A Novel method of IoT security System for Remote Patient's Health monitoring and Alert System

Dr. AmanDeep Singh[1], Dr. P. Devi[2], Dr. Sankit Ramkrishna Kassa[3], Rishu Kumar[4], Mr Veeramani Ganesan[5], Dillip Narayan Sahu [6]*

[1]Professor & Deputy Dean, Department of Computer Science & Engineering, Gulzar Group of Institutions, Ludhiana, Punjab, India.

[2]Assistant Professor, School of Social Sciences and Humanities, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India.

[3]Assistant Professor, Department of Electronics and Telecommunication Engineering, Symbiosis Institute of Technology, Symbiosis International Deemed University, Pune, India.

[4]Computer Science and Engineering, Institute of Technical Education and Research, SOA, Bhubaneswar, Odisha.

[5]Sr Mobile and OTT Engineer, Department of CBS News, Paramount, Bengaluru, Karnataka

[6*]Assistant Professor, Department of MCA, Gangadhar Meher University, Odisha, India.

*Email: dillip1seminar@gmail.com

Abstract

The most fascinating trend of our day is undoubtedly remote health monitoring. There are many potentially fatal illnesses in the contemporary world due to the ways in which people live. However, with the right measures done, you may avoid contracting any of these ailments. However, several deaths occur daily as a direct result of cardiac arrest. The delay between when symptoms first appear and when a patient is seen by a doctor is the main cause of this problem. If patients are being monitored by a remote monitoring system, any changes in heart rate might be sent to physicians and carers in real time through a smartphone app. This type of approach was necessary to prevent needless human deaths. The second rationale is that rural residents simply cannot afford high-priced medical treatment. If there is a way to check their health remotely, they can save time and energy. However, if they need medical treatment, they may go to the local PHC in their community. In order to store and analyse healthcare data and deliver it back to mobile applications used by the stakeholders in real time, there is a requirement for smart beds integrated IoT system that connects to cloud. The importance of the claim that "remote health monitoring serves common man to avail healthcare services with technology driven approaches" is best shown by this example. The challenge of improving the planned remote health monitoring system's security such that all communications are encrypted from end to end, without compromising patients' right to privacy. Therefore, the difficult topic discussed in this study is the actualization of a revolutionary healthcare system that addressed these concerns.

Keywords: Security, IoT, Health care system, Patient's, Records, Data, Communication and Monitoring System.

DOI: 10.48047/ecb/2023.12.si4.991

1. INTRODUCTION

The healthcare industry is one that affects individuals from all areas of life. Numerous methods, tools, and ICT integrations have previously been used in this field to enhance medical care delivery. Internet of Things (IoT) is a cutting-edge technological framework for connecting and syncing devices in the real and virtual worlds. Wearable devices, RFID, NFC, WSN, WSAN (Wireless Sensor and Actuator Network), cloud computing, mobile cloud computing, web services, Service Oriented Architecture (SOA), smart homes, Web 2.0, Web 3.0, and gateway technologies to seamlessly integrate cross-domain devices for optimal innovation utilisation[1]. Internet of Things (IoT) and its applications allow for the synergistic impact of such technologies to be realised. Unprecedented quality in healthcare services is possible when IoT is realistically integrated with healthcare facilities. The Internet of Things allows for the remote monitoring of health thanks to its integration of many technologies. This hypothesis paper serves as the primary foundation for the investigation presented here. In this part, we'll discuss how the Internet of Things may be used for remote health monitoring.

Now that we know what features a system for real-time health monitoring must have, we can focus on developing one that can handle distant health monitoring. To be successful, however, a wide range of technologies—including sensors, actuators, wearable gadgets, identity management systems like RFID, gateways, the Internet, and cloud computing—are required. The idea of a "smart bed" is applied to an IoT setting by considering a primary healthcare centre (PHC) in a rural area with minimal resources[2]. As a result, more rural residents will have easier access to medical care. Time, energy, and resources are all greatly reduced because to this approach. It also facilitates the improvement of healthcare facilities to the next quality level.

Many people throughout the globe have died recently from heart attacks and other illnesses. However, heart illness is widespread because it affects such a vital organ. The reality is that many people all over the world have perished simply because they were too slow to go to a hospital after experiencing the first signs of a heart attack or other potentially fatal illness. People's lives can be saved if these situations are recognised in real time[3]. Diseases like high blood pressure and diabetes are becoming more common in today's society. However, cardiac dysfunction over time is a major contributor to many disorders. Traditional healthcare requires patients to spend time, energy, and money travelling to a healthcare facility. Instead, with the help of IoT technology, a system that can remotely monitor the health of chosen patients may be realised. Thus, physicians may keep tabs on the health of a specific patient round-the-clock from afar[4]. This technology facilitates real-time monitoring and treatment of cardiac conditions and other diseases. It is feasible that human life might be improved

with the implementation of a remote health monitoring system. To put it another way, it improves people's standard of living.

2. LITERATURE SURVEY

People from all areas of life are being affected by the development of cutting-edge technology. The Internet of Things (IoT) is the result of a convergence of technologies (cross-disciplinary) that made it possible to connect the digital and physical realms. Numerous applications will have a tangible impact on society. However, one of the industries where IoT integration will have the greatest effect on people is the healthcare sector. Villagers that lack the resources to go to larger cities for medical treatment might benefit greatly from remote health monitoring systems[5]. Here, we had a look at the research done on the subject of implementing healthcare facilities with Internet of Things integration so as to provide remote health monitoring services. It sheds light on the potential of IoT in the healthcare industry, IoT and robotics, cyber physical systems, security and privacy challenges in healthcare systems, and the roles of mobile computing, RFID and NFC-type technologies, machine learning for performing analytics on health data, ECG signal analysis, the cloud's utility, and SOA-based IoT messaging[6]. The Internet of Things (IoT) has the potential to unite not just businesses and governments, but also individuals and healthcare providers, smart homes and transportation systems, and even military, remote sensing, smart grid, infrastructure, and other utilities on a national and even global scale. Since the Internet of Things generates copious data that needs to be processed, big data is inextricably linked to it, in Mohak Shah's view. The healthcare sector saw an immediate increase in the use of wearable sensors[7]. Doctors may use their ability to get vital signs from patients to help them make educated judgements. presented a cloud-based healthcare administration system that makes use of IoT devices. It uses data analytics on information gathered from wearable sensors to generate a clinical diagnosis or prediction about a patient's condition. Figure.1 depicts the system in action.

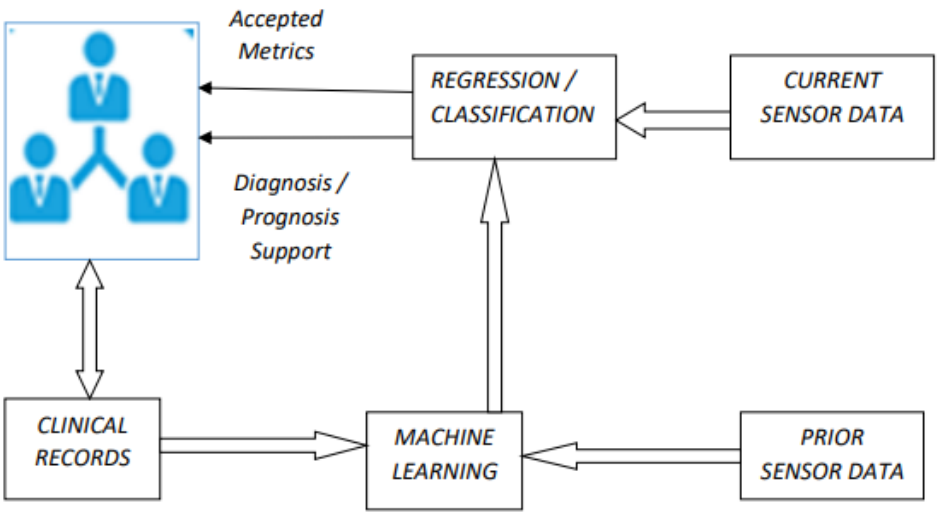

Figure.1: Wearable sensing and analytics in the healthcare system

The system incorporates both past and current information for enhanced analytics performance. Machine learning is at the heart of the cloud-based diagnostics system. Algorithms for machine learning are a component of AI and the growing subject of data science[8]. Various difficulties in the actual world are addressed with their help. Predicting cardiovascular disease is no different. Several methods are proven to be useful in the literature for cardiac disease prediction. However, these methods are informational in nature. Enhancing classification algorithms requires the extraction, selection, and optimisation of relevant features[9]. After receiving proper training, classification algorithms can reliably carry out prediction tasks. This is why these algorithms are classified as supervised machine learning techniques. Classes of machine learning include: supervised, unsupervised, semi-supervised, and reinforcement. Data mining operations like regression and classification are within the capabilities of supervised learning techniques[10]. Classification is used to do prediction or divide sample into classes, while regression is used to predict relationships between dependent and independent variables. Clustering and association mining are two examples of unsupervised learning activities. The former is implemented to generate clusters of comparable things. One such practise is customer segmentation. Conversely, data indicating potential consumer conduct may be analysed and understood by association rule mining. Classification and clustering are two examples of semi-supervised learning. Classifying texts and locating GPS coordinates are two such instances[11]. On the other hand, reinforcement learning involves a process of regulation and categorization. Reinforcement learning may be used to operate autonomous vehicles and categorise them into marketing categories. These ML techniques see extensive usage in medical software. In order to establish a link between the dependent and independent variables and arrive at a definitive diagnosis, clinicians use regression or classification to the patient's medical history, past data observed by wearable body sensors, and real-time data[12]. The electrocardiogram (ECG) is a crucial indicator of heart health. It has found extensive use in medical practise. Taking a sick or injured person to the hospital, however, requires significant investment of time, energy, and money[13]. The patient's electrocardiogram (ECG) may be taken in real time from a faraway location thanks to the Internet of Things. Figure.2 from Sundarasekar et al.'s exploration of this idea. The patient's ECG data is collected utilising an ECG collecting equipment and an IoT integrated application. When the information reaches an analytics system, the findings may be visualised and presented to a healthcare provider.

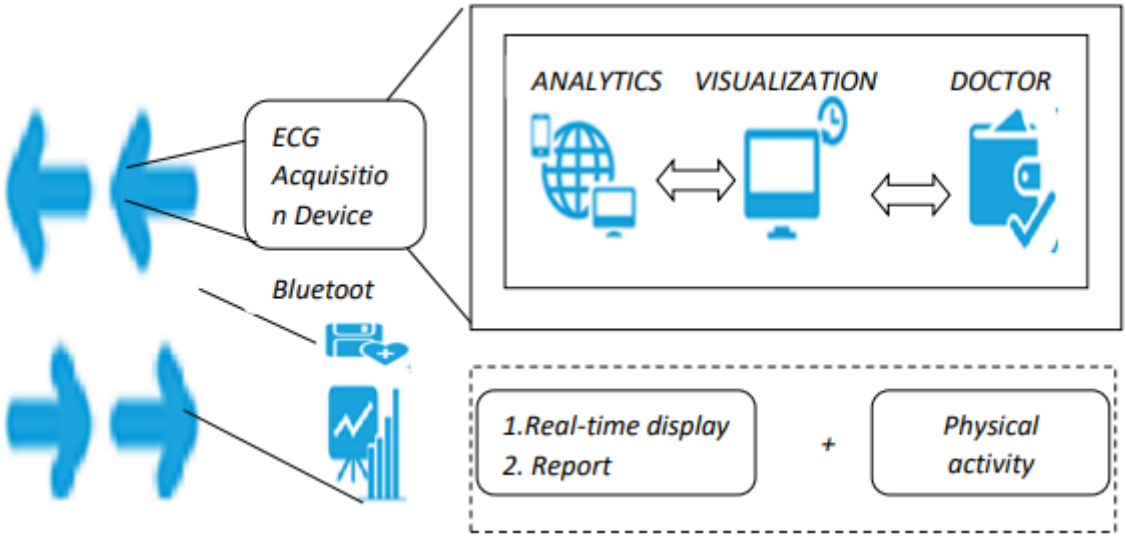

Figure.2: ECG-based remote health monitoring

The patient at a faraway location provides data in real time. Analytics and diagnostics are performed on the data. The Internet of Things is crucial to the realisation of this kind of system, which displays and reports data in real time. Patients' physical activity levels may be monitored in this way[14]. Optical sensors keep tabs on tissue characteristics and oximetry, while electrical sensors handle monitoring things like electrocardiograms, electromyograms, and electroencephalograms (EEGs). Personalised medical treatment will be crucial in the years to come[15]. They presented a framework for providing individualised medical treatment to patients. "sensor devices, M2K gateway, communication technologies, cloud storage, and access control mechanisms" are all part of the overall design. Real-time communication using Google Cloud Messaging push alerts. The Internet of Things, health monitoring, and smart home are all made possible by Raspberry Pi. Saha et al. investigate this hypothesis. Figure 3 depicts the same thing. Multiple wearable sensors are used in this cloud-based system[16]. Heart rate, blood pressure, respiration, temperature, acceleration, and infrared (IR) sensors are all included. With the help of Raspberry Pi technology, the collected data from these sensors can be uploaded to the cloud, where it can be processed and the results forwarded to the appropriate authorities by text message (SMS), electronic mail (email), or a web-based application.

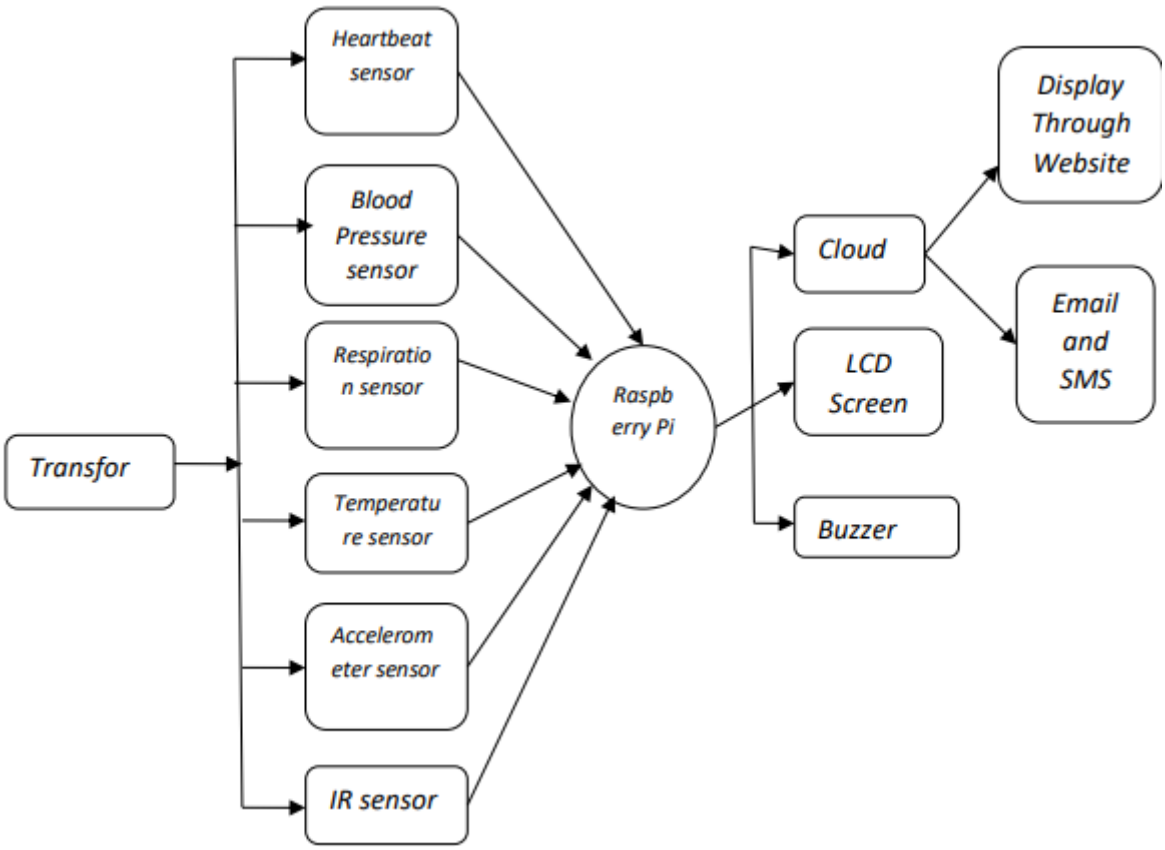

Figure.3 : Raspberry Pi-based Internet of Things health monitor

Integrating smart home with remote health monitoring apps is doable with a simple design. Telehealth at home refers to "the utilisation of telecommunication technologies by patients and healthcare service providers to have an equitable exchange of information pertaining to healthcare." To facilitate real-time healthcare services with coordinated efforts among patients, carers, and doctors, they created a system called CogSense[17,18]. Patients' health is monitored via the use of sensors, and data is sent and analysed so that better decisions may be made. Services with custom data storage and retrieval are now feasible thanks to cloud computing.

3. PROPOSED MODEL

The framework for distant health monitoring is described here. The patient's vitals may be recorded using an IoT-based solution as they lie on a smart bed at a rural health clinic. It uses measurements of body heat and heart rate to diagnose systemic and cardiovascular illness. Since IoT can be applied to any preexisting system, it opens the door to the possibility of merging the virtual and the real[19]. The human body is purely physical. RFID (for one-of-a-kind identification and authentication) and sensors connected to the human body are included into the digital system. As seen in Figure 4, several sensors might theoretically be implanted into the human body.

Figure.4: Sensor-equipped wearables of various types

Wireless Body Area Network (WBAN) is a network made up of human-related sensors. In turn, this network connects to others in the medical field. A network may also be built between two such WBANs belonging to different people. In this work, we examine the feasibility of doing empirical research on a single WBAN connected with the human body and linked to a smart bed in PHC. IEEE 802.15.4, Bluetooth, and Radio Frequency Identification (RFID) are only few of the technologies used in the communications. These tools see extensive application in IoT-based medical networks[20]. The suggested system collects data, which is then saved in the cloud. Patients who want to use the IoT integrated healthcare system for remote health monitoring must visit the village PHC (though it may be set up at home as well). Once the patient is positioned on the smart bed, the necessary sensors are attached, and the Internet of Things devices are connected through gateways[21]. The doctor receives real-time updates on the patient's health status. This means that the doctor may see the patient's temperature and heart rate without any wait. The term "real-time health monitoring" describes this development. Many lives are saved because the need to wait for treatment is eliminated.

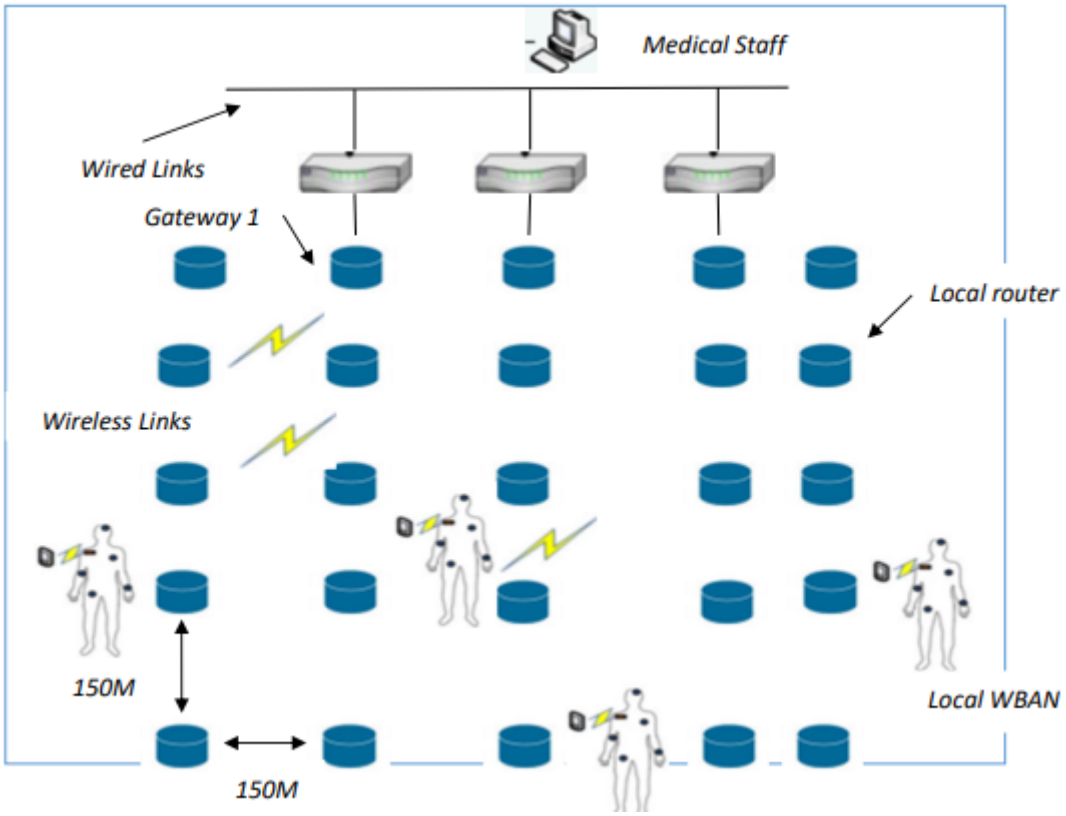

Figure.5: Global framework for health monitoring through the Internet of Things

Figure.5 depicts the realised architecture of a remote health monitoring system. Many people in this area are participating in WBAN by donning sensors on their bodies. This means that many WBANs contribute to the system for telehealth monitoring. Usefulness is made possible in large part by wireless connections, smart gadgets, and local routers. In the end, a gateway connects the system to the cloud and the Internet.

4. SECURITY FOR IOT INTEGRATED HEALTHCARE UNITS

End-to-end security is crucial for IoT integrated healthcare systems. "mobility enabled healthcare IoT for providing a scheme to enable end-to-end security" [STE+16] was the topic of study for Sanaz Moosavia et al. The approach is multi-faceted, including things like user identification and authorisation processes, a healthcare network that takes into account patients' need for mobility, and encrypted data transmissions from sensors. End-to-end encrypted healthcare IoT is shown in Figure.6.

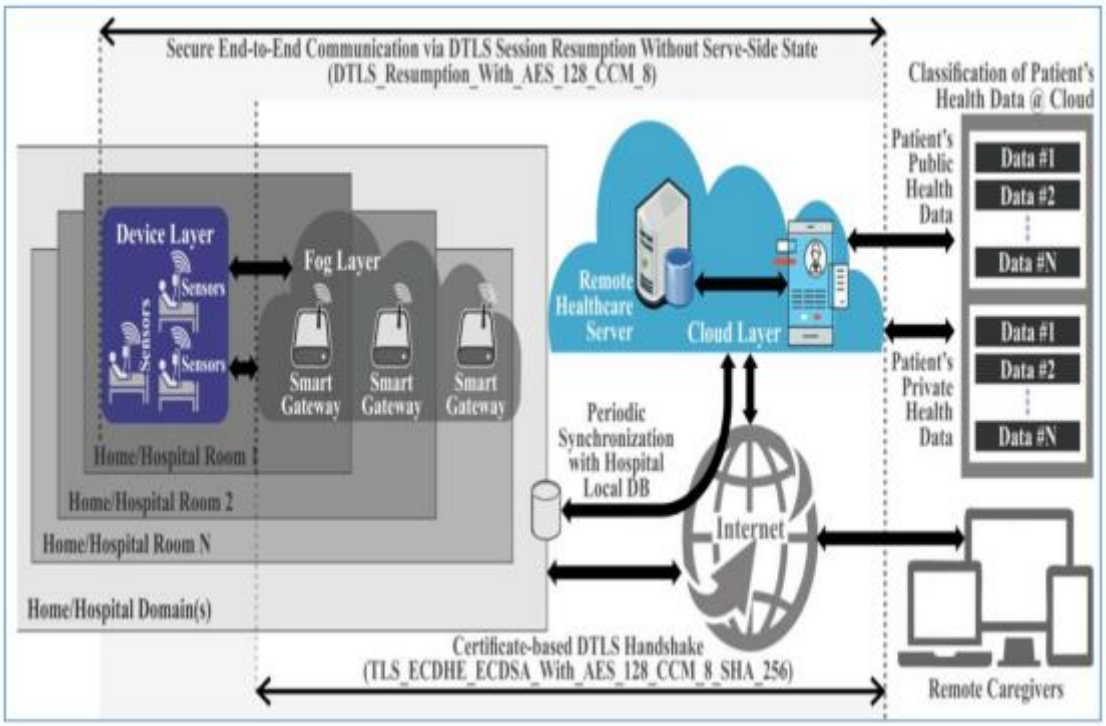

Figure.6: End-to-end encrypted healthcare internet of things: an overview

The structure consists of many levels. There are a few different layers, and these are devices, fog, and clouds. The healthcare service providers are interconnected with these levels. The device layer displays the available sensor devices. at the fog layer, smart gateways are employed, and at the cloud layer, cloud services are made available[22]. End-to-end security is achieved with the use of Elliptic Curve DiffieHellman (ECDH) public key encryption, digital certificates, and Elliptic Curve Digital Signature Authentication (ECDSA). In the instance of smart cities using IoT-integrated healthcare, Daniela Popescul et al. [DaLa16] investigated vulnerabilities such as hacking, loss of boundaries, messy complexity, and hyperconnectivity. Inadequate setting of smart devices, left-alone gadgets, lack of security for sensitive data, spam, and social engineering were all highlighted. In light of the Internet of Things (IoT), the cloud, and the impending integration of these technologies into healthcare, Guido Noto La Diega reviewed data privacy and consumer regulations [Gui16]. Clouds of Things (CoT) are the result of the combination of M2M communications with the Internet of Things (IoT). For the purpose of "sharing healthcare data through social media related to healthcare domain or Health Social Networks" (HSNs), Xiaohui Liang et al. [XMR+12] established a system called "Health Share." Their design incorporates a trusted authority for attributes, which allows for proper authorization of healthcare personnel.

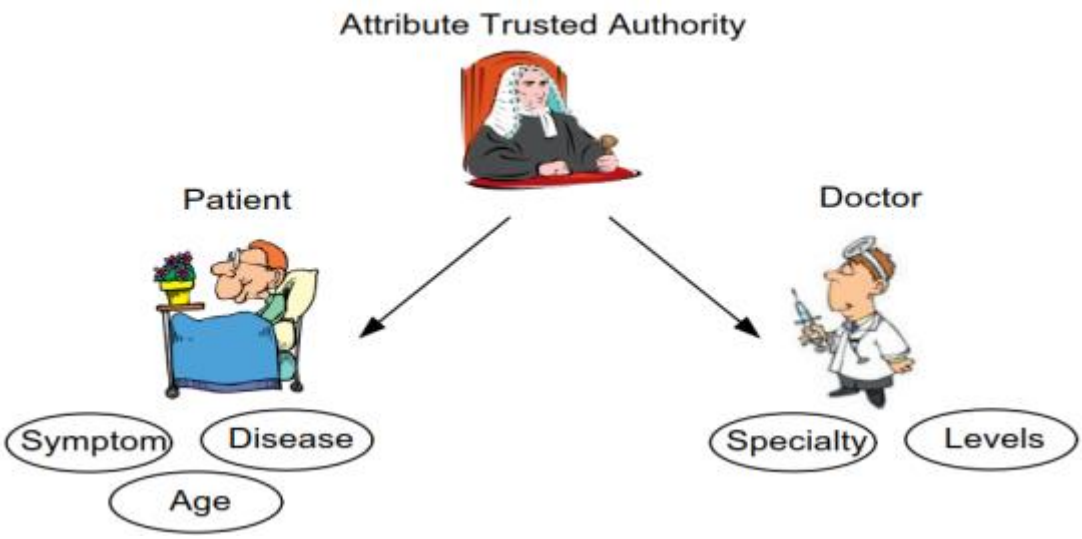

Figure.7: The Safe Exchange of Health Information

Figure.7 makes it clear that there is a trusted authority responsible for attributing privileges to various parties, including physicians and patients. Stakeholders are only given permission to see their required characteristics. To facilitate secure data exchange, appropriate policies are established. Their system uses attribute-oriented authentication and permission. Their approach employs the security principles of signature and verification. Charlotte Garrett et al. [CLR+12] looked at data access issues in the healthcare sector. An infrastructure for easy sharing of primary care records was envisioned. According to Roman et al., the dispersed nature of the Internet of Things and associated technologies poses privacy and security risks. security architecture for the Internet of Things. The framework accommodates NSOs (Networked Smart Objects) by including a policy engine and security rules. Security is given, as stated in the framework, and the NSOs are incorporated into IoT. The administrator handles all security-related NOS settings. Data API, data normalisation, Message Queue Telemetry Transport (MQTT), a security analyser, and HTTPS/SSL are all supported by the framework's design. Privacy and security threats in healthcare IoT systems were studied by Sicari et al. [SRG+14]. They determined that conventional healthcare facility security strategies are insufficient for IoT linked healthcare facilities. As a means of improving the scalability, privacy, and security of such systems, they developed a versatile design. The Internet of Things has made it possible to link devices everywhere, at any time. It provides the door for people (physical items) to be integrated with digital systems using technologies like RFID and NFC in conjunction with wearable gadgets and sensors. In the medical literature, there are several IoT integrated healthcare designs. All of them have the common denominator of being primarily theoretical and intellectual in scope. The principles expressed in such buildings, however, are quite useful. The goal of using remote health monitoring is to assist low-income rural communities in need. To achieve this goal, many designs have been

suggested. Unfortunately, they have the following issues. First, they haven't developed a framework based on smart beds and village primary healthcare, where patients use wearable gadgets to remotely gather and monitor their vital signs in real time. Second, a practical aspect that explores the components towards realisation of such application is required in place of a theatrical viewpoint. Third, due to the sensitive nature of healthcare data, end-to-end security and privacy must be maintained at all times.

5. RESULTS AND DISCUSSION

The healthcare system provided by the Internet of Things can track vitals like body temperature and heart rate, and it also allows for encrypted communication between all of the system's participants. A body sensor, data transmitter, data receiver, server, and healthcare provider or caretaker all play a role. Here we provide the empirical study's findings in terms of security analysis, encryption performance, decryption performance, upload/download times, and temperature/heart rate monitoring. The horizontal axis depicts the time interval between temperature readings taken from the patient. Temperature in a different heat unit is shown along the vertical axis. The findings indicate that core body temperature fluctuates throughout time. By keeping an eye on the patient's core temperature, doctors can determine whether they are experiencing any of the many illnesses that manifest themselves in the form of elevated core temperature. Given that temperature is regarded an important indication in the medical field. It's useful for doctors to get an idea of how well their therapy is working. Disease-specific triggers like fever are common. It gives the doctor crucial information for making educated choices. Since the human body already has its own defensive system set up, the regular temperature is adjusted to accommodate it. The temperature of a person's body may be taken in a variety of settings. Forehead, underarm, mouth, ear, and rectum are all examples. A typical body temperature ranges from between 97.3 to 99.5 degrees Fahrenheit. A fever or a fever induced by another ailment is diagnosed if the temperature rises over this threshold. All of these notes pertain to Patient 1.

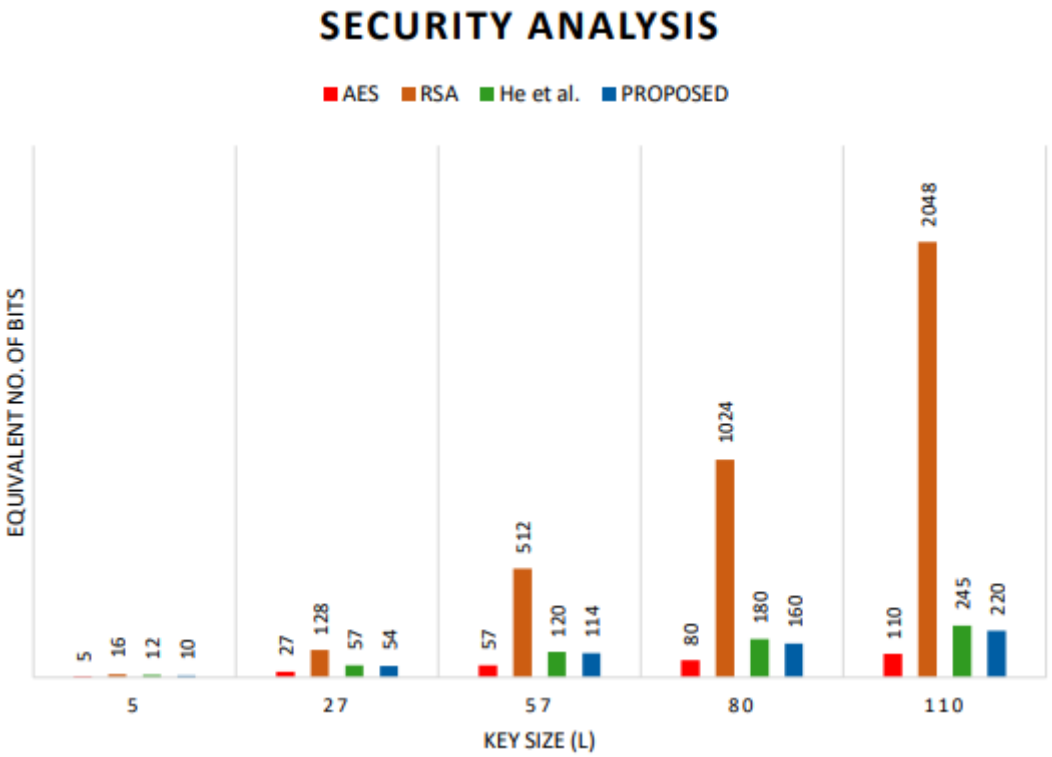

Figure.8: Evaluation and study of the proposed system's security

Figure.8 shows how the key size, represented by L, varies among the various cryptographic methods. The horizontal axis is used to determine its worth. The security level is represented vertically by the number of bits that are comparable to it. When compared to RSA, the suggested system requires less equivalent bytes for its implementation. In comparison to RSA's 16 equivalent bits for a key size of 5, the suggested approach only requires 10. The suggested approach requires just 220 bits in comparison to the RSA's 2048 bits for a key of size 110. The suggested system is also superior to that of He et al., which demonstrates the proposed security strategy's low weight and high performance.

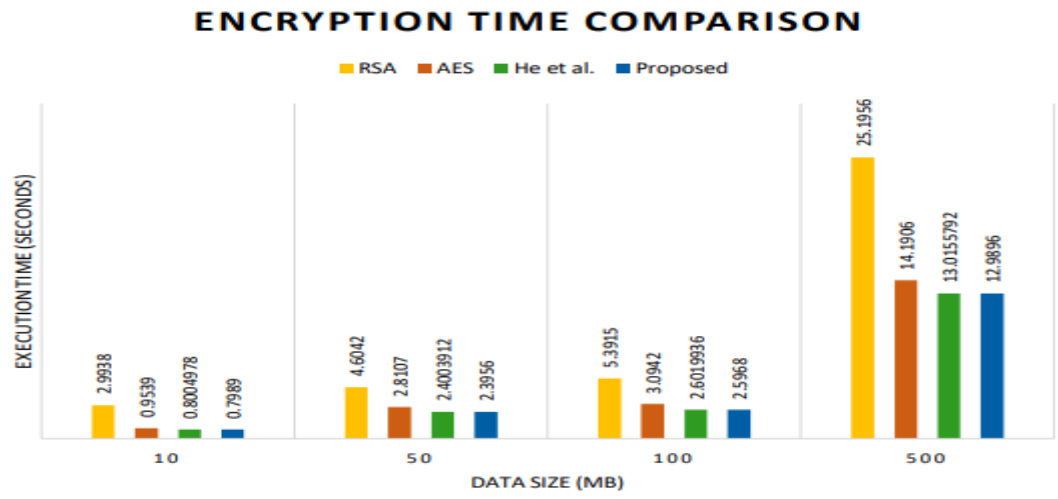

Figure.9: A Study of Encryption's Efficiency

Figure.9 shows the results of a detailed analysis of how well encryption performs in terms of how long it takes to run. The horizontal axis lists the security primitives that were employed in the empirical investigation, and the vertical axis lists how long it takes to execute each of those primitives. In seconds, the code will be run. Data sizes of 10 MB, 50 MB, 100 MB, and 500 MB are used in the experiments. Security techniques required linearly more time for encryption as workload size rose. The execution time for RSA was the longest across all data sizes. The suggested method outperforms the current gold standard. When compared to He et al.'s system, AES, and RSA, the suggested system required the least amount of time to run. This is justified by the fact that the suggested security method is quite lightweight.

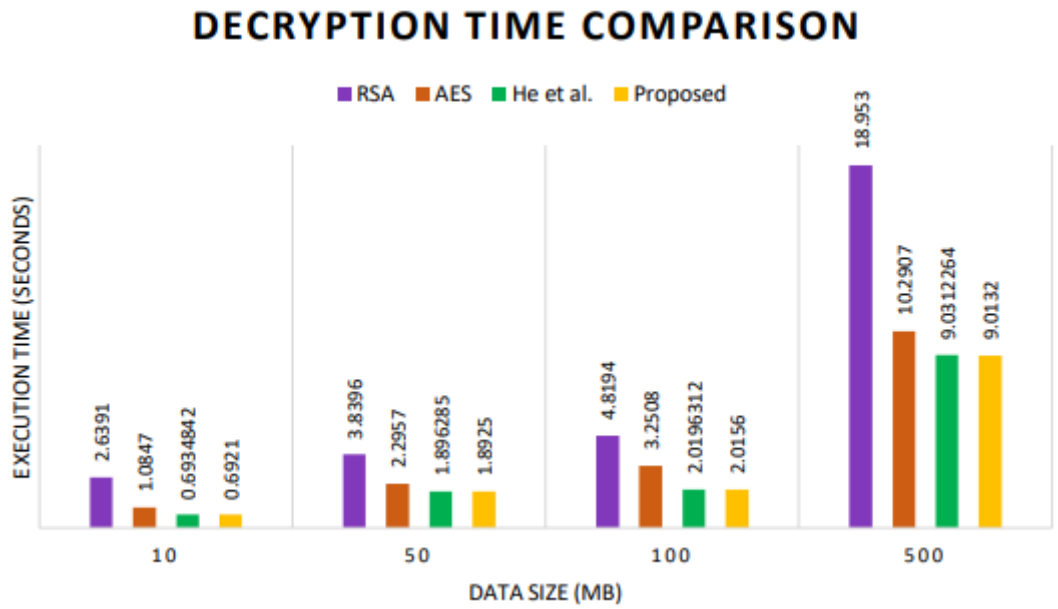

Figure.10: Decryption performance analysis

Figure.10 shows the results of a time analysis of the decryption process. The horizontal axis lists the security primitives that were employed in the empirical investigation, and the vertical axis lists how long it takes to execute each of those primitives. In seconds, the code will be run. Data sizes of 10 MB, 50 MB, 100 MB, and 500 MB are used in the experiments. Security measures saw a linear rise in decryption time as workload size rose. The execution time for RSA was the longest across all data sizes. The suggested method outperforms the current gold standard. When compared to He et al., AES, and RSA, the suggested system had the quickest runtime. This is justified by the fact that the suggested security method is quite lightweight.

6. Conclusion

This study presents the suggested method for distant health monitoring. Simply said, it's the technology behind our current state of the art in continuous health monitoring. It connects healthcare facilities with IoT scenarios linked with PHC in rural areas, allowing for continuous monitoring of patients' conditions. The system is implemented using a wide variety of technologies, including but not limited to standard digital infrastructure, wearable body sensors, RFID, Bluetooth, and other Internet of Things (IoT) infrastructure. The suggested technology provides real-time healthcare by keeping tabs on vitals including body temperature and heart rate. It's linked to doctors, so they can see their patients' records and respond in real time. The Internet of Things (IoT)-related smart bed based PHC system is made possible by a wide range of technologies and underlying protocols. However, there are safety concerns owing to the diversity of available technology. The suggested security solution is minimal in scope and allows for complete confidentiality of all transmitted data. And although RSA requires 16 bits for a key size of 5, the suggested security techniques only need 10. The suggested approach requires just 220 bits in comparison to the RSA's 2048 bits for a key of size 110.

REFERENCES

1. S. Misra, A. Roy, C. Roy, and A. Mukherjee, “DROPS: Dynamic radio protocol selection for energy-constrained wearable IoT healthcare,” IEEE J. Sel. Areas Commun., early access, Aug. 31, 2020, doi: 10.1109/JSAC.2020.3020679.
2. B. D. Deebak and F. Al-Turjman, “Smart mutual authentication protocol for cloud based medical healthcare systems using Internet of medical things,” IEEE J. Sel. Areas Commun., early access, Sep. 7, 2020, doi: 10.1109/JSAC.2020.3020599.
3. S. S. Gopalan, A. Raza and W. Almobaideen, "IoT Security in Healthcare using AI: A Survey," *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, Sharjah, United Arab Emirates, 2021, pp. 1-6, doi: 10.1109/ICCSPA49915.2021.9385711.
4. T T Chhowa, M A Rahman, A K Paul and R Ahmmed, "A Narrative Analysis on Deep Learning in IoT based Medical Big Data Analysis with Future Perspectives", *2nd Int. Conf. Electr. Comput. Commun. Eng. ECCE 2019*, pp. 1-6, 2019.
5. C Ieracitano, A Adeel, M Gogate, K Dashtipour, F C Morabito, H Larijani, et al., "Statistical Analysis Driven Optimized Deep Learning System for Intrusion Detection", *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10989 LNAI, pp. 759-69, 2018.
6. A K Alharam and W El-Madany, "Complexity of cyber security architecture for IoT healthcare industry: A comparative study", *Proc. - 2017 5th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2017*, vol. 2017-Janua, pp. 246-50, 2017.
7. P Ghosal, D Das and I Das, "Extensive survey on cloud-based IoT-healthcare and security using machine learning", *Proc. - 2018 4th IEEE Int. Conf. Res. Comput. Intell. Commun. Networks ICRCICN 2018*, pp. 1-5, 2018.

8. D He and S Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography", *IEEE Internet Things J*, vol. 2, pp. 72-83, 2015.
9. A M Elmisery, S Rho and D Botvich, "A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things", *IEEE Access*, vol. 4, pp. 8418-41, 2016.
10. S. M. Karunarathne, N. Saxena and M. K. Khan, "Security and Privacy in IoT Smart Healthcare," in *IEEE Internet Computing*, vol. 25, no. 4, pp. 37-48, 1 July-Aug. 2021, doi: 10.1109/MIC.2021.3051675.
11. M. Wazid, A. K. Das, N. Kumar, M. Conti and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment", *IEEE J. Biomed. Heal. Inf.*, vol. 22, no. 4, pp. 1299-1300, Jul. 2018.
12. Y. Yang, X. Liu, R. H. Deng and Y. Li, "Lightweight sharable and traceable secure mobile health system", *IEEE Trans. Dependable Secur. Comput.*, vol. 17, no. 1, pp. 78-91, Jan./Feb. 2020.
13. S. R. Moosavi, E. Nigussie, M. Levorato, S. Virtanen and J. Isoaho, "Performance analysis of end-to-end security schemes in healthcare IoT", *Proc. Comput. Sci.*, vol. 130, pp. 432-439, 2018.
14. F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges", *IEEE Commun. Surv. Tuts*, vol. 22, no. 3, pp. 1686-1721, Jul.–Sep. 2020.
15. Y Leandro et al., "Exploiting IOT technologies for enhancing Health Smart Homes through patient identification and emotion recognition", *Computer Communications.*, vol. 89, pp. 178-190, 2016.
16. World Health Organization. (2018). Towards a Global Action Plan for Healthy Lives and Well-Being for All: Uniting to Accelerate Progress Towards the Health-Related SDGs World Health Organization. [Online]. Available: https://apps.who.int/iris/handle/10665/311667
17. WHO/ITU National eHealth Strategy Toolkit, World Health Org., Geneva, Switzerland, 2012.
18. G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of medical things (IOMT): Applications, benefits and future challenges in healthcare domain," J. Commun., vol. 12, no. 4, pp. 240–247, Apr. 2017.
19. A. A. Toor, M. Usman, F. Younas, A. C. M. Fong, S. A. Khan, and S. Fong, "Mining massive E-health data streams for IoMT enabled healthcare systems," Sensors, vol. 20, no. 7, p. 2131, 2020.
20. H. Mshali, T. Lemlouma, M. Moloney, and D. Magoni, "A survey on health monitoring systems for health smart homes," Int. J. Ind. Ergonom., vol. 66, pp. 26–56, 2018, doi: 10.1016/j.ergon.2018.02.002.
21. G. Cai, Y. Fang, P. Chen, G. Han, G. Cai, and Y. Song, "Design of an MISO-SWIPT-aided code-index modulated multi-carrier M-DCSK system for e-Health IoT," 2020, arXiv:2003.07107. [Online]. Available: https://arxiv.org/abs/2003.07107
22. X. Zhang, L. Yang, Z. Ding, J. Song, Y. Zhai, and D. Zhang, "Sparse vector coding-based multi-carrier NOMA for in-home health networks," IEEE J. Sel. Areas Commun., early access, Aug. 31, 2020, doi: 10.1109/JSAC.2020.3020679.