Data and Metadata. 2024; 3:368
doi: 10.56294/dm2024368

ORIGINAL

A secured and energy-efficient system for patient e-healthcare monitoring using the Internet of Medical Things (IoMT)

Un sistema seguro y energéticamente eficiente para el seguimiento de la atención sanitaria electrónica de los pacientes mediante Internet of Medical Things (IoMT)

Veera V Rama Rao M[1], Kiran Sree Pokkuluri[2], N. Raghava Rao[3], Sureshkumar S[4], Balakrishnan S[5], Shankar A[6]

[1]Shri Vishnu Engineering College For Women. Bhimavaram, India.
[2]Department of Computer Science and, Engineering, Shri Vishnu Engineering College for Women. Bhimavaram, India.
[3]Information Technology, Department of Information Technology Institute of Aeronautical Engineering. India.
[4]Department of CSE, P. A. College of Engineering and Technology, Pollachi-642002, India.
[5]Department of Computer Science and Engineering, Aarupadai Veedu Institute of Technology, Vinayaka Missions Chennai Campus. Paiyanoor, India.
[6]Department of ECE, Manakula Vinayagar Institute of Technology. Puducherry, India.

Cite as: Rama Rao M VV, Sree Pokkuluri K, Raghava Rao N, S S, S B, A S. A secured and energy-efficient system for patient e-healthcare monitoring using the Internet of Medical Things (IoMT). Data and Metadata. 2024; 3:368. https://doi.org/10.56294/dm2024368

Submitted: 23-01-2024 **Revised:** 05-04-2024 **Accepted:** 16-06-2024 **Published:** 17-06-2024

Editor: Adrián Alejandro Vitón-Castillo

ABSTRACT

Introduction: the Internet of Things (IoT) is gaining popularity in several industries owing to the autonomous and low-cost functioning of its sensors. In medical and healthcare usage, IoT gadgets provide an environment to detect patients' medical problems, such as blood volume, oxygen concentration, pulse, temperatures, etc. and take emergency action as necessary. The problem of imbalanced energy usage across biosensor nodes slows down the transmission of patient data to distant centres and has a detrimental effect on the health industry. In addition, the patient's sensitive information is sent through the insecure Internet and is exposed to potential threats. For clinical uses, information privacy and stability against hostile traffic constitute a further research challenge.
Methods: this article proposes a Secured and Energy-Efficient System (SEES-IoMT) e-healthcare utilizing the Internet of Medical Things (IoMT) monitoring, the main goal of which is to reduce the connectivity cost and energy usage between sensing devices while feasibly forwarding the medical data. SEES-IoMT also guarantees the clinical data of the patients against unverified and malevolent nodes to enhance the privacy and security of the system.
Result and Discussion: in consideration of the memory and power limitations of healthcare IoT gadgets, this approach is designed to be very lightweight. A thorough examination of this system's safety is performed to demonstrate its reliability.
Conclusion: in terms of computing speed and security, the research compares SEES-IoMT to relevant methods in the IoT medical environment to demonstrate its applicability and resilience.

Keywords: Internet of Medical Things; Energy Efficiency; Security; Healthcare Monitoring.

RESUMEN

Introducción: internet de las Cosas (IoT) está ganando popularidad en varias industrias debido al funcionamiento autónomo y de bajo costo de sus sensores. En el uso médico y sanitario, los dispositivos IoT proporcionan un entorno para detectar los problemas médicos de los pacientes, como el volumen sanguíneo, la concentración de oxígeno, el pulso, la temperatura, etc., y tomar medidas de emergencia según sea necesario. El problema del uso desequilibrado de energía entre los nodos biosensores ralentiza la transmisión de datos de pacientes a centros distantes y tiene un efecto perjudicial en la industria de la salud. Además, la información sensible del paciente se envía a través de Internet insegura y queda expuesta a posibles amenazas. Para usos clínicos, la privacidad de la información y la estabilidad frente al tráfico hostil constituyen un desafío de investigación adicional.

Métodos: este artículo propone un sistema de atención médica electrónica seguro y energéticamente eficiente (SEES-IoMT) que utiliza el monitoreo de Internet de las cosas médicas (IoMT), cuyo objetivo principal es reducir el costo de conectividad y el uso de energía entre dispositivos sensores, al mismo tiempo que es factible. remitir los datos médicos. SEES-IoMT también garantiza los datos clínicos de los pacientes contra nodos malévolos y no verificados para mejorar la privacidad y seguridad del sistema.

Resultado y discusión: considerando las limitaciones de memoria y energía de los dispositivos de IoT para el cuidado de la salud, este enfoque está diseñado para ser muy liviano. Se realiza un examen exhaustivo de la seguridad de este sistema para demostrar su confiabilidad.

Conclusión: en términos de velocidad informática y seguridad, la investigación compara SEES-IoMT con métodos relevantes en el entorno médico de IoT para demostrar su aplicabilidad y resiliencia.

Palabras clave: Internet de las Cosas Médicas; Eficiencia Energética; Seguridad; Monitoreo de la Atención Médica.

INTRODUCTION

The internet of things (IoT) has gotten much attention lately because of the low cost and high efficiency with which automated sensors can perform their functions. For example, in healthcare and medicine, IoT devices provide an ecosystem to monitor vital signs, oxygen levels, heart rates, and temperatures and respond effectively in scenarios an emergency.(1) The IoT-dependent medical sensor's cloud stores patient data for analysis and processing. Internet, internet, and sensor networks are the most advanced approaches for patient care. IoT-based systems transfer information to a server to monitor healthcare (2) accurately. The secure e-healthcare records in virtualization settings with decreasing security and privacy health, including data loss, alteration, and leaks. Virtualization technology has enabled internet data center computing and e-healthcare data networking resources to be manageable.(3) IoT development has brought about a positive enhancement in healthcare, and current healthcare systems, often known as e-healthcare, have made life easier for patients and healthcare practitioners. However, the patient's data is sensitive and private, and illegal access can lead to tragedy.(4) The IoMT employs medical devices as nodes in the IoT to monitor and record patients cost-effectively. The IoMT can monitor patients in hospitals and at home, relieve consulting doctors and nurses in monitoring health status at regular intervals, and provide emergency care warnings.(5) An IoMT's infrastructure includes online networks and numerous communications systems. With that kind of environment, innovation can enable healthcare device communication abroad. Sensor responses and medical information from IoMT devices can be recorded and processed on online systems.(6) A secured and Energy-Efficient System (SEES) is an essential feature of IoT healthcare. The sensor node's low energy can cause service interruptions and lower illness diagnostic accuracy. Due to data transfer between IoT devices and the cloud server, energy depletion is significant.(7) IoMT can be observed as an improvement and development in enabling to react more effectively and efficiently to the demands of patients. However, IoMT has several concerns and obstacles, including a lack of security and privacy safeguards and essential training and information.(8) Sensing and various processes are automated with the help of device understanding. A patient's time spent in the hospital and the number of tests needed can be shortened, provided either invasive or non-invasive facilities gather sufficient information regarding patients. In that respect, IoMT can improve the patient's financial burdens and doctors' efficiency.(9) Sensing nodes are important for healthcare usage, as devices can recognize and provide doctors' servers with health-related parameters, cutting medical expenses. And since this contains private information like patients' health, the information communicated across healthcare systems can be secured.(10) Smart healthcare systems struggle with battery life and energy efficiency. The report provided a smart healthcare system based on IoMT and identified the integration. The energy-efficient strategy uses battery recovery to extend battery life and reduce energy consumption.(11) Sensors monitor exercise, blood glucose, and other smart home diagnostics. However, improper classification of such sensors has caused delays in government clearance, gaps inpatient-doctor relationships, and societal reluctance against employing them in regular life.(12) E-healthcare systems can meet the requirements and desires of patients, professionals, and medical and research organizations at a high rate. Patients can get medications, consultations, and e-prescriptions online, saving time and energy.(13) Due to the IoMT healthcare system's low processing capacity and power constraints, security and privacy at the sensor level confront the greatest difficulties. The main processes are now being moved to the mobile server level in sensor-level security research. As a result, sensor-level security solutions must be both lightweight and low in communication overhead.[14] Smart devices that use the telecare medical information system can compute more due to innovation. To claim trustworthiness, efficiency, and creativity that improves medical identification. To reduce professional duties, telecare services automate remote healthcare monitoring. It's designed to save time and money and simplify healthcare.[15] The network's optimal route for processing can be determined by identifying sensors via routing, which can improve energy efficiency. An improvement in the network's energy efficiency is possible with a careful selection of sensors through routing to locate the most effective route for communication.[16]

The main contribution of the paper:

- The IoMT devices are layered with patient archives that can save confidential information, including patients' identities, addresses, and health records. However, securing confidentiality and integrity in dealing with a large volume of data can be impossible.
- To research the different health domains covered by the IoMT framework and its applications in the state-of-the-art healthcare system, including the wide variety of sensors employed in each health area.
- Increase the reliability of medical records by analyzing and contrasting different data collection techniques that have been obtained.

The remainder of the essay is in section 2, which deals with the application of the current methodology; section 3 suggests that the SEES-IoMT approach be examined; section 4 is an experimental analysis; and section 5 is with an examination of the paper's conclusions.

Literature review

Asad Abbas et al. (2021) detailed the IoMT-based Blockchain-assisted Secure Data Management Framework (BSDMF) to facilitate the safe transfer of patient information and enhance the scalability and accessibility of healthcare data.[17] The term "Internet of Medical Things" refers to the interconnected network of smart medical devices, applications, health services, and systems (IoMT). Data privacy and security, scalability, and accessibility all pertain to this category of problems. Blockchain is used in the IoMT's security architecture for secure data storage and movement between connected nodes.

Mengting Liu et al. (2019) illustrated the analysis develops a unique increasing the performance of blockchain-enabled systems using Deep Reinforcement Learning (DRL) to meet the high throughput demand.[18] The primary goals are to provide a mechanism for assessing the platforms on which the block producers, consensus algorithm, block size, and block interval are all up for grabs through the DRL method. In addition, the framework's potential to improve the efficiency of blockchain-based IIoT systems and to easily adapt to change has been shown via simulation.

In [19] discussed the significant need to create a Convolutional Neural Network (CNN)-a based ubiquitous real-time healthcare system that can determine whether and if a given set of frames indicates a person falling. The difficulty in deploying widespread, high-quality, and low-cost smart health services developed a new framework for meeting the world's growing need for high-quality medical care. In addition, due to the demographic shift toward an aging patient population, falls in healthcare facilities and private residences have become a major issue for medical providers. The suggested technique is tested on publicly available hospital datasets, which consistently outperforms state-of-the-art solutions.

Majid Alotaibi et al. (2022) illustrated the extracted variables are subsequently categorized using a Deep Convolutional Neural Network (DCNN).[20] Initially, nodes were clustered to save energy, and the cluster's centroid was ideally picked using a novel hybrid method. Furthermore, this cluster formation was guided by restrictions such as distance and energy. Finally, a security system was enabled through the severity level estimate that evaluated the seriousness of the condition and advised individuals to attend the hospital. Finally, the superiority of the strategy is assessed by comparing it to various available strategies.

Ripty Singla et al. (2021) discussed the interest in Wireless Body Area Networks (WBAN) because numerous biosensors may be integrated with or worn on the human body to assess health indicators.[21] Human life expectancy is rising, and the expense of medical services is rising, posing significant issues for the government and healthcare business. A comparison of many current state-of-the-art safe routing protocols, and a critical analysis based on security approaches and other performance characteristics, have been provided. In addition, due to an unhealthy lifestyle, there is a greater requirement for ongoing health monitoring and illness diagnosis.

Khalid Haseeb et al. (2021) detailed that centralized-based Software Define Network (SDN) architecture mitigates network risks among distributed sensors at a low administration cost.[22] Utilizing health applications has since seen a significant uptick in popularity in smart cities because of the IoMT. That suggests that patients and medical staff can benefit from numerous real-time innovations that enable remote data access and appropriate reaction. The research develops an SDN-enabled machine learning approach for secure network resource use prediction and sensor data improvement transmission.

The above discussion shows privacy concerns are among the most pressing issues facing an Internet of Things-enabled healthcare system. There is a lack of data protocol and security standards despite IoT devices gathering and transmitting data in a real-time setting. In the case of electronic gadgets, information governance regulations are uncertain, such as [17,18] and [19] compared with the proposed SEES-IoMT method.

METHOD

Proposed method SEES-IoMT

To accurately assess health, sensors must measure various physiological indicators. The existing medical equipment is both energy- and money-consuming. Hence, sensors are used in IoMT-based medical systems to save power and implement cheap and fast solutions. Peers track several patient metrics in real-time and measure various physical factors. A sensor's main function is facilitating IoMT-based healthcare solutions that help reduce hospitalizations. Medical professionals and patients alike will appreciate the time savings afforded by the widespread use of biomedical sensors that depend on machine-to-machine interactions to streamline care and improve patients. The patient's ability to control medical health records is a significant research focus in several of these studies. If patients are given this access, people can limit the information being provided to the doctors.

IoT and IoMT

The IoMT, a subsection of IoT technologies, comprises networked devices and software for the healthcare and medical industries. The IoMT exclusively pertains to the medical and healthcare sector, while IoT is a wide area that deals with the collection of sensing and actuating devices. The IoMT pertains to a collection of connected medical devices. The IoMT's essential device communication is made possible by Wi-Fi-enabled medical devices. Interconnected medical nodes, software, health systems, and infrastructure make up the IoMT. A wave of sensor-based solutions for remote patient surveillance ultimately characterizes the IoMT ecosystem. Due to the rapid advancements in technology and medicine and the subsequent explosion of smart medical devices, the healthcare ecology has evolved significantly.

Additionally, the advancement of communication technology has increased accessibility for various medical services, including computer-assisted and remote monitoring systems. IoT installations have significantly influenced societal life and healthcare organizations in medical systems. Corporations and scientists use IoT applications to provide better and more efficient healthcare. The conventional medical system comprises patients, doctors, pharmaceuticals, and therapies. Cloud data is included in the IoMT medical ecosystem and cloud data applications. The standard health ecosystem can be changed into an IoMT environment using a variety of innovative and effective concepts that have been forward by researchers. The improvements impact several facets of the system, including application, construction, technology, communication, and safety.

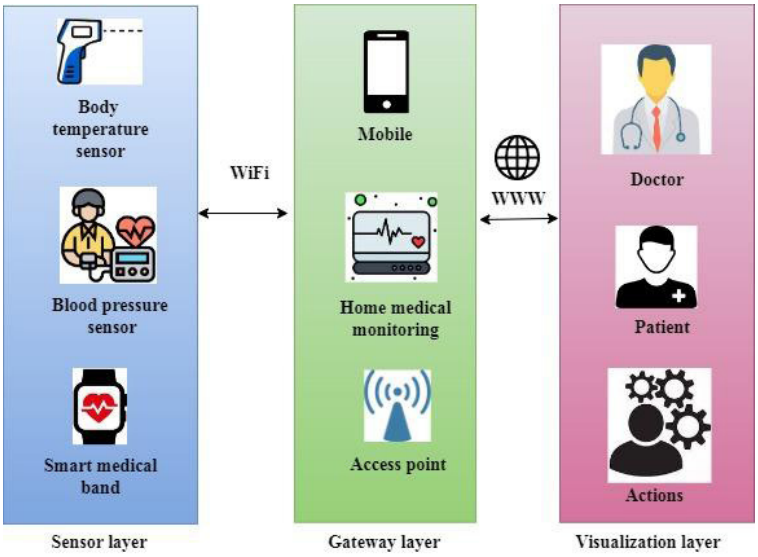

Figure 1. IoMT architecture

Figure 1 shows that the information can then be delivered via a gateway to the subsequent component, which will deal with the prediction and analysis process. With the receipt of the medical data, the analysis may be performed utilizing an appropriate data transformation and interpretation approach. In a significant crisis, physicians and other medical needs can be contacted via smart-based applications on cell phones. With the help of apps built using advanced devices, smartphone users may get in touch with physicians or other medical professionals if they have major concerns. Identity measures are possible to perform when the situation is not life-threatening.

In comparison to the application layer responsible for medical information decision-making, which focuses on the analysis of data like patients, diseases, medications, diagnoses, and treatments, the medical information application layer stores various healthcare equipment and other materials related to information for maintaining patient information like inpatient, outpatient, medical treatment, and records. An automated warning may be sent to several parties in an emergency scenario, allowing them to take swift action that might save a human being's life. As an additional layer of protection, blockchain technology may be included in an IoMT network. To ensure the safety and accuracy of the stored data, the database is spread so that neither single entity is responsible for its care. As a result, confidence is built up with the need for an impartial mediator. The layer focuses on gathering information effectively from the source and constructing meaningful interpretations. These multiple outcomes have confirmed that data access and collection are essential components of the perception layer.

The primary responsibility of the data collection sublayer is a perception from the gathered data, which is accomplished with the aid of a wide variety of medical perception equipment and signals acquisition equipment. The data collected at the perception layer is sent accurately, consistently, in real-time, and without obstruction through mobile communication networks, wireless sensor networks, and the internet. But the service layer makes it possible to connect disparate systems like data warehouses, information description formats, and communication protocols. It does this by providing open interface services and other platform-related services to make these connections. Finally, the medical information decision-making application layer analyzes various information, such as patients, diseases, medications, diagnoses, and treatments.

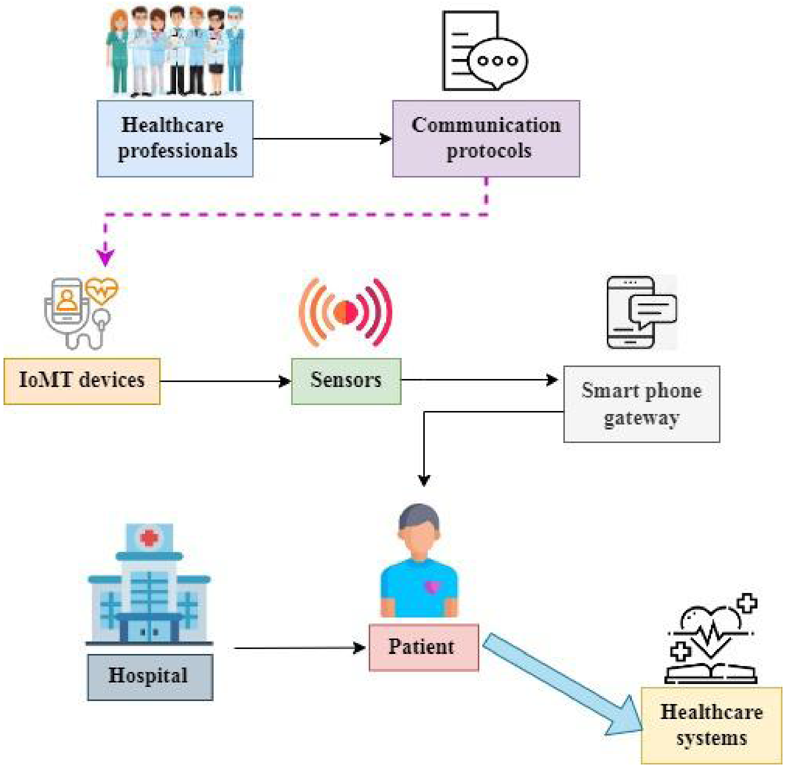

Figure 2. IoMT-based e-Health system

Figure 2 shows that the medical field has greatly changed over the last several decades, particularly in newly developed technology and treatment strategies. Developments in the Internet, wireless technologies, and communication links have led to improvements in the quality of healthcare that can be provided to patients either on the premises of a healthcare provider or remotely when patients have located a significant distance from their physicians. Remote monitoring uses various sensors to monitor vital signs, which are then communicated to remote physicians via the Internet by smartwatches, smartphones, and laptops. The Internet of Things results from many of these gadgets being linked to the internet to one another and various devices in the outside world IoT. The IoMT refers to the inclusion of various medical equipment and the ability to link them to various healthcare providers via the IoMT. By linking patients and doctors and enabling the transmission of medical data via the internet, a typical IoMT-based e-Health system can potentially lessen the need for patients to make trips to the hospital. With bringing together patients and medical professionals and facilitating the transmission of medical information online, IoMT has the potential to cut down on the number of hospital visits and related costs. Data obtained from patients are again entered into an electronic health record. A medical record displayed in digital rather than paper is labeled an electronic health record. The electronic health record can include information on the patient's demographics, symptoms, health information, various health data, vaccinations, laboratory and radiology findings, and patients' progress in terms of their medical treatment. Therefore, it is necessary to protect electronic medical records while transported and after data have been stored at the destination.

- As most IoMT devices are built with wireless communication capabilities, the are subject to most wireless security issues.
- Minimal compatibility across various IoMT software from different distributors can result in inadequate service safety.
- Security calculations need substantial computing power, and many IoMT devices are resource restricted. As a result, strong standard encryption is unsuitable for IoMT applications.
- Medical sensors, actuators, and gadgets may not meet security requirements, posing a threat to network durability. Furthermore, devices can be stolen, hijacked, and utilized to access patient and medical healthcare provider data.
- The utilization of the Internet to offer healthcare is a developing innovation field in that neither appropriate research has been performed. Likewise, medical device makers need IoMT security solutions.

Algorithm: The medical server handles sensor node data from the aggregator.
Agg: Aggregator for current sensing/transmission round

```
Distance between node  and node
Distance between node  and Aggregator
D (i; RN): Distance between node  and Relay Node
N: Total number of sensor nodes
Condition1:
Condition 2:
Condition 3: Data is not critical. Condition 4: Data is critical
for each node i of N, do
if (Condition 2 is true) then
This observation can be predicted accurately, and the detected value is discarded as it is redundant.
else
if (Condition 2 is true) then
if (Condition 4 is true) then
Node-i Transmit data directly to Aggregator
Else
If (Condition 3 is true) then
if D (i; Agg)  D(i; RN) then
Node-i Ta transmits data directly to Relay Node
end if
end for
```

Data Aggregation at Aggregator

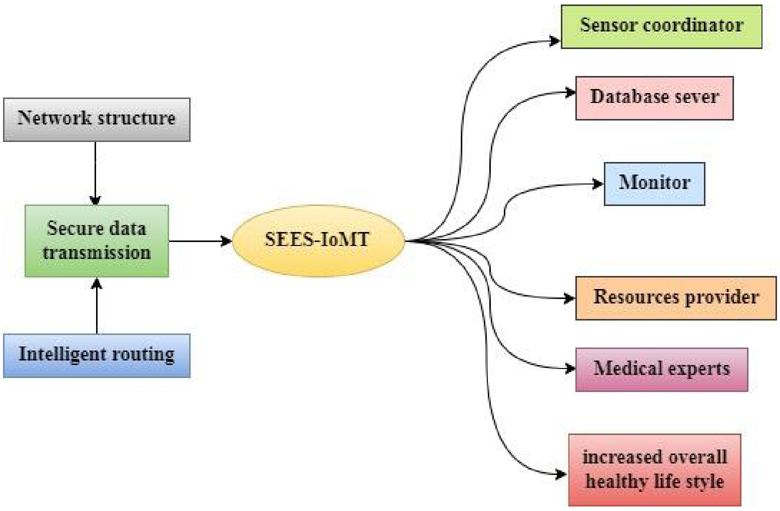

Figure 3. SEES-IoMT for e-healthcare

Figure 3, shown in the area, provides a comprehensive analysis of the mentioned framework tailored specifically for use in the healthcare industry. The suggested system reduces energy waste between biosensors and improves data security from a sink node to hospitals. The framework provides effective, reliable, and trusted emergency remote patient monitoring methods. basis of need; in case of necessity. In entering into the specifics of the framework, let's explore several network factors to keep in mind when modeling and developing a network. The sensor node is a device aware of the nodes immediately around it. The sensor nodes are identical in processing speed, amount of storage space, and bandwidth. There are no limits on the resources available at the sink node, and it also has greater computational power than the sensors. The sink node, similarly situated inside the patient's body, receives data from the sensor nodes and processes it. Intermediate devices transmit healthcare data from the sink node to medical professionals. Malicious nodes can launch attacks on the network infrastructure, destroying confidentiality, authenticity, and data integrity. Engineers discard data packets and broadcast faulty packets for route requests and answers to demonstrate their realistic behavior. In contrast, hospital, outpatient, and medical treatment records are stored in the medical information application layer and related healthcare devices.

- In addition, the medical data application layer contains various healthcare equipment and other materials related to information for maintaining patient information. SEEF-IoMT was created to ensure that the sensor nodes could optimally share power; therefore, it prioritizes low-power, short-range, reliable, and secure routing.
- The multi-parameter metric lessens the ratio of energy used by the nodes in producing unneeded route request packets while cutting down on the additional overheads on the node levels owing to the selection of the most reliable connections for data forwarding. In addition, the private-public key-based digital authentications are also integrated into data transmission using the cipher block interleaving method to assure validity and integrity.
- Statistical analysis of the simulation-based studies confirmed that the SEEF-IOMT is superior to previous work in energy efficiency, security, and network latency. However, future focus on enhancing the SEEF-IoMT in medical settings, including mobility sensor positions, is often modified due to human motion. In addition, energy efficiency and network security are areas where the proposed SEF-IoMT architecture might improve.

Experimental analysis

The IoT is now seeing widespread implementation among various industries, and the IoMT, a subdomain of the IoT used in the medical industry, is likewise getting the effective application. Health systems rely on this factor if this regard provides high-quality medical treatment. Consultants have offered an integration and a framework to solve the problems and difficulties associated with the IoMT. However, for future research to be successful, various factors must be investigated in complexity. With the tremendous improvements in IoT and communication innovation, healthcare has improved, and lives have been saved thanks to remote healthcare warning about the state of patients to doctors. However, there were issues with IoMT, particularly if healthcare pertained to the confidentiality and privacy of patient's medical records during transmission and storage. Since the previous several years, many studies have been conducted, mainly focusing on the IoMT's architecture and wearable medical devices.

Dataset Description: A 10 patient information is gathered using electrocardiogram patches that also track their activity levels and heart rates at night. The ability to measure oxygen saturation with a pulse is a bedside scale. Devices measuring and keeping track of respiratory function include a spirometer and a sphygmomanometer.

Table 1. Comparison of patient e-healthcare monitoring using the SEES-IoMT

Number of patients	BSDMF	DRL	CNN	SEES-IoMT
1	26,5	19,8	41,5	36,5
2	29,2	19,2	31,5	49,5
3	16,6	25,6	39,1	57,6
4	19,8	17,8	29,3	39,1
5	35,9	29,9	36,2	55,9
6	39,6	19,6	37,2	49,5
7	30,5	32,5	42,8	59,4
8	15,7	29,7	39,5	58,3
9	52,2	62,2	55,4	69,7
10	55,2	49,2	65,3	67,2

Table 1 denotes a knowledgeable e-healthcare system can function exactly if that receives correct and speedy information. As a result, the segment compares many intelligent healthcare data-collecting strategies to ensure accurate data collection. The patient reviewed a wide range of research on collecting private medical information, taking into account factors including precision, recall, and the likelihood of a positive or negative outcome. The benefits of data mining in healthcare are supported by research. Comparing the patient e-healthcare monitoring using the proposed method for the value calculated in 67,2 %.

Table 2. Error comparison of the patient e-healthcare monitoring in SEES-IoMT

Number of patients	BSDMF	DRL	CNN	SEES-IoMT
1	29,8	51,5	38,5	18,8
2	19,2	32,1	21,5	39,2
3	21,6	30,6	18,1	26,6
4	18,8	40,1	28,3	21,8
5	25,9	36,9	46,2	39,9
6	18,6	47,5	31,2	29,6
7	22,5	59,4	39,8	30,5
8	29,7	57,3	40,5	30,7
9	52,2	62,7	45,4	32,2
10	50,2	68,2	56,2	44,2

Table 2 says that The IoMT network can use a great variety of sensors, as shown in this section. Several factors must be considered in designing an IoMT network rather than merely picking the right sensor for the job. Therefore, solutions to the problems mentioned above cannot be found inside the implanted wearable IoMT devices but in the network and protocol that connects developing methods by focusing on efficient network structure, power conservation, and channel efficiency. As a result, here are a few factors to keep at heart while planning an IoMT network. The comparison of the proposed patient monitoring e-healthcare in the lowest error rate of 44,2 %.

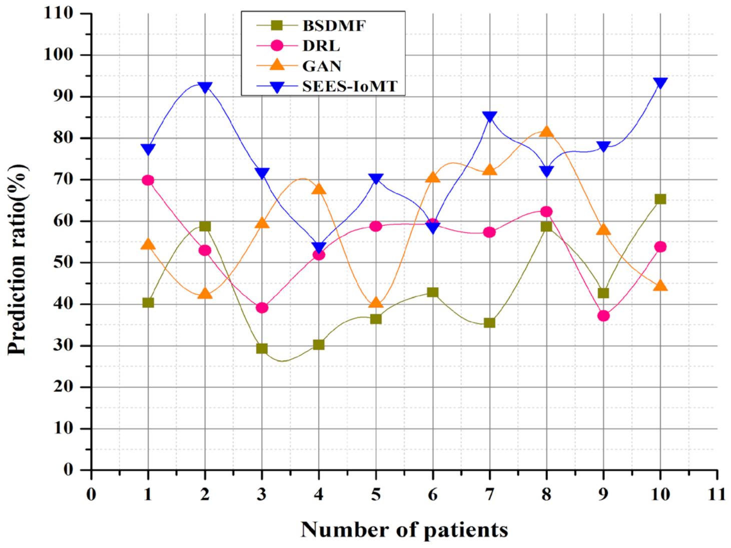

Figure 4. Prediction of patient monitoring e-healthcare in SEES-IoMT

Figure 4 shows that to facilitate the electronic storage and prompt transmission of medical records to the doctor, patient monitoring systems aim to standardize medical terminology and networking protocols. Providers can manage either acute or chronic diseases with the use of remote patient monitoring. Moreover, patients save money and avoid becoming sick by avoiding unnecessary trips. By facilitating more dialogue between doctors and their patients, remote monitoring can help increase patient satisfaction and retention rates. It reassures patients that their doctor is constantly looking in on reason; it is important to keep a face on a patient's identity to cut unnecessary suffering and expenses later on by catching diseases early on through monitoring.

Prompt diagnosis and treatment of various diseases can significantly enhance medical options for treatment. The comparison of prediction of patient e-healthcare in the proposed method is better than 93,2 %.

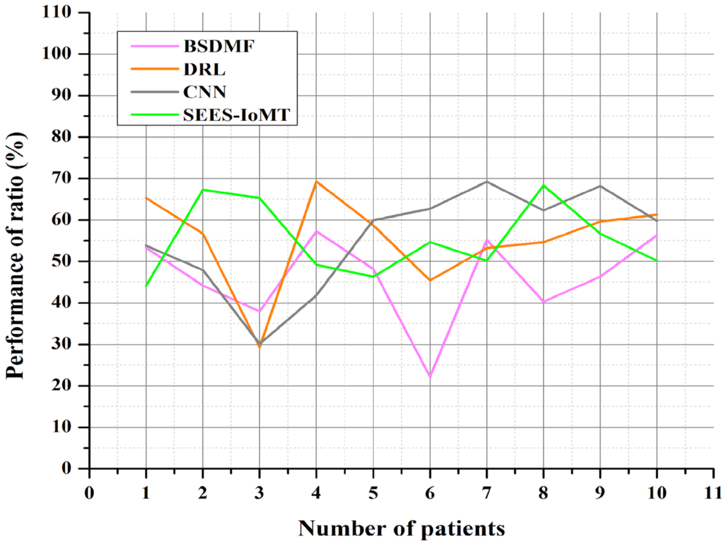

Figure 5. Performance of patient monitoring e-healthcare in SEES-IoMT

Figure 5 shows that Monitoring patients are crucial since it alerts doctors to potentially serious changes in a patient’s condition early enough so that doctors may improve their therapy appropriately. The aim may be attained by implementing a remote patient monitoring system that includes a medication management mechanism. The following are examples of ways Revolutions per minute may improve patients’ adherence to prescribed medical treatments: Medication compliance may be tracked via wireless patches. Compostable capsules with sensors for collecting patient information. However, the hardware, software, and capital equipment that make a patient monitoring system fall into one of three broad groups. Comprehensive administration of these medical devices at both the institutional and national levels is made possible by an information system that makes all performance metrics readily accessible. The result demonstrates that the overall deviation for patient monitors performance by 56,5 % after being subjected to a based framework for medical device management and evaluation over a period.

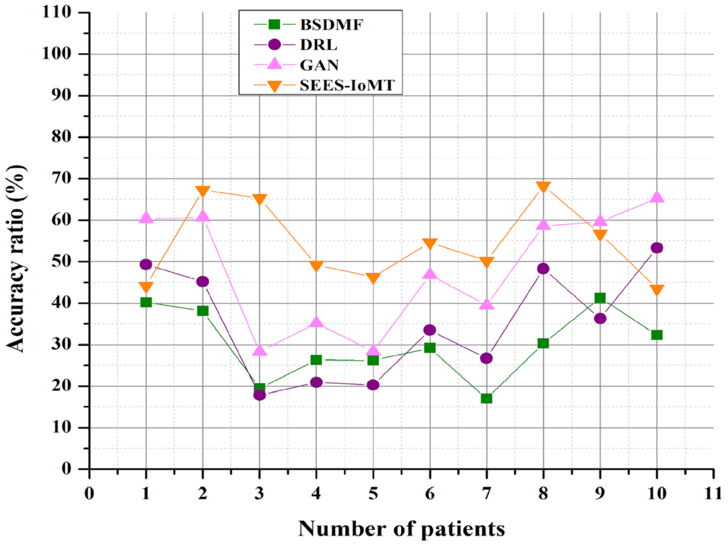

Figure 6. Accuracy of e-healthcare in SEES-IoMT

Figure 6 shows that patient-reported data can be explored as a possible means of strengthening documentation. Still, it is unlikely to be as thorough and reliable as more extensive data exchange between clinicians. Safeguarding sensitive information has been identified as the primary difficulty. Both patients and medical staff need to have complete faith in the privacy of electronic health records. The remainder were either wrong or unimportant. Sites run by government agencies were consistently rated as the most reliable. In healthcare, having correct data may be a matter of the distinction between life and death for the patient and the entire patient community. During each point in a patient's care, medical professionals require instantaneous access to the most up-to-date, accurate patient data possible. A long list of obstacles is in the way of a fully functional and efficient e-health system. The biggest problems are the lack of healthcare authorities' dedication and the inability to share data amongst health information systems. Scientists have been pointing up problems with e-health for over a decade. The accuracy comparison of the proposed method is the lowest ratio at 43,5 %.

CONCLUSION

The IoT has changed healthcare monitoring and patient data recording by making constant monitoring possible with fewer errors, lower costs, and fewer restrictions on available human resources. Vital indications of the human body, such as glucose levels, can be monitored to enhance the quality of life for the general population. Unfortunately, across the world, the prevalence of diabetes is rising, posing new difficulties for the healthcare system. To reduce energy usage and improve timely data distribution to medical specialists, offer a secure and energy-efficient architecture employing IoMT for e-healthcare. Using this implementation, SEEF-IoMT forwards data in chains encrypted with cypher blocks, making it more difficult for hackers to access sensitive information stored in electronic health records. Statistical analysis of the simulated tests shows that, compared to competing works, the SEEF-IOMT is superior in energy efficiency, security, and network latency. In the future, want to refine the SEEF-IoMT for use in medical settings that rely on mobility, where the location of sensors is often altered due to the patient's motion. Movements of the patient's body regularly, fluctuations An IoMT-based smart healthcare system can meet stringent criteria in areas such as the health monitoring device's temperature, the network's energy efficiency, the transmission range, the device's performance in a heterogeneous environment, the quality of service, and security. Although enlarged on previous efforts to tackle one of the fundamental difficulties of the effective use of energy, further investigation and analysis of the challenges themselves is necessary. Due to the sensitive nature of medical information, a thorough study and ongoing improvements are necessary to ensure the system's safety.

REFERENCES

1. Alam S, Shuaib M, Ahmad S, Jayakody DNK, Muthanna A, Bharany S, and Elgendy IA. Blockchain-based solutions supporting reliable healthcare for fog computing and Internet of medical things (IoMT) integration. Sustainability, 14(22), pp. 1-17. https://doi.org/10.3390/su142215312.

2. Kapoor B, Nagpal B, and Alharbi M. Secured healthcare monitoring for remote patient using energy-efficient IoT sensors. Computers and Electrical Engineering, 106, pp.108585. https://doi.org/10.1016/j.compeleceng.2023.108585.

3. Zala K, Thakkar HK, Jadeja R, Singh P, Kotecha K, and Shukla M. PRMS: design and development of patients' E-healthcare records management system for privacy preservation in third party cloud platforms. IEEE Access, 10, pp. 85777-85791. https://doi.org/10.1109/ACCESS.2022.3198094.

4. Saba T, Haseeb K, Ahmed I, and Rehman A. Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. Journal of Infection and Public Health, 13(10), pp. 1567-1575. https://doi.org/10.1016/j.jiph.2020.06.027.

5. Hireche R, Mansouri H, and Pathan ASK. Security and privacy management in Internet of Medical Things (IoMT): a synthesis. Journal of Cybersecurity and Privacy, 2(3), pp.640-661. https://doi.org/10.3390/jcp2030033.

6. Kapoor B, Nagpal B, and Alharbi M. Secured healthcare monitoring for remote patient using energy-efficient IoT sensors. Computers and Electrical Engineering, 106, pp.108585. https://doi.org/10.1016/j.compeleceng.2023.108585.

7. Bharathi R, Abirami T, Dhanasekaran S, Gupta D, Khanna A, Elhoseny M, and Shankar K. Energy efficient clustering with disease diagnosis model for IoT based sustainable healthcare systems. Sustainable Computing: Informatics and Systems, 28, pp. 100453. https://doi.org/10.1016/j.suscom.2020.100453.

8. Yaacoub JPA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, and Chehab A. Securing internet of medical things systems: Limitations, issues and recommendations. Future Generation Computer Systems, 105, pp. 581-606. https://doi.org/10.1016/j.future.2019.12.028.

9. Hireche R, Mansouri H, and Pathan ASK. Security and privacy management in Internet of Medical Things (IoMT): a synthesis. Journal of Cybersecurity and Privacy, 2(3), pp. 640-661. https://doi.org/10.3390/jcp2030033.

10. Kapoor B, Nagpal B, and Alharbi M. Secured healthcare monitoring for remote patient using energy-efficient IoT sensors. Computers and Electrical Engineering, 106, pp. 108585. https://doi.org/10.1016/j.compeleceng.2023.108585.

11. Sodhro AH, Al-Rakhami MS, Wang L, Magsi H, Zahid N, Pirbhulal S, Nisar K, and Ahmad A. Decentralized energy efficient model for data transmission in IoT-based healthcare system. In IEEE 93rd vehicular technology conference (VTC2021-Spring), pp. 1-5. https://doi.org/10.1109/VTC2021-Spring51267.2021.9448886.

12. Ray PP, Dash D, and Kumar N. Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions. Computer Communications, 160, pp. 111-131. https://doi.org/10.1016/j.comcom.2020.05.029.

13. Vora J, DevMurari P, Tanwar S, Tyagi S, Kumar N, and Obaidat MS. Blind signatures based secured e-healthcare system. In International conference on computer, information and telecommunication systems (CITS), pp. 1-5. https://doi.org/10.1109/CITS.2018.8440186.

14. Sun Y, Lo FPW, and Lo B. Security and privacy for the internet of medical things enabled healthcare systems: A survey. IEEE Access, 7, pp. 183339-183355. https://doi.org/10.1109/ACCESS.2019.2960617.

15. Deebak BD, and Al-Turjman F. Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. IEEE Journal on Selected Areas in Communications, 39(2), pp. 346-360. https://doi.org/10.1109/JSAC.2020.3020599.

16. Ullah A, Azeem M, Ashraf H, Alaboudi AA, Humayun M, and Jhanjhi NZ. Secure healthcare data aggregation and transmission in IoT—A survey. IEEE Access, 9, pp. 16849-16865. https://doi.org/10.1109/ACCESS.2021.3052850.

17. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, and Almansour FM. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and ubiquitous computing, 28(1), pp. 59-72. https://doi.org/10.1007/s00779-021-01583-8.

18. Liu M, Yu FR, Teng Y, Leung VC, and Song M. Performance optimization for blockchain-enabled industrial Internet of Things (IIoT) systems: A deep reinforcement learning approach. IEEE Transactions on Industrial Informatics, 15(6), pp. 3559-3570. https://doi.org/10.1109/TII.2019.2897805.

19. Patel WD, Pandya S, Koyuncu B, Ramani B, Bhaskar S, and Ghayvat H. NXTGeUH: LoRaWAN based NEXT generation ubiquitous healthcare system for vital signs monitoring & falls detection. In IEEE Punecon, pp. 1-8. https://doi.org/10.1109/PUNECON.2018.8745431.

20. Alotaibi M, and Alotaibi SS. Optimal disease diagnosis in internet of things (IoT) based healthcare system using energy efficient clustering. Applied Sciences, 12(8), pp. 1-16. https://doi.org/10.3390/app12083804.

21. Singla R, Kaur N, Koundal D, and Bharadwaj A. Challenges and developments in secure routing protocols for healthcare in WBAN: A comparative analysis. Wireless Personal Communications, pp.1-40. https://doi.org/10.1007/s11277-021-08969-0.

22. Haseeb K, Ahmad I, Awan II, Lloret J, and Bosch I. A machine learning SDN-enabled big data model for IoMT systems. Electronics, 10(18), pp. 1-13. https://doi.org/10.3390/electronics10182228.

23. https://datasetsearch.research.google.com/search?src=0&query=%20the%20Internet%20of%20Medical%20Things%20(IoMT)&docid=L2cvMTFrNDlienZjbg%3D%3D

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Veera V Rama Rao M.
Data curation: Shankar A.
Formal analysis: Balakrishnan S.
Research: N. Raghava Rao.
Methodology: Sureshkumar S.
Drafting - original draft: Kiran Sree Pokkuluri.
Writing - proofreading and editing: Veera V Rama Rao M.