International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-9, Issue-1, 2022 Regular Edition E-ISSN: 2349-7084

Secure Smart bed on villages for monitoring and storing patient records on Cloud using IoT with Android Mobile

P. Divyaja[1], M. Kalpana Devi[2], M. Usha Rani[3]

[1]*Research Scholar,* [2]*Assoc. Professor, MCA Department, SITAMS, Chittoor,*
[3]*Professor, Department of Computer Science, SPMVV, Tirupati.*

Email ID: [2]kalpana40.melpadi@ gmail.com , [3]mur@spmvv.ac.in

**Corresponding Author:* kalpana40.melpadi@ gmail.com

Available online at: http://www.ijcert.org

Received: 10/01/2022, Revised:21/01/2022, Accepted:26/01/2022, Published: 30/01/2022

Abstract: - Wireless Sensor Networks (WSNs) are broadly used in health information departments. Virus-free and wearable sensors have become established devices to observe or monitor the threat of any illnesses. It supports patient information and their treatment tactics and protect them throughout immediate attacks. There is a complete data collected from dissimilar sensors. In this paper, we are referring to monitor the patients who suffer from diseases that can be composed and managed in a secure cloud. The important encounter is to bring out only sensitive data related to the patient's health. The paper aims to make an Internet of things (IoT) based application for patient observation. Smart bed sensor network development in health applications has been made possible by patient monitoring. We are offering Android Mobile Application (AMA) based Patient Healthcare System (PHS) using smart mobile. The smart bed sensor network's nodes are live data transmission. The proposed plan is to oversee the patient's ECG and Heart Beat Pulse using live health care datasets with strong secure algorithms.

Keywords: Cloud Computing, Smart Bed Sensor Network, IOT

---

1. Introduction

The structure of cloud activation has several layers. On the top of the layers, the applications hosted in the cloud environment are accessed by the user through the browser runs on PC or desktop and mobile devices. Cloud services and applications used by the cloud user that form the next two important layers [1]. These services and applications run on software platforms such as Oracle, SAP, .NET, etc.

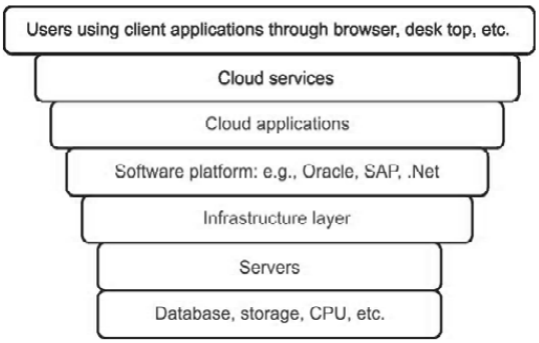

Figure 1. Cloud Computing Layers

 https://doi.org/10.22362/ijcert/2022/v9/i01/v9i0103

IoT collects and shares data directly from patients and enables them to quickly and accurately record and analyse novel data flows [2]. The technology supporting for collecting, analysing and moving data in IoT continues to mature, with the support of actuators, sensors and computing devices, which provides digital communication capabilities. For data transportation these are connected to networks. This integrated healthcare environment promotes the rapid flow of data and allows quick access to diseases such as hypertension, diabetes and heart disease. Researchers and analysts have identified some of the best advanced technologies at the Internet of Things (IoT) for health monitoring that are safe for the public and can be addressed by all [3].

The ability to collect data on their own by the devices removes the limitations of human intervention and it automatically sends data to the physician when needed. This way of automatic collection and transfer of data reduces the risk of error. For these sensors are used to collect detailed physical information and uses gateways and clouds to research and store information, which then sends the analysed data through wireless to custodians for further analysis and review. It changes the method of getting a specialist at the right interval to see the patient's important symptoms, instead of providing continuous automated information. Here, it simultaneously improves the maintenance standard through consistent attention and reduces maintenance costs by eliminating the need to actively improve the caregiver's performance in data collection and analysis. Powerful wireless solutions connected via IoT devices now make it possible to see patients information [4]. These solutions use sophisticated algorithms to securely capture patient data from the spread of sensors, research information, share it over a wireless network, and provide appropriate health recommendations to patients.

2. Internet of Things

The Internet of Things (IoT) devices directly collects and shares information from patients and it enables to record and analyse new data streams accurately and quickly [5]. The technology development for collecting, analysing and moving data in IoT, with the support of actuators, sensors and computing devices continues to improve, which provides digital communication capabilities. This integrated healthcare environment promotes the rapid flow of data and allows quick access to diseases such as hypertension, diabetes and heart disease. In these Internet of Things (IoT), researchers and analysts have jointly identified the best advanced technologies for health monitoring and it is safe for the public and is addressed by all.

The Internet of Things has grown exponentially over the past decade and is still a growing trend for researchers in both academia and industry. Many of the results of IoT reported in the literature provide meaningful definitions. According to the Casagrass Paper: "Global network infrastructure that connects physical and virtual objects through the exploitation of cognitive and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It is the basis for the occurrence of independent collaborative services and applications because it provides specific object recognition, sensor and connection capabilities. CERP emphasizes Internetworking between different 'smart' devices such as sensors, actuators, computers and smart phones and hence the use of services on the web. Any application development framework for IoT should, therefore, support these diverse devices.

3. Smart Hospital Beds Enabling Effective Patient Monitoring

Smart hospital beds have a foreign monitoring system that monitors the patient. Smart hospital beds have sensors for blood heat, pulse, blood oxygen and pressure [6]. All of those signs are necessary and necessary for physicians to look after the health of patients. This technique can be found in hospital beds and transmits all patient signals to the supervisor, especially in cases where intensive treatment is required. This important information is sent to the hospital central system and allows the patient supervisor to immediately review and monitor the patient's cells. Additionally, this technique sends alert messages or signals to supervisors in the event of any sudden change in the patient's condition. Hospitals had to monitor the condition of patients so that they could spend more time for a patient, while the person was in bed. Smart beds provide an excellent solution for health care providers to constantly monitor patients to provide better care for patients [7]. Such sophisticated beds with monitoring equipment will not place a burden on the hospital staff to see the patient's condition. In addition, smart beds have proven to be a tool for health providers to diagnose and stop unplanned bed departures.

The smart hospital beds market is in a growing phase and is expected to make an impression on medical devices with its commercial growth. There are a number of factors contributing to this market expansion, such as rising

comfort from hospitals, rising health care costs, continued technological advances, and chronic diseases [8]. However, the high cost of such sophisticated beds has limited the acceptance of smart beds and is a serious obstacle to the expansion of this market.

The Asia Pacific smart hospital bed market is expected to grow at a large growth rate due to the privatization of hospitals in major countries including China, India, Indonesia and Thailand. Furthermore, factors such as the aging population and rising health care costs in the region are expected to contribute to the expansion of the smart hospital beds market in the Asia-Pacific region. Hospitals in major countries, including China, Japan, India, Indonesia, Thailand and Malaysia, are using mobile health monitoring systems in the Asia-Pacific region, with high demand for smart hospital beds [9].

4. Existing Algorithm

In the existing system we use blowfish algorithm for encryption and decryption purpose. Blowfish can be a symmetric encryption algorithm that uses a secret key similar to encrypted and decrypted messages. Blowfish block cipher separates the message into fixed length blocks during encryption and decryption. 64 bits block length for blowfish; The dimensions of the eight byte coefficient should be thicker [10].

Algorithm Pseudo code

1. Begin Item
2. This Blowfish Algohas 16 rounds.
3. The input is a 64-bit data element, Y.
4. YL, YR. i.e., Divide x into two 32-bit halves:
5. Then, for j = 1 to 16:
6. YL = YL XOR Qi
7. YR = E(YL) XOR YR
8. Swap YL and YR
9. After the sixteenth round, swap YL and YR again to undo the last swap.
10. Then, YR = YR XOR Q17 and YL = YL XOR Q18.
11. Finally, recombine YL and YR to get the ciphertext.

The encryption is exactly the same as the encryption, except that Q1, Q2, ..., Q18 are used in reverse order. Blowfish's operations that require high speed must unroll the loop and ensure that all sub keys are stored in the cache [11].

Table 1 . Existing Blowfish Algorithm

File size	encryption/decryption time	CPU time
100	2050	1563
200	3800	3005
450	4500	3986
550	5680	5123
900	6956	6258
950	7865	7102
1020	8100	8200
1100	8400	8700
1200	8600	9010
1300	9101	9400

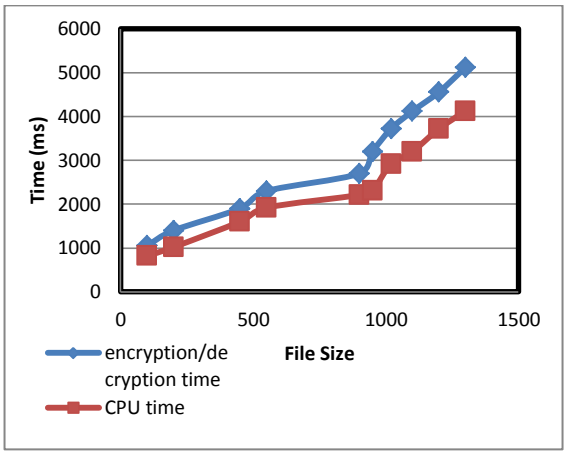

Figure 2. Existing Blowfish Algorithm Graph

5. Proposed Algorithm

In proposed system we implement Temporary key encryption and Description algorithm to make more secure way to transmit cloud data from one end to another end[12].

5.1 Temporary key Encryption and Decryption

In this concept we've to implement temporary key whenever search keyword is going to be changed. The search keyword is that the file attribute. With rapid development in databases, networking, and computing technologies, an outsized number of knowledge are often

analyzed individually, resulting in the high consumption of knowledge mining tools to predict trends and patterns. it's raised universal concerns over the privacy of people.

Data records are often obtained by removing key identifiers like personal records, name and social-security numbers. However, the opposite record features (commonly referred to as the quasi-identifier) are wont to accurately identify personal records. For instance, the name, birth, gender, disease and zip are available publicly like the list of voters. When these features are available within the data set, like medical data, they will identify the corresponding person by linking the operation with a high probability. this is often the first dataset

Table 2. Data records

Name	DOB	Gender	Zipcode	Disease
Anu	11-10-1991	Female	876767	Cancer
Abirami	13-04-1993	Female	675656	Cancer
Banu	11-09-1994	Female	874545	Flu
Devi	10-09-1888	Female	657676	Cancer
Lakshmi	09-09-1883	Female	675656	Cancer
Rahul	11-11-1992	Male	766767	Cancer

After the data hiding encryption, the data are shown as below format

Table 3. Data format after hiding encryption

Name	DOB	Gender	Zipcode	Disease
Anu	1991	Female	876**	Cancer
Abirami	1993	Female	675**	Cancer
Banu	1994	Female	874**	Flu
Devi	1888	Female	657**	Cancer
Lakshmi	1883	Female	675**	Cancer
Rahul	1992	Male	766**	Cancer

The data uploader uploads the data in the cloud. After that whoever want to get the data, they need to get the access permission from data uploader. After that the data user use the key and access the data. The key generates as time based. Every 15 minutes the key will be changed. Every time the user needs the data uploader permission.

The algorithm definition is

Step 1: (Authentication) Setup(1^{λ}): It runs on cloud algorithm. It maintains the security parameter λ as input and authenticates based on the username and password.

Step2: Encrypt Crypt (k; tmi; Ats; username; password): This algorithm generates a searchable cipher associated with the keyword k and allows a set of attribute time to encrypt tmi, which is determined by the data uploader.

Step 3:sk←TokenGen(w; [tm_s,tm_e]): The information user runs this algorithm to make the search keyword sk for pointed the ciphertexts which are encrypted in the time interval [tm_s; tm_e], and contain the keyword w, according to its username and password authentication.

Step 4 : (true,false) := Search(cipher; sk): For each stored cryptographic cipher and the received search keyword sk it is associated with a specific keyword w and attribute set Ats, which will be true if all of the following conditions are met simultaneously :Tr(Ats) = true,

Cipher*←Encrypt(w^{*},tm_i,Ats)
St^{*}←KeywordGen(w*,tm_s,tm_e)
tm_i € [tm_s,tm_e]
Otherwise, it is incorrect.

In this new primitive state, the access control system creates a cipher that each data uploader can search for an arbitrary keyword and encryption time. Each data user searches for a keyword over a period of time, generating a search keyword that is valid over a period of time. Data users can create a search keyword by interacting with the data uploader. Based on the search keyword obtained, the cloud server can see the documents encrypted contains the intended keyword and are generated over a period of time. It provides a search result for data users who have fulfilled the access control policy implemented by the data uploader.

Table:4 Temporary key Encryption and Decryption Graph

	Access Time in ms	
File size	encryption/decryption time	CPU time
100	1050	820
200	1400	1020
450	1900	1600
550	2300	1920
900	2700	2210
950	3200	2310
1020	3721	2920
1100	4120	3200

1200	4560	3720
1300	5120	4129

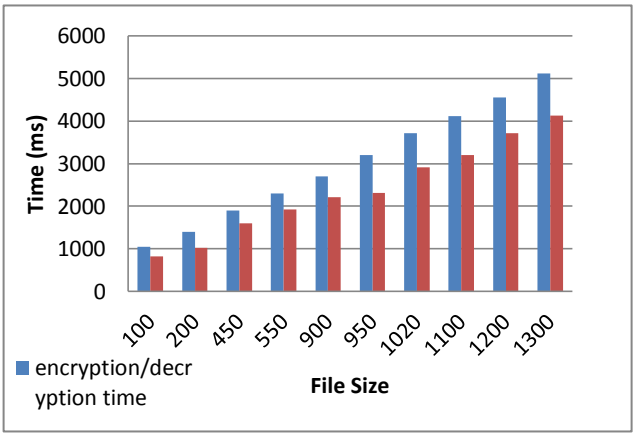

Figure 3. Temporary key Encryption and Decryption Graph

6. Conclusion

Aiming at current issues in the health monitoring system, a safe health care system using a body sensor network is proposed in this paper. The app meets standards such as recording, collecting and presenting real-time body vitals to relevant professionals. It can be calibrated in a very short period of time and can be made any number of measurements. Because there is a limited record interval for specific information.

References:

[1].AzzamSleit, Nada Misk, FatimaBadwan, Tawfiq Khalil(2013),Cloud Computing Challenges With Emphasis On Amazon Ec2 And Windows Azure, IJCNC, Vol.5, No.5, DOI : 10.5121/ijcnc.2013.5503.

[2] ProsantaGope et al. 2016. BSN-Care: A Secure IoTbased Modern Healthcare System Using Body Sensor Network. IEEE Sensors Journal. 16(5): 1368-1376.

[3] Tzonelih Hwang et al. 2016. Untraceable Sensor Movement in Distributed IoT Infrastructure. IEEE Sensors Journal. 15(9): 5340-5348.

[4] Tae-Yoon Kim et al. 2015. Multi-Hop WBAN Construction for Healthcare IoT Systems. IEEE Platform Technology and Service (PlatCon), International Conference. pp. 27-28.

[5] CharalamposDoukas et al. 2015. Bringing IoT and Cloud Computing towards Pervasive Healthcare. IEEE Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), International Conference. pp. 922-926.

[6] Tianhe Gong et al. 2015. A medical Health care system for privacy protection based on IoT. IEEE Parallel Architecture, Algorithms and Programming (PAAP). pp. 217-222.

[7] Lin Yang et al. 2014. A Home Mobile Healthcare System for Wheelchair Users. Proceedings of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design. pp. 609-614.

[8] J. Wu, S. Yuan, S. Ji, G. Zhou, Y. Wang, and Z. Wang, "Multi-agent system design and evaluation for collaborative wireless sensor network in large structure health monitoring," Expert Systems with Applications, vol. 37, no. 3, pp. 2028–2036, 2010.

[9] K. Liu, C. Wang, and S. Liu, "A novel mobile data collection algorithm for wireless sensor networks," Adhoc& Sensor Wireless Networks, vol. 36, no. 1-4, pp. 285–311, 2017.

[10] S. Vaudenay, "On the Weak Keys in Blowsh," Fast Software Encryption, Third International Workshop Proceedings, SpringerVerlag, 1996, pp. 27-32.

[11]. P. Karthigai Kumar and K. Baskaran. 2010. An ASIC implementation of low power and high throughput blowfish crypto algorithm. Microelectron. J. 41, 6 (June 2010), 347-355.

[12] Public Key Cryptography - Applications Algorithms and Mathematical Explanations

