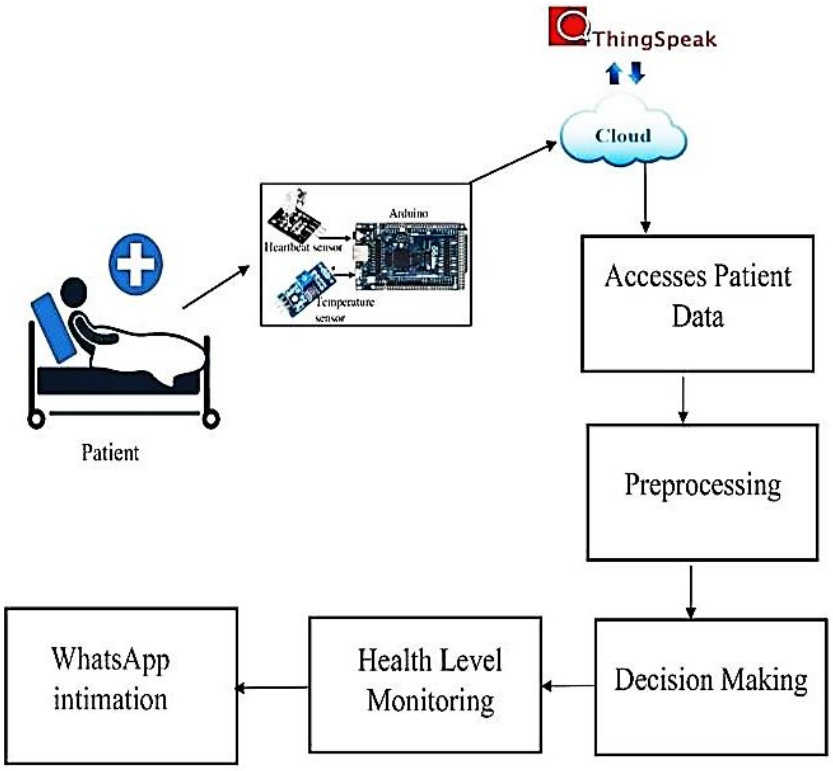

Figure 1. IoT-based patient health monitoring and alert system.

Table 1 displays the ESP 32 model's specifications.

Table 1. Specification of ESP 32.

Module Model	**ESP-WROOM-32S**
SPI Flash	32Mbit(default)
Support interface	UART/GPIO/ADC/DAC/SDIO/SD card/PWM/I2C/I2S
Integrated crystal oscillator	40MHz Crystal oscillator
IO Port	38
Antenna	Onboard antenna
Power Supply	Voltage 3.0V–3.6V, Typical 3.3V, Current >500 mA
Operating Temperature	–40°C–85 °C
Storage Environment	–40 °C–120 °C
Length(mm)	25.4
Width(mm)	48.26
Height(mm)	3
Weight(g)	10
Shipment Weight	0.015 kg
Shipment Dimensions	12 × 8 × 2 cm
Module model	ESP-WROOM-32S

Figure 2 shows the ESP 32's connectivity circuit diagram with the temperature sensor.

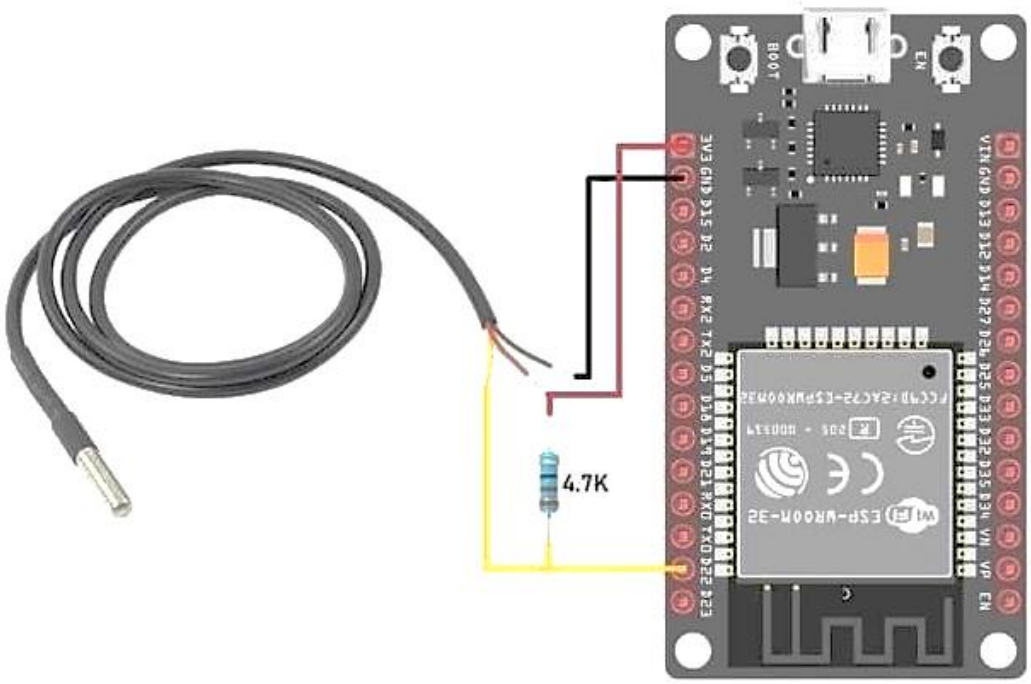

Figure 2. Circuit diagram of the proposed model.

Step 2
Preprocessing

The list of processed and sent sensor input values is passed as input to the Python function. These factors successfully look for an interface and temperature threshold. We then reduce the strings and eliminate the junk values from the data that has already been preprocessed. We then assess the patient's severity using the findings.

Step 3
Decision Making

The sensor's configuration enables the patient to wear it along with the required power source. The sensor values are continuously sent to the thing talk cloud on the assigned channel and ID using their corresponding API credentials. To determine whether the sensor's readings alter or surpass a predetermined threshold when the temperature rises sufficiently, all this data is stored on the server. When this threshold is crossed, the temperature is uncontrollably rising above the tolerable level, and the situation could be classified as a serious level scenario. This decision-making module determines the circumstance by applying its if–then rules. The decision-making technique activates a voice alarm at the patient's home to get a current picture of the patient and alert their loved ones. At the server end, we generate a message string and a map URL using Python's Pywhatkit module. We then use the WhatsApp app to send information to the physician treating the patient (Table 1).

RESULTS

Using Internet of Things (IoT) sensors, the installed system continuously measures the body temperature and pulse rate of bedridden patients. Real-time remote patient health monitoring is made possible by the transmission of the gathered data to a cloud-based server. In the event of anomalies, the system generates notifications and guarantees ongoing observation.

The system interface makes it simple for caregivers to monitor health parameters in real time, such as temperature and pulse rate, as seen in Figure 3. Furthermore, the system automatically sends the designated doctor an SOS notice via WhatsApp in the case of a medical emergency such as an abrupt increase or decrease in vital signs.

Figure 3. WhatsApp message sent by the system to doctor when critical situation occurs.

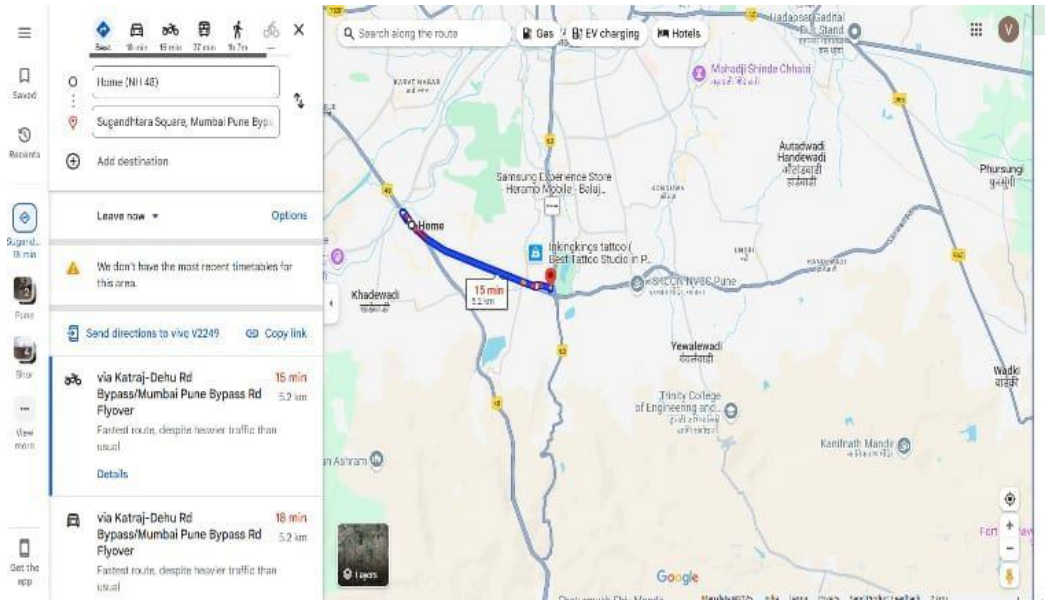

Figure 4. Live location tracking of ambulance.

By using the live location monitoring tool (Figure 4), medical professionals can quickly summon an ambulance, if necessary, by pinpointing the patient's precise location.

The outcomes show how responsive, dependable, and successful the system is at giving patients critical care at home. The suggested method improves real-time monitoring and emergency response through IoT and cloud integration, which raises patient safety and healthcare management standards overall.

CONCLUSION AND FUTURE SCOPE

First, the Arduino Uno board is connected to the medical sensors. After connecting to the system, the ESP 32 microcontroller starts gathering sensor data and sending it to the recommended manner.

Using this method, the data is encrypted and converted to a list. This list is then stored on Thing Speak, a public cloud storage platform. Most of this sensor data is being uploaded to cloud servers, which jeopardizes its security. The healthcare sector needs a reliable alternative to the data security techniques used today because of the greater convenience that cloud platforms and IoT devices offer. Thus, this approach outlines a way to effectively move data from sensors to the Thing Speak cloud via the cloud and the IoT. The server concurrently accesses this data to preprocess it and make decisions utilizing WhatsApp notifications to track the patient's vitals. In the future, this system can incorporate several sensors, including those for electrocardiograms, blood pressure, and electroencephalograms, to enable real-time patient monitoring.

REFERENCES

1. Gao X, Yu J, Chang Y, Wang H, Fan J. Checking only when it is necessary: Enabling integrity auditing based on the keyword with sensitive information privacy for encrypted cloud data. IEEE Trans Depend Secure Comput. 2022;19(6):3774–3789. doi: 10.1109/TDSC.2021.3106780.
2. Abdelfattah S, Wang J, Alasmary W, El-Latif AAA, Li F. Effective search using known-plaintext/background models and unlinkability for encrypted medical data. IEEE Access. 2021;9:151129–151141. doi: 10.1109/ACCESS.2021.3126200.
3. Kwon H, Hahn C. Asymptotically optimal and secure multiwriter/multireader similarity search. IEEE Access. 2022;10:101957–101971. doi: 10.1109/ACCESS.2022.3208962.
4. Wu B, Wang J, Li M, Zhang Z, Wang Y. Privacy-protection path finding supporting the ranked order on encrypted graph in big data environment. IEEE Access. 2020;8:214596–214604. doi:

10.1109/ACCESS.2020.3040781.
5. Tao L, Xu H, Shu Y, Tie Z. An effective search method using features to match joint keywords on encrypted cloud data. IEEE Access. 2022;10:42836–42843. doi: 10.1109/ACCESS.2022.3168730.
6. Liu G, Yang G, Bai S, Zhou Q, Dai H. FSSE: An effective fuzzy semantic searchable encryption scheme over encrypted cloud data. IEEE Access. 2020;8:71893–71906. doi: 10.1109/ACCESS.2020.2966367.
7. Liu X, Lu T, He X, Yang X, Niu S. Verifiable attribute-based keyword search over encrypted cloud data supporting data deduplication. IEEE Access. 2020;8:52062–52074. doi: 10.1109/ACCESS.2020.2980627.
8. Cui Y, Gao F, Shi Y, Yin W, Panaousis E, Liang K. An effective attribute-based multi-keyword search scheme in encrypted keyword generation. IEEE Access. 2020;8:99024–99036. doi: 10.1109/ACCESS.2020.2996940.
9. Liu L, Chen Q. A novel category group index mechanism for efficient ranked search of encrypted cloud data. IEEE Access. 2020;8:54601–54610. doi: 10.1109/ACCESS.2020.2977430.
10. Qin S, Zhou F, Zhang Z, Xu Z. Privacy-preserving substring search on multi-source encrypted gene data. IEEE Access. 2020;8:50472–50484. doi: 10.1109/ACCESS.2020.2980375.
11. Shen H, Xue L, Wang H, Zhang L, Zhang J. B+-tree based multi-keyword ranked similarity search scheme over encrypted cloud data. IEEE Access. 2021;9:150865–150877. doi: 10.1109/ACCESS.2021.3125729.
12. Dai H, Ji Y, Yang G, Huang H, Yi X. A privacy-preserving multi-keyword ranked search over encrypted data in hybrid clouds. IEEE Access. 2020;8:4895–4907. doi: 10.1109/ACCESS.2019.2963096.
13. Liu L, Chen Q. A novel feature matching ranked search mechanism over encrypted cloud data. IEEE Access. 2020;8:114057–11465. doi: 10.1109/ACCESS.2020.3002236.

