IoT BASED SECURE TRANSACTION IN REMOTE PATIENT MONITORING USING CRYPTOGRAPHY TECHNIQUES

*C.Preethika** [1], *E.J.Thomson Fredrik* [2]

ABSTRACT

Remote patient monitoring involves using technology to collect health data from individuals in one location and electronically communicating that information to healthcare sources in aaltered location. This allows healthcare professionals to monitor patients' conditions remotely. Health data collected by IoT devices are transmitted over the internet. While data transaction, security challenges are faced in remote patient monitoring .Safeguarding sensitive patient information is crucial to prevent from unauthorized access. In this article purpose cryptographic algorithm is used to prevent data during transaction,AES (Advanced Encryption Standard) and Blowfish algorithm is used in a hybrid encryption approach for securing data in remote patient monitoring. In this paper, IoT devices like SPO2 (blood oxygen saturation), temperature, and heart pulse sensors involves the continuous collection and transmission of vital signs from patients to healthcare providers. The integration of wearable devices and a secure remote monitoring system enhances the ability to detect and address medical issues promptly.Using a hybrid encryption approach with both AES and Blowfish can enhance security, mitigate various Cyber Attack and can do secure transaction in IoT. This combination helps protect against attacks such as brute-force attacks, cryptanalysis, and vulnerabilities specific to each algorithm. Additionally, it adds an extra layer of defense by diversifying the encryption methods, making it more challenging for attackers to exploit potential weaknesses in a single algorithm. The implementation result of this hybrid algorithm ensures confidentiality, integrity, authentication and trust in remote patient monitoring systems. In essence, the future of secure transactions in remote patient monitoring lies in a dynamic, adaptive approach that integrates cutting-edge technologies to fortify the overall cybersecurity posture and safeguard patient data with the highest level of resilience.

Keywords: Advanced Encryption Standard, Blow fish, Cryptography, Healthcare, Hybrid encryption, Internet of Things(IoT)

I. INTRODUCTION

IoT refers to the network of interconnected physical devices that communicate and exchange data over the internet to enhance various aspects of patient care, monitoring, and management. devices, equipped with sensors and connectivity, can collect, share, and act upon information to enable smart applications and services in various domains. IoT devices in remote patient monitoring offer real-time health data, enabling timely interventions, reducing hospitalizations, enhancing patient independence, and providing healthcare professionals with comprehensive insights for personalized care. This interconnected network of devices facilitates the collection and exchange of health-related data, promoting efficiency and improving patient outcomes. IoT in healthcare aims to improve patient outcomes, enhance preventive care, streamline processes, and provide more personalized and efficient healthcare services.

Temperature Monitoring monitors the patient's body temperature is crucial for identifying potential infections, inflammatory conditions, or abnormalities and helps in assessing the effectiveness of treatments and interventions. Digital thermometers or wearable temperature sensors. Continuous temperature monitoring aids in early detection of fever or hypothermia, enabling timely medical interventions. SPO2 (Oxygen Saturation) Monitoring measures the percentage of oxygen saturation in the patient's blood, indicating how well oxygen is being transported to the body's

Department of Computer Technology[1]
Karpagam Academy of Higher Education, Coimbatore, India[1]
preethi150702@gmail.com[1]
Department of Computer Technology[2],
Karpagam Academy of Higher Education, Coimbatore, India[2]
thomson500@gmail.com[2]

* Corresponding Author

tissues. It's crucial for assessing respiratory function and detecting conditions like hypoxemia. Continuous SPO2 monitoring is vital for early detection of respiratory distress, especially in patients with respiratory conditions. Heart Pulse Monitoring measures the heart rate, providing insights into cardiovascular health and overall cardiac function. It's essential for detecting irregularities, arrhythmias, or abnormal heart rates .Continuous heart pulse monitoring assists in early identification of cardiac issues, enabling prompt medical attention. While sharing a data from IoT devices to Website, security issue is the most common problem in using remote patient monitoring.

Some of the specific challenges are confidentiality, data integrity, key management, resistance to attacks, adaptability, performance, quantum resistance, and secure communication issues in the context of remote patient monitoring (RPM).

Addressing these issues requires a comprehensive security strategy and privacy of patient data in remote monitoring scenarios. AES and Blowfish are commonly used symmetric key encryption algorithms that can be employed together as part of a hybrid encryption approach to provide a more secure and efficient encryption process. AES is known for its speed and strong security, making it suitable for encrypting larger volumes of data efficiently. The remaining sections are literature review, proposed work, methodology, result and discussion, conclusion and future work.

II. LITERATURE REVIEW

IOT devices like temperature, heart pulse, blood pressure and oxygen meter are used to measure the real time data of the patients in healthcare. An alert system is used for the timely detection and notification of abnormal health parameters, enabling swift medical intervention to prevent or address potential health complications. Using an alert system cause the possibility of false alarms, Which an lead to unnecessary anxiety for the patient and healthcare providers, as well as potential overuse of medical resources. [1]

Wireless sensor network is mainly used for data assortment in remote patient monitoring. Wireless sensor networks facilitate seamless data collection in remote patient monitoring by deploying sensors to measure vital signs and transmit real-time health data wirelessly. Wireless communication introduces security considerations. [2]

Sensors are used to collect real time patient data, and helps healthcare providers assess and manage patients from distance. This enables healthcare professionals to remotely monitor patients, ensuring timely interventions and personalized care. This interference may lead to signal degradation, data packet loss, or even temporary loss of connectivity between the wireless sensors and the monitoring system. [3]

Automation through RFID tags reduces the risk of errors associated with manual data entry. By scanning RFID tags, healthcare providers can access accurate and up-to-date patient information, minimizing the chances of administering the wrong medication or treatment. RFID tags transmit and store patient information wirelessly. If proper security measures are not in place, there is a risk of third party access to this personal data. Without robust encryption and authentication protocols, RFID data may be susceptible to hacking or interception. [4]

Certificate less public key cryptography eliminates the need for digital certificates, streamlining key management processes. In traditional public key infrastructures, digital certificates are used to verify the authenticity of public keys. Certificate less public key cryptography is not as standardized as traditional public key infrastructure (PKI) systems that rely on digital certificates. The lack of standardized protocols can lead to interoperability challenges when integrating different systems or devices. [5]

Using genomic data and chaos theory for encryption in remote patient monitoring can provide a high level of security. Genomic data, being unique to individuals, adds a personalized layer of encryption. Chaos theory introduces further safeguarding sensitive health information. Disadvantage of using genomic and chaos as an encryption method in remote patient monitoring is the potential for increased computational complexity. Analyzing genomic

data and implementing chaos-based algorithms may require significant computational resources, leading to slower processing times and potential challenges in real-time monitoring scenarios. [6]

AES is a widely adopted and standardized encryption algorithm, known for its robustness and efficiency. Regular key management practices are crucial to mitigate this risk and maintain the effectiveness of AES encryption.[7]

Block chain offers advantages like data integrity and decentralized control. Using block chain in monitoring comes with challenges like scalability issues, high energy consumption and complexity. [8]

Blow fish as individual algorithm provides strong encryption, enhancing the security of sensitive patient data during transmission. Blow fish is an older encryption algorithm, and while it's still secure the fixed key size may limits its adaptability. [9]

Cryptographic algorithms are essential for securing financial transactions, authentication processes, and other critical operations in cloud based applications. Managing cryptographic keys in the cloud can be more complex than in traditional databases. Key distribution, rotation, and secure storage become challenging, and any compromise in key management can lead to security vulnerabilities. [10]

A database like PREDICT RM may incorporate predictive analytics algorithms. These algorithms can analyse patient data over time, identifying patterns and trends that may indicate potential health issues or deterioration in a patient's condition. Patients and healthcare providers need assurance that their data is protected against cyber threats and unauthorized use.[11]

During Pandemic time like COVID-19, Remote patient monitoring will be more helpful like finding first stage of COVID like, monitoring Heart pulse, oxygen level and temperatures. Patients may worry about the security of their health information, leading to hesitancy in adopting remote monitoring technologies. [12]

Disruption Tolerant Networking is used to ensure data delivery even in scenarios with intermittent or unreliable network connectivity. While DTN is designed to handle intermittent connectivity, the inherent delay-tolerant nature of the network may lead to slower data delivery. In time-sensitive healthcare situations, such delays could impact the promptness of medical interventions or decision-making based on real-time patient data. [13]

While Arduino and Proteus are popular tools for prototyping and small-scale projects, they may face limitations in terms of scalability when it comes to large-scale and robust remote patient monitoring systems. Building and maintaining a scalable, enterprise-grade solution for remote patient monitoring often requires professional support, specialized hardware, and dedicated software platforms. [14]

It can be prevented using Block chain encryption .While Block chain provides decentralized security features, it may not be the most efficient choice for remote patient monitoring due to its inherent complexity, performance overhead, and scalability challenges compared to dedicated encryption. [15]

In IoT based healthcare the design and implementation are discussed in this paper. This limitation can affect the device's ability to handle advanced data analytics, real-time processing, or support multiple sensors simultaneously, potentially impacting the overall performance and responsiveness of the monitoring system. [16]

DS18B20 temperature sensor with Arduino is used for health monitoring. It can measure body temperature, ambient temperature, or other relevant data. Connect the DS18B20 to the Arduino and can monitor temperature readings. But, Factors such as self-heating or response time variations in the DS18B20 may affect its performance in dynamic environments. This could be a consideration in scenarios where rapid changes in temperature need to be monitored accurately. [17]

The Thing Speak library for Arduino is commonly used in remote patient monitoring. Thing Speak library to send data from sensors (e.g., temperature, heart rate) connected to an Arduino to the Thing Speak platform. This enables remote monitoring, data logging, and real-time visualization through charts and graphs. However, when using a third-party cloud service like Thing Speak, there may be concerns related to data privacy and security. [18]

Tele health is used for connecting with your health care provider online safe and secure. Access to high-quality healthcare facilities and improved emergency services are among the better healthcare choices it provides. [19] Wireless Body Area Network implementation in remote patient monitoring involves utilizing wearable sensors to collect and transmit health-related data to a centralized system. These networks enable real-time monitoring and enhance healthcare delivery. The presence of other wireless networks, electronic devices, or physical obstacles may disrupt or weaken the communication signals between the body-worn sensors and the monitoring system. This interference can result in data packet loss, delays, or even complete communication failures. [20]

III. PROPOSED WORK

Using AES and Blowfish as a hybrid algorithm in remote patient monitoring offers several benefits compared to using individual algorithms. The combination provides a layered security approach, leveraging the strengths of both AES and Blowfish to enhance overall data protection. As data is collected from IoT sensors, the initial step involves encrypting this sensitive information using the Advanced Encryption Standard (AES). AES, known for its robust security and computational efficiency, ensures that the collected data remains confidential during transmission.. To address this, the hybrid approach incorporates Blowfish, a symmetric key algorithm with a distinct encryption process. The AES key is encrypted using Blowfish, adding an extra layer of security to the key exchange process. This hybrid encryption strategy combines the strengths of both algorithms—AES for efficient and secure data encryption and Blowfish for a protected key exchange mechanism. By leveraging AES and Blowfish in tandem, the hybrid algorithm helps safeguard sensitive patient data during its journey from IoT sensors to websites. This approach mitigates potential vulnerabilities associated with individual algorithms, providing a robust and well-rounded security framework for remote patient monitoring transactions in the evolving landscape of healthcare IoT.

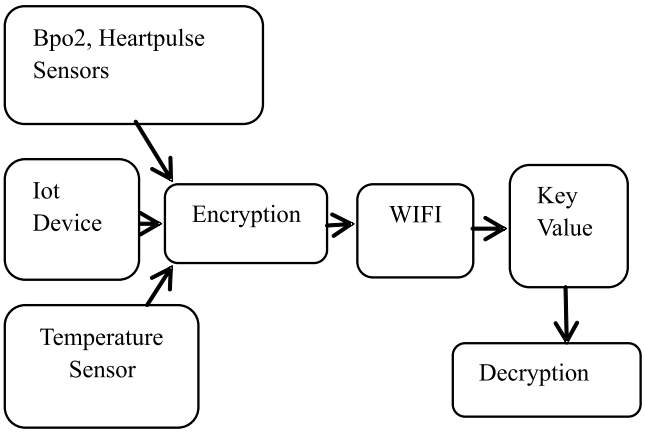

Figure 1. Block diagram of Secure Remote Patient Monitoring

IV. METHODOLOGY

Real time data was composed from IoT devices by using its sensors. The three IoT devices used for monitoring the patient's health conditions. It helps to monitors oxygen levels, crucial for respiratory health, and detects potential issues like hypoxemia. Temperature sensors track a patient's body temperature. Data is sent in real-time through IoT connectivity for continuous monitoring. It helps identify fever, a common symptom in various illnesses, providing early detection and intervention.DS18B20 is used as temperature sensor to get data from patient and helps in monitoring temperature level. Pulse sensors capture the heart rate of the patient. Transmitting heart rate data through IoT enables real-time monitoring by healthcare professionals. Monitor cardiovascular health, aids in identifying irregularities or abnormalities in heart rate.MAX30100 is also acting as heart rate sensor and helps to monitor the patient's heart rate. This sensor is used to get real time data for monitoring. MAX30100 and DS18B20 sensors are used for collecting the data of blood oxygen level, temperature, and heart pulse. The integration of SPO2, temperature, and heart pulse sensors as IoT devices in remote patient monitoring enhances healthcare by providing real-time data for better diagnosis, early intervention, and improved patient outcomes.

Arduino is an open-source electronics platform that combines programmable hardware with an easy-to-use

software environment. It consists of a microcontroller-based board and an Integrated Development Environment (IDE) for writing and uploading code. Designed to simplify microcontroller programming, Arduino provides an accessible and flexible framework for developers and hobbyists. Its adaptability makes it valuable in various fields, including healthcare, where it enables the development of innovative medical and assistive devices.

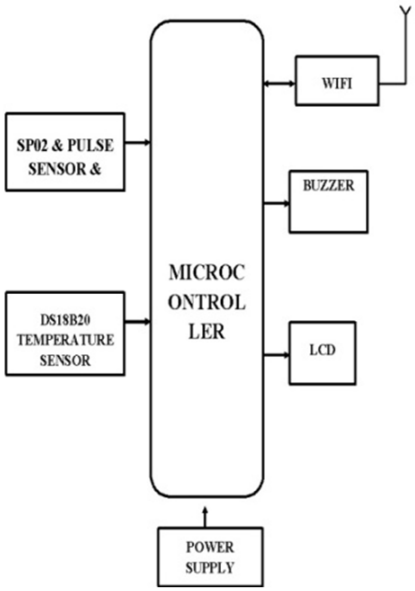

Figure 2. Methodology of overall circuit board

Buzzer is also connected to an Ardiuno board. A buzzer is a signaling device that consists of switches or sensors linked to a control unit. When a button is pressed or a set time elapses, the control unit activates a light on the corresponding button or panel. It then produces an alert through a continuous or intermittent buzzing or beeping sound.

For power supply, the proper operation of an electronic device or product, a reliable power supply unit (PSU) is essential. Built into the device, this power supply unit converts AC mains voltage to an appropriate level of DC voltage. The Switching Mode Power Supply (SMPS) is the most commonly used type of power supply circuit, efficiently transforming AC mains power to 12V DC with its designated current rating

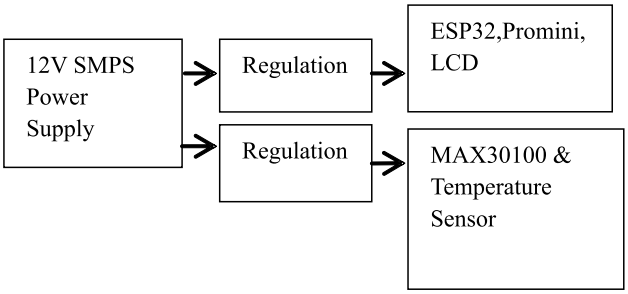

Figure 3. Power Supply between Sensor Board and Arduino Board

The ESP32, with its built-in Wi-Fi capabilities, can be utilized in various healthcare applications to enable connectivity, remote monitoring, and data transmission. This device enables real-time health data transmission to a website via Wi-Fi, facilitating remote patient monitoring and timely interventions. Compared to the ESP-12e, the ESP32 offers significant improvements, including a more powerful CPU, faster Wi-Fi connectivity, and additional GPIO pins, particularly for analog inputs. It also supports Bluetooth 4.2 and Bluetooth Low Energy. Moreover, the board features touch-sensitive pins and integrates built-in Hall Effect and temperature sensors.

The ESP-WROOM-32 is widely utilized in IoT applications because of its integrated Wi-Fi and Bluetooth features. It enables devices to establish internet connectivity and communicate wirelessly with other systems.

A. System Design

The ESP32, MAX30100, TEMPERATURE SENSORS require 3.3V while LCD, PRO-MINI use 5V DC for their operation and relay modules need 12V DC for their procedure. The ESP32 can operate using either a USB connection or a 12V adapter with a 5V DC regulated power supply. As the voltage supply and ground pins of other modules share a common VCC and ground, the components receive power from the regulator's 5V output. The system's LCD is connected to the I2C 21st and 22nd pins, enabling serial communication. A buzzer is linked to the digital 4th pin of the ESP32. The LCD display presents sensor-scanned values.

The temperature sensor is linked to 15th digital pin of esp32 as one wire communication input to monitor patient body temperature, system alerts if temperature value exceeds. MAX30100 SPO2 and HEART PULSE sensor is connected to Arduino pro-mini controller in order to continuously scan and send the spo2 and heart pulse value to ESP32 via UART Communication. ESP32 Reads SPO2 and Heart Pulse value and displays in LCD. Also alerts when Heart Pulse and SPO2 are in abnormal.All parameters can be monitored remotely using IoT (Internet of things) via online server by updating the entry of patient parameters every minute and also updates warnings online in any abnormal cases.

B. System Implementation

In RPM, the asymmetric algorithm may be used to exchange a symmetric key, enabling subsequent data encryption using a symmetric algorithm like AES or Blowfish. Before initiating data transmission, a symmetric key is generated for use in encrypting the sensitive patient information. Subsequently, the AES algorithm is employed to encrypt the patient health data, ensuring its confidentiality during transit. To address the secure exchange of the symmetric key, the AES key is further encoded using the Blowfish algorithm. This two-layered encryption process fortifies the key exchange mechanism, mitigating risks associated with potential interception.Once the encrypted data, along with the Blowfish-encrypted AES key, reaches its destination on the website, the decryption process is initiated. The Blowfish key, which was securely shared between the IoT devices and the server, is utilized to decrypt the AES key. Subsequently, the decrypted AES key is employed to decrypt the patient health data. This meticulous decryption process ensures that only authorized entities possessing the appropriate keys can access and interpret the sensitive health information. Ultimately, the hybrid algorithm's application of AES and Blowfish shows a pivotal part in preserving the reliability and privacy of patient data throughout the remote patient monitoring process.

V. RESULT AND DISCUSSION

Table 1: Decryption Data using AES and Blowfish algorithm

S.No	Date	Decrypted Temperature	Decrypted Heart Pulse	Decrypted spo2
1	08-03-2024 08:10:48	36	97	96
2	08-03-2024 08:09:33	36	100	96

In secure transaction of remote patient monitoring, we implemented a hybrid encryption approach utilizing the AES (Advanced Encryption Standard) and Blowfish algorithms. channel for transmitting sensitive patient health data. The encryption process effectively safeguarded the confidentiality and integrity of the information exchanged between remote patient monitoring devices and the central monitoring system.

By leveraging both AES and Blowfish, the system not only meets industry standards but also addresses the dynamic nature of IoT devices and the critical nature of health data. The encryption provided by this hybrid algorithm ensures confidentiality, integrity, and authenticity, essential pillars for maintaining trust in remote patient monitoring systems.

VI. CONCLUSION

From the result the implementing of hybrid algorithm with AES and Blowfish in remote patient monitoring offers a comprehensive solution for securing data during transactions from IoT devices to healthcare professionals. AES brings efficiency and widespread acceptance, ensuring swift encryption of vital signs such as temperature, BPO2, and heart pulse. Complementarily, Blowfish adds an extra layer of security with its unique algorithm, contributing to a robust defense against potential threats. In conclusion, the AES and Blowfish hybrid algorithm stands as a robust solution, effectively securing patient data transactions in the realm of remote healthcare monitoring. It's essential to keep these algorithms up-to-date and follow best practices in key management, protocol design, and implementation to ensure the highest level of security in remote patient monitoring systems. In essence, the future of secure transactions in remote patient monitoring lies in a dynamic, adaptive

approach that integrates cutting-edge technologies to fortify the overall cyber security posture and safeguard patient data with the highest level of resilience.

REFERENCES

[1] Warsi, G. G., Hans, K., &Khatri, S. K. (2019, February). IOT based remote patient health monitoring system. In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 295-299).IEEE.

[2] Malasinghe, L. P., Ramzan, N., &Dahal, K. (2019). Remote patient monitoring: a comprehensive study. Journal of Ambient Intelligence and Humanized Computing, 10, 57-76.

[3] Hilty, D. M., Armstrong, C. M., Edwards-Stewart, A., Gentry, M. T., Luxton, D. D., &Krupinski, E. A. (2021). Sensor, wearable, and remote patient monitoring competencies for clinical care and training: scoping review. Journal of Technology in Behavioral Science, 6, 252-277.

[4] Ahmed, M. I., &Kannan, G. (2022). Secure and lightweight privacy preserving Internet of things integration for remote patient monitoring. Journal of King Saud University-Computer and Information Sciences, 34(9), 6895-6908.

[5] Hamoud, O. N., Kenaza, T., Challal, Y., Ben-Abdelatif, L., &Ouaked, M. (2022). Implementing a secure remote patient monitoring system. Information Security Journal: A Global Perspective.

[6] Aledhari, M., Marhoon, A., Hamad, A., &Saeed, F. (2017, July).A new cryptography algorithm to protect cloud-based healthcare services. In 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE) (pp. 37-43). IEEE.

[7] Sandhiya, D. S., Karthikeyan, M. V., &Priya, M. S. (2022). Secured Health Monitoring System Using AES. East Asian Journal of Multidisciplinary Research, 1(6), 1175-1182.

[8] Pighini, C., Vezzoni, A., Mainini, S., Migliavacca, A. G., Montanari, A., Guarneri, M. R., ...&Cesareo, A. (2021). SynCare: An innovative remote patient monitoring system secured by cryptography and blockchain. In IFIP International Summer School on Privacy and Identity Management (pp. 73-89). Cham: Springer International Publishing.

[9] Hussaini, S. (2020). Cyber security in cloud using blowfish encryption. Int. J. Inf. Technol.(IJIT), 6(5).

[10] R. S. Devi and M. M. Kumar, "Testing for Security Weakness of Web Applications using Ethical Hacking," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India, 2020, pp. 354-361, doi: 10.1109/ICOEI48184.2020.9143018.

[11] Rajarathna, S. N. A Study on Different Types of Cryptographic Algorithms in Securing Cloud Based HealthCare Services.

[12] Hummel, J. P., Leipold, R. J., Amorosi, S. L., Bao, H., Deger, K. A., Jones, P. W., ... &Akar, J. G. (2019). Outcomes and costs of remote patient monitoring among patients with implanted cardiac defibrillators: an economic model based on the PREDICT RM database. Journal of Cardiovascular Electrophysiology, 30(7), 1066-1077.

[13] Sabukunze, I. D., Setyohadi, D. B., &Sulistyoningsih, M. (2021, April). Designing an Iot based smart monitoring and emergency alert system for Covid19 patients. In 2021 6th International Conference for Convergence in Technology (I2CT) (pp. 1-5). IEEE.

[14] Yaacoub, E., Abualsaud, K., Khattab, T., &Chehab, A. (2020). Secure transmission of IoTmHealth patient monitoring data from remote areas using DTN. IEEE Network, 34(5), 226-231.

[15] Mihat, A., Saad, N. M., Shair, E. F., Aslam, A. B. N., & Rahim, R. A. (2022). SMART HEALTH MONITORING SYSTEM UTILIZING INTERNET OF THINGS (IoT) AND ARDUINO. Asian Journal Of Medical Technology, 2(1), 35-48.

[16] Pham, H. L., Tran, T. H., & Nakashima, Y. (2018, December).A secure remote healthcare system for hospital using blockchain smart contract. In 2018 IEEE

[17] Ashraf, S., Khattak, S. P., &Iqbal, M. T. (2023).Design and Implementation of an Open-Source and Internet-of-Things-Based Health Monitoring System. Journal of Low Power Electronics and Applications, 13(4), 57.globecom workshops (GC Wkshps) (pp. 1-6).IEEE.

[18] Saha, R., Biswas, S., Sarmah, S., Karmakar, S., & Das, P. (2021). A working prototype using DS18B20 temperature sensor and arduino for health monitoring. SN Computer Science, 2, 1-21

[19] P. GURUNATHAN and R. S. DEVI, "RSA Cryptography and GZIP Steganography Techniques for Information Hiding and Security using Java," 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2023, pp. 654-659, doi: 10.1109/ICOEI56765.2023.10125906.

[20] Hartalkar, A., Kulkarni, V., Nadar, A., Johnraj, J., &Kulkarni, R. D. (2020, September).Design and development of real time patient health monitoring system using Internet of Things. In 2020 IEEE 1st International Conference for Convergence in Engineering (ICCE) (pp. 300-305). IEEE.

[21] Schultz, M. A. (2023). Telehealth and Remote Patient Monitoring Innovations in Nursing Practice: State of the Science| OJIN: The Online Journal of Issues in Nursing. Online Journal of Issues in Nursing, 28(2).

[22] Majeed, J. H., &Aish, Q. (2021). A remote patient monitoring based on WBAN implementation with internet of thing and cloud server. Bulletin of Electrical Engineering and Informatics, 10(3), 1640-1647.