International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 2, Mar-Apr 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Intensive Patient Care at Home using IOT and Cloud

Wankhede S.M[1], Shravani Bhoite[2], Vaishnavi Shingare[3], Sai Pilane[4], Tejaswini Lad[5], Jori Shweta[6]

*[1]Prof.Department of Computer Technology, Rajgad Dnyanpeeth Technical Campus Pune, Maharashtra, India
*[2,3,4,5]Department of Computer Technology, Rajgad Dnyanpeeth Technical Campus Pune, Maharashtra, India

----------**********----------

Abstract:

Every country recognizes the right of every person to have good health throughout their lives and to take all necessary measures to ensure that their health continues to improve. An individual's health is a crucial factor that can impact their productivity. Having a healthy employee makes everyone around them happier and increases productivity, which in turn benefits the business. The healthcare industry has benefited greatly from recent technological developments. In addition to allowing for constant patient monitoring, the concept of remote medicine made possible by Internet of Things (IoT) sensors has the potential to greatly alleviate doctors' workloads. However, there have been cases where these sensors have been used more frequently, which puts sensitive data at danger of being stolen or altered. An increased degree of vulnerability exists because the majority of this sensor data is being transferred to cloud systems. There must be a substitute that securely protects the increasingly convenient use of the internet of things (IoT) devices and cloud platform in healthcare. Consequently, this method specifies a successful means of transmitting sensor data to the ThingSpeak cloud via the Internet of Things (IoT) and the cloud. In order to keep tabs on the patient's vitals, the server accesses this data in parallel for preprocessing and decisionmaking via WhatsApp Intimation.

Keywords: Internet of Medical Things, Public Cloud, Medical Health Records.

----------**********----------

I. INTRODUCTION

The quantity of data generated by consumers is likewise increasing at an exponential rate as the information age advances. The user's local PC memory clearly isn't enough. Cloud computing services are becoming increasingly popular for data archiving, processing, and administration. Although cloud-based applications have many positive uses, they also pose serious risks to users' privacy and security. The data owner loses control of their data when it is uploaded to a remote server; instead, they must rely on the server to carry out any necessary procedures. Additional difficulties with data privacy in the cloud have emerged since then, including methods to guarantee data privacy and the efficacy of authorization management and user restricted access. Conversely, data administration is

proxy re-encryption, which facilitates easier data handling for data owners and permits more flexible ciphertext management of identities. The data owner can provide access to the plaintext message by enabling the authorized user to decrypt any reencrypted ciphertext using the user's component. Subsequently, it was suggested that including components of environment, credentials, and individuality into a proxy reEncryption process might be beneficial.

modern cloud storage systems due to their centralized nature. Utilizing this method entails substantial computation charges in addition to distribution prices. Offering a dependable, secure, and effective means of working together on cloud storage is, thus, crucial. To safeguard confidential data, we offer an authorization mechanism that makes use of cloud ciphertext. Protecting sensitive information is our first priority, which is why we use key encryption and store encrypted messages on

the cloud. Keys and, by implication, access rights, belong to the data owner as well.
The function is proposed as a decryption criterion in traditional studies, which promotes a participation-based encryption method. Using attribute cryptography as a foundation, one may construct an integrated cloud re-encryption data sharing architecture to address this issue. The author provides a clever and versatile approach of

The aforementioned safeguards are adequate in protecting sensitive information, but they do little to facilitate users' ability to swiftly gain access to the precise data and expertise they require throughout the data sharing process. A novel proxy reencryption approach based on cryptographically indexed phrases is introduced by the authors to enhance access performance during data exchange. However, a practical ciphertext decryption algorithm cannot be created using this method. Current research tackles this problem by demonstrating the efficacy of a key-based characteristic proxy re-encryption process inside a randomized oracle paradigm, with the goal of improving keyword search. Unfortunately, the method is too computationally complex to be extensively used, according to performance tests. Transferring user information to a remote cloud storage facility for administration is a common component of these methods. The management teams of third-party cloud systems are vulnerable to attacks that could compromise or delete critical customer data permanently.

[1]Some facts based on the thought analyses of various authors' works are finally revealed in this portion of the literature survey:

Xiang Gao takes on a new challenge by conducting loud data integrity assessments based on the term with private data. Authors developed a new label called RAL to confirm that files contain the searched-for keyword and to generate auditing evidence without disclosing the file's identity. The researchers show that the proposed method is safe and evaluate its practicality through rigorous testing.

[2] Sherif Abdelfattah proposed a secure and effective method of searching encrypted medical cloud data in a situation where many data owners are involved. Cheap and Private Searching in the Medical Cloud is the Name of the Game. Although the cloud server lacks the ability to comprehend the semantic similarity of indexes and partitions, it is capable of calculating noisy values and communicating them to the doctor for de-noising, enabling economical and confidential medical cloud searching. Additionally, EPSM enables a new feature that allows doctors to personalize their search results by entering specific criteria in the trapdoors. In contrast to well-known plaintext and known background modeling, EPSM is secure and can be utilized to safeguard patient privacy, according to this extensive demonstration and sensitivity analysis. Furthermore, EPSM ensures that no two indices or trapdoors sharing the same terms are linked. EPSM is better suited to medical applications due to its optimization for multi-dataowner situations; extensive research by the author demonstrates that it requires few keys and little calculation and communication overhead expenses.

[3] A safe and successful similarity search strategy for M/M environments was suggested by the author, drawing on the work of Hyunsoo Kwon. In the absence of comparable data, the suggested method guarantees asymptotically optimal comparison searching and query privacy. Before demonstrating the approach's adaptive semantic security, the author ensured its security from the perspectives of request, indexing, and file confidentiality using standard complexity considerations. One of the first is determining a way to provide advance and reverse privacy, which are essential for updating data in real-time. The second is to eliminate the potential necessity of a key service or other core trusted component in the proposed protocol.

The study is structured into five parts. We present a comprehensive overview of ITS in the second section. A concise introduction to deep learning and its uses is given in Section 3. Section 4 details how smart cities and ITS make use of deep learning to detect pedestrians, summarizes the work of several academics in the area, and lays out the obstacles to further study in each subfield. Next, in Section 5, we shall present the final verdict.

II. LITERATURE SURVEY

[4] Shubham Gade et al. used the Hungarian approach in his research, which significantly decreases the time spent allocating Ev-changing vehicle spots. This enables the Hungarian neural network to manage slot allocation more efficiently. The Hungarian Network (Hnet) is a Hungarian approach that uses deep learning to help with assignment problem resolution. This approach, when combined with a deep learning neural network, has the potential to be used for further deep learning issues requiring permutation invariant training (PIT). This Hungarian technique can be employed in the process of scheduling to call the emergency vehicle upon the identification of irregularities in patient health parameters.

[5]Using features to identify joint words (FMJK), Lingbing Tao suggests an efficient search method for encrypted cloud data. A greatly reduced dimensionality keyword dictionary is created by randomly selecting a subset of non-duplicated keywords from the data owner's documents. These keywords, when combined, form joint keywords. This improves search speed by reducing the size of the dictionaries' keys, indexes, and trapdoor. With meticulous attention to detail, each index and trapdoor is constructed. By comparing document attributes and query keywords with the combined terms in the words lexicon, a weighted score is generated, ensuring that the query is accurate.

[6]According to Guoxiu Liu, if the user's query keyword doesn't match the specified keyword, the fuzzy searching of the phrase is ignored. This could be the result of typos or other input errors made when entering the query phrase. Many realworld scenarios can make use of a single phrase with many meanings. The user is causing the search to return inaccurate results by not considering the term's larger meaning. In response to this, the authors introduce a fuzzy semantic encryption system that is compatible with the cloud and can be searched using several keywords. To conduct the fuzzy search, we combine the Distance measure with the fingerprints of the query keywords and the dictionary that is created using a way to generate fingerprints of keywords.

[7]Xueyan Liu suggests an attribute-based keyword search approach to avoid duplicate data and guarantee trustworthy search words. Data encryption using the ABE disguised access policy approach not only keeps data private but also gives you finer control over who can access it. After a TPA verifies the legitimacy of search engine results, the user verifies the integrity of their own data by performing hash functions on secret cryptography and decryption. To alleviate the computational load caused by ABE, outsourced decryption is also employed. To achieve cloud data minimization, data labels are also used to verify that the given data is reproducible with both the cloud information and the data stored locally. Users' connection traffic usage and the amount of data stored on the public cloud are both reduced as a result.

[8]Yuanbo Cui's ABMKS enables secure multikeyword searches with fine-grained permissions by generating encrypted keyword indices using only multiplication computations. When creating an index, all that's needed is multiplication, which is a faster computation method than pairing and arithmetic operations. Also, the identified keyword indices are combined into one single data point, therefore it doesn't matter how many hidden keywords there are in a certain file. Formal analysis has proven that this method is

secure. The performance analysis reveals that the ABMKS-WM system exhibits reduced computational and network delay when contrasted with previous efforts.

[9]Lianggui Liu proposed a ranked search method that effectively searches encrypted cloud data. Different from previous encrypted search methods, they employ a categorization system to arrange the documents and produce group vectors for every index, hence reducing the dimensionality of the encryption keys. In terms of total time saved for index generation, there is a net benefit. It is also easier for users to update their information because grouped vectors are created inside each entry.
When users add, edit, or remove documents, they should simply reconstruct the group vectors that correspond to the updated sets of category keywords. The authors also provide a targeted search method for feature extraction in CGIM. Instead of computing the products of all possible combinations of group vectors that match query terms in the dictionary and each index, the cloud server can use this method to increase search performance and efficiency by calculating just the products of a subset of these vectors.

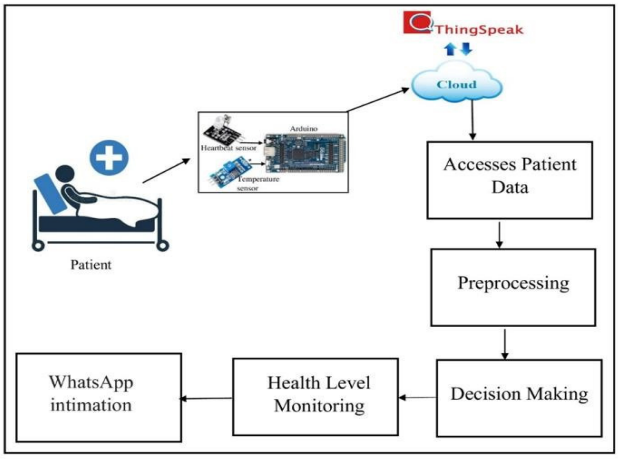
[10]For gene information from several sources stored in the cloud, Shiyue Qin proposed a private information substring searching technique to identify all instances where the query text matches the gene sequences. With the system's robust security features, several users can be set up simultaneously. The substring scan can be performed by authorized inquiries using query strings of varied lengths. This method is secure and can protect the privacy of genetic sequence data and queries, depending on the complicated mathematical problem. The ideal amount of interaction sessions and level of communicative sophistication are also achieved by the researchers. The effectiveness of this approach is high enough to warrant its application in real-world medical research.

[11]After conducting thorough research, Huanglin Shen suggests a secure and efficient method for performing ranked searches using multiple keywords via encrypted cloud data. Search times can be reduced to levels higher than logarithmic,and the approach also offers exact multi-keyword ranked searching. Gaining accurate search engine rankings is made easier with the use of vector space modeling and TF-IDF (term frequency inverse document frequency) modeling. The combination of the safe kNN computation offers protection to the technique from two distinct sorts of threats. In order to improve search performance, a BC-tree structure is used to index each page. Before encryption, a cluster of similar documents is constructed for each one.

[12]It is nevertheless impossible to ensure the efficacy of the query, even if the author assumes that the search queries would provide correct results (Hua Dai). Also, most solutions for prioritized multi-keyword searches over encrypted text are currently only available in public clouds. For use in private hybrid clouds, the authors introduce MRSEHC, an authenticated Multi-Keyword Ranking Searching. This approach, which is based on bisecting k-means segmentation, uses a keyword partition technique to distribute the vocabulary of keywords in an article evenly.

[13] Lianggui Liu has proposed a novel feature that will provide a prioritized search technique for safe cloud data. By utilizing a feature score technique, indexes are built in a manner that assigns each retrieved keyword to only one ranking dimension. This approach may lower the index dimension in comparison to constructing indexes with separate keywords. Additionally, FMRSM's trapdoor generator contains a custom-made matching score algorithm. In order to better address users' goals, the system may assign a score to the query based on the type of similarity and the quantity of matching phrases.

METHODOLOGY



The method that has been suggested to establish a patient's IOT remote health monitoring system is depicted in the system overview in Figure 1 up top. The suggested method was based in part on the execution of the procedures detailed below.

Step 1: Sensor Data Collection: The procedure begins with the patient lying in bed at home having their temperature sensor calibrated and the order attached to a board. But the microcontroller board already has the API built in, thus connecting it to the laptop serves this purpose. To supply power and collect input values, the ESP32 board connects to the sensor. The sensor can be powered on and data can be sent to the board through its respective inputs. Python is programmed onto the board with the goal of acquiring sensor data, and then it is linked. Once the Python code is uploaded to the board, it starts collecting data from the sensors right away. The Python function can access these data because they are considered input and essentially saved in a list.

The Specifications of the ESP 32 model can be seen below in the Table.

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 >500mA
Operating Temperature	-40 ℃ ~ 85 ℃
Storage Environment	-40 ℃ ~ 120 ℃
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

The connectivity circuit diagram of the ESP 32 with the temperature sensor can be seen in below figure 3:

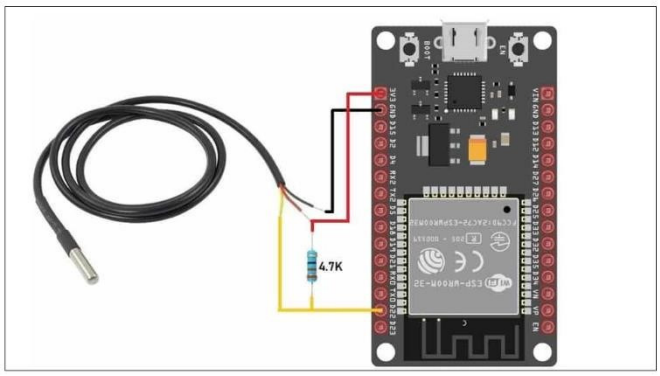


Figure 2: Circuit Diagram of the proposed model

Step 2: Preprocessing: The Python code receives the processed and propagated list of sensor input values as input. These variables search for a temperature threshold and interface successfully. Next, we decrease the strings and remove the garbage values from the preprocessed data. Then, we use the results to determine the patient's severity.

Step 3: Decision Making: The setup of the sensor allows it to be worn by the patient, together with the necessary power source. Through the use of their respective API keys, the sensor values are continuously streamed to the thing talk cloud on the designated channel and ID. All of this information is saved on the server so we can see if the sensor's readings change or go over a certain threshold when the temperature gets hot enough. When this threshold is breached, it becomes abundantly

evident that the temperature is rising beyond the acceptable level in an uncontrolled manner, and the situation might be categorized as a serious level scenario.

This decision-making module uses its if then rules to figure out what the situation is. In order to gather a current picture of the patient and notify their loved ones, the decision-making strategy sounds a voice alarm at the patient's residence. At the server end, we use the Pywhatkit module in Python to create a map URL and a message string. We then transmit this to the doctor who is caring for the patient through the WhatsApp app.

RESULTS AND DISCUSSIONS

Using Python, Spyder as the integrated development environment (IDE), and MySQL as the database, the suggested model for the intensive patient care system was constructed. The machine has a Core i5 processor and 8 GB of RAM. To find the root mean square error (RMSE), compare the actual and expected evaluations and then deduct the difference from the total. The equation below describes this procedure.

$$RMSE = \sqrt{(xp - xo)}^{\,2} \quad \text{---------- (1)}$$

Where
Xp – Expected number of Alerts
Xo – Obtained number of Alerts

Below we can see a table and graph displaying the results of the experimental evaluation, which involved processing an increasing number of patient care alerts using the suggested system.

Experiment No	Expected No of alerts	Obtained No of Alerts	MSE
1	2	2	0
2	4	3	1
3	6	6	0
4	8	7	1
5	10	10	0

Table 1: Recorded MSE

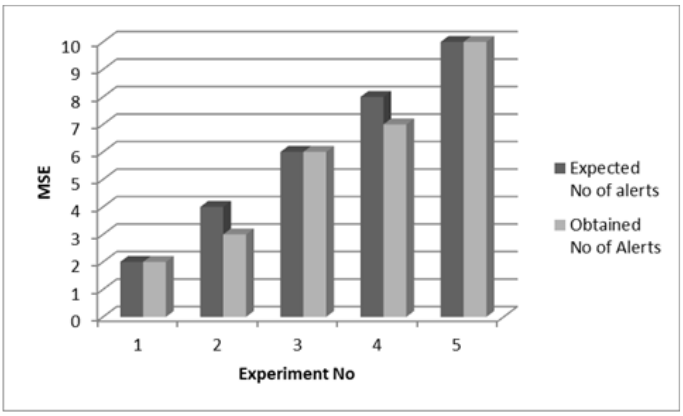


Figure 2: MSE for the Conducted experiment

The outcomes of this early intensive patient care system's first implementation demonstrate the feasibility of the proposed methodology. To assess the magnitude of the methodology's errors, we calculated the root-mean-squared error (RMSE), which provided a value of 0.624 for the proposed technique.

III. CONCLUSION AND FUTURE SCOPE

The method starts by hooking up the medical sensors to the Arduino Uno board. Following its connection to the system, the ESP 32 microcontroller begins collecting data from the sensors and transmitting it to the suggested method. This method transforms the data into a list while also encrypting it. This list is then kept on the public cloud storage called thing speak. The security of this sensor data is being compromised because most of it is being uploaded to cloud servers. There needs to be a solid substitute for current methods of data security in the healthcare industry due to the increased convenience that IoT devices and cloud platforms provide. So, this method lays forth a means to efficiently transport data from sensors to the Thing talk cloud through the IoT and the cloud. In order to monitor the patient's vitals, the server accesses this data simultaneously to preprocess it and make judgments

using WhatsApp notifications. A variety of sensors, such as those for electrocardiogram

(ECG), blood pressure (BP), and electroencephalogram (EEG), can be integrated into this system in the future to allow for real-time patient monitoring.

REFERENCES

[1] X. Gao, J. Yu, Y. Chang, H. Wang and J. Fan, ”Checking Only When It Is Necessary: Enabling Integrity Auditing Based on the Keyword With Sensitive Information Privacy for Encrypted Cloud Data,” in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 6, pp. 3774-3789, 1 Nov.-Dec. 2022, doi: 10.1109/TDSC.2021.3106780.

[2] S. Abdelfattah et al., ”Efficient Search Over Encrypted Medical Data With KnownPlaintext/Background Models and Unlinkability,” in IEEE Access, vol. 9, pp. 151129-151141, 2021, doi:10.1109/ACCESS.2021.3126200.

[3] H. Kwon and C. Hahn, ”Asymptotically Optimal and Secure Multiwriter/Multire ader Similarity Search,” in IEEE Access, vol. 10, pp. 101957-101971, 2022, doi: 10.1109/ACCESS.2022.3208962.

[4] Shubham Gade, Amita Singh, Shubham Sarote, “ Efficient H-net model-based slot assignment solution to accelerate the EV charging station searching process “,ISSN: 2349-6002,Volume:11 ,Issue: 6,PageNo: 2590-2597

[5] L. Tao, H. Xu, Y. Shu and Z. Tie, ”An Efficient Search Method Using Features to Match Joint Keywords on Encrypted Cloud Data,” in IEEE Access, vol. 10, pp. 42836-42843, 2022, doi: 10.1109/ACCESS.2022.3168730.

[6] G. Liu, G. Yang, S. Bai, Q. Zhou and H. Dai, FSSE: An Effective Fuzzy Semantic Searchable Encryption Scheme Over Encrypted Cloud Data,” in IEEE Access, vol. 8, pp. 71893- 71906, 2020, doi:0.1109/ACCESS.2020.2966367.

[7] X. Liu, T. Lu, X. He, X. Yang and S. Niu, ”Verifiable Attribute-Based Keyword Search Over Encrypted Cloud Data Supporting Data Deduplication,” in IEEE Access, vol. 8, pp. 52062-52074, 2020, doi: 10.1109/ACCESS.2020.2980627.

[8] Y. Cui, F. Gao, Y. Shi, W. Yin, E. Panaousis and K. Liang, ”An Efficient Attribute-Based Multi-Keyword Search Scheme in Encrypted Keyword Generation,” in IEEE Access, vol. 8, pp. 99024-99036, 2020, doi: 10.1109/ACCESS.2020.2996940.

[9] L. Liu and Q. Chen, ”A Novel Category Group Index Mechanism for Efficient Ranked Search of Encrypted Cloud Data,” in IEEE Access, vol. 8, pp. 54601- 54610, 2020, doi:1109/ACCESS.2020.2977430.

[10] S. Qin, F. Zhou, Z. Zhang and Z. Xu, ”PrivacyPreserving Substring Search on Multi-Source Encrypted Gene Data,” in IEEE Access, vol. 8, pp. 50472-50484, 2020, doi: 1109/ACCESS.2020.2980375.

[11] H. Shen, L. Xue, H. Wang, L. Zhang and J. Zhang, ”B+-Tree Based Multi- Keyword Ranked Similarity Search Scheme Over Encrypted Cloud Data,” in IEEE Access, vol. 9, pp. 150865-150877, 2021, doi: 10.1109/ACCESS.2021.3125729.

[12] H. Dai, Y. Ji, G. Yang, H. Huang and X. Yi, ”A Privacy-Preserving Multi- Keyword Ranked Search Over Encrypted Data in Hybrid Clouds,”

in IEEE Access, vol. 8, pp. 4895-4907, 2020, doi: 1109/ACCESS.2019.2963096.

[13] L. Liu and Q. Chen, ”A Novel Feature Matching Ranked Search Mechanism Over Encrypted Cloud Data,” in IEEE Access, vol. 8, pp. 114057-114065, 2020, doi: 1109/ACCESS.2020.3002236.

*****

