Educational Administration: Theory and Practice
2024, 30(5), 15173 - 15183
ISSN: 2148-2403
https://kuey.net/

Research Article

Designing High-Efficiency Health Monitoring Systems With Enhanced Sensor Network Optimization

Ms. Heena Mehta[1*], Dr. Mukesh Singla[2]

[1*]Research Scholar, Department of Computer Science & Engineering, Baba Mastnath University, Rohtak.
[2]Supervisor & Professor, Department of Computer Science & Engineering, Baba Mastnath University, Rohtak.

Citation: Ms. Heena Mehta, et.al (2024), Designing High-Efficiency Health Monitoring Systems With Enhanced Sensor Network Optimization, *Educational Administration: Theory and Practice*, 30(5) 15173 - 15183
Doi: 10.53555/kuey.v30i5.8501

ARTICLE INFO

ABSTRACT

This study clarifies the advancement and enhancement of sophisticated sensor network-based health monitoring systems. In response to the growing need for precise health data in real-time, sophisticated devices capable of incessantly monitoring vital parameters have been developed. Modern sensor technologies, including biosensors, IoT devices, and wireless sensor networks, allow these systems to conduct data collecting and processing with little disruption. Optimization methods like as Particle Swarm Optimization (PSO), with machine learning algorithms and energy saving strategies, are used to improve the system's performance, dependability, and battery lifespan. The research emphasizes the creation of resilient and scalable systems applicable to many healthcare contexts, while examining data processing, communication protocols, network design, and sensor selection. Advanced sensor networks will be essential for future health monitoring, since studies demonstrate significant improvements in monitoring precision, system efficacy, and patient outcomes. The current technique is intended to provide a scalable and efficient solution. Furthermore, it would uphold privacy to provide a safe solution.

Keywords: Health monitoring systems, WSNs, IoT, Real-time monitoring, PSO, Machine learning.

[1] INTRODUCTION

The advancement of health monitoring technology has enabled continuous, real-time observation of vital signs and overall physiological health, therefore profoundly transforming healthcare. Their benefits to early disease identification, preventative care, chronic illness treatment, improved patient outcomes, and decreased healthcare costs are documented in [2]. The recent proliferation of sensor networks and advancements in research and development for optimal health monitoring systems has surged significantly. Contemporary sensor networks, including implanted sensors, wearable devices, and remote monitoring tools, provide the acquisition of complete and accurate health data. These devices can monitor almost all physiological parameters, including blood pressure, heart rate, glucose levels, temperature, and oxygen saturation. Cloud computing, artificial intelligence, and wireless networking technologies have significantly improved their capacity to analyze vast amounts of data and provide rapid, actionable insights. Nevertheless, the design of high-performance health monitoring systems necessitates the resolution of certain issues. It include guaranteeing sensor accuracy and reliability, developing techniques for prolonged device operation with minimal battery consumption, processing enormous data volumes, maintaining secure connection, and protecting user privacy [5]. For patients with chronic illnesses requiring ongoing monitoring, the systems must be user-friendly and comfortable for extended usage. This study primarily focuses on the optimization and enhancement of health monitoring systems via the utilization of sophisticated sensor networks. This study underscores the need of integrating system design, sensor selection, data handling, and energy optimization methods to develop robust, scalable, and efficient health monitoring systems [6]. The primary objective is to demonstrate how contemporary sensor technology and network architecture may revolutionize healthcare delivery, notwithstanding the many hurdles encountered. Modern technology has enabled HMSs to monitor and regulate vital health parameters of patients in real time. HMS utilizes equipment equipped with wearable sensors to monitor several physiological parameters, including heart rate, body temperature, and movement [7]. These technologies facilitate rapid treatments by allowing healthcare practitioners to

remotely access critical patient data via mobile applications, eliminating the need for continuous bedside monitoring. Individuals with chronic ailments or the elderly, who are particularly susceptible and need ongoing surveillance, may get significant advantages from Health Management Systems (HMS). The capability of HMS to promptly communicate with medical experts and caregivers during emergencies facilitates rapid reactions to any health deteriorations. HMS delivers real-time data, enhances patient safety, and reduces the need for ongoing physical monitoring relative to conventional patient care methods.

The Internet of Things (IoT) is an extensive system of interconnected computing devices, sensors, and other infrastructural elements capable of transmitting and disseminating data over the internet. Sensors, software, and communication technologies facilitate these "smart" gadgets in acquiring, transmitting, and autonomously analyzing data [9]. The Internet of Things encompasses wearable health gadgets, smart homes, municipal infrastructure, and industrial automation. Healthcare is a significant use of IoT; wearable sensors provide remote patient monitoring, while smart cities enhance public safety, traffic management, and energy efficiency [10]. The Internet of Things (IoT) has the potential to revolutionize interactions between organizations, people, and the environment by facilitating automation and real-time data transmission, hence enhancing efficiency and decision-making. The increasing use of this technology creates concerns around data privacy, security, and the administration of vast quantities of generated data [11].

Sensor networks consist of several dispersed sensors that measure and communicate data on physical or environmental parameters such as motion, humidity, pressure, temperature, and sound [12]. Establishing a network of these often interconnected wirelessly facilitates data collection, monitoring, and analysis over extensive regions. Sensor networks are essential in several fields, including healthcare, smart cities, industrial automation, environmental monitoring, and military surveillance [13, 14]. Wearable sensor networks have the potential to revolutionize healthcare by continuously monitoring patients' vital signs and health issues. This would facilitate the prompt identification of any concerns that may arise. In industrial settings, sensor networks optimize processes, monitor equipment performance, and identify errors [15]. These networks may either localize the data or transmit it to a centralized location for additional analysis to facilitate automation and enhance decision-making. Fundamental components of contemporary smart systems and sensor networks are evolving with emerging technologies to enhance scalability, energy efficiency, and the ability to handle intricate tasks. An HMS employs sensor networks that integrate various ambient and wearable sensors to continuously monitor and manage health parameters, hence enhancing patient care.

These technologies, including smartwatches and wristbands equipped with integrated sensors, monitor users' activity levels, heart rate, and temperature. A centralized system or cloud-based platform analyzes data received wirelessly from sensors in real-time to detect abnormalities and forecast probable health risks. This facilitates prompt interventions and reduces the need for hospital visits [18]. Through continuous, remote monitoring, HMS revolutionizes patient safety, data precision, and the ability to develop personalized treatment programs, marking a significant advancement in healthcare IT [19]. An IoT-based health monitoring terminal system represents a contemporary approach to health management that is comprehensive and current. This system links a centralized terminal or cloud-based platform to a network of health monitoring devices, including ambient sensors, intelligent medical apparatus, and wearable sensors via IoT. These devices monitor the patient's vital signs, activity levels, and environmental factors in real time, transmitting the data to a central database for further health assessments. The health monitoring terminal system, grounded in IoT, offers several benefits [21]. This encompasses the capability to remotely access patient information, get real-time notifications for critical medical occurrences, and seamlessly engage with healthcare providers' systems. The system facilitates data exchange and continuous monitoring, hence reducing the need for frequent in-person consultations by enabling prompt interventions. The system may also collect data from other sources to create comprehensive health profiles, therefore facilitating personalized therapy and long-term health management. The Internet of Things-based health monitoring terminal systems improve healthcare delivery and provide a contemporary answer to the challenges of patient health management in a globally interconnected environment [22].

Medical professionals and business leaders debate the evolution of healthcare monitoring systems. Extensive research has been conducted in this domain, with further studies underway. As the population ages and the prevalence of chronic diseases increases, the service gaps cited by healthcare professionals are expanding rapidly. Medical therapy, being solely administered in hospitals, often proves unsuitable and insufficiently responsive to the demands of the aged and disabled individuals. Sensor readings from IoT and telecommunications provide a viable solution for real-time geriatric health monitoring. The integration of IoT with smart technologies may boost several services. Researchers have developed many emergency systems using sensors and wireless communication technology. Numerous medical applications use these technology to monitor the health of the elderly. This enables the capture of vital signs and the collection of health and risk data. The Internet of Things will transform the healthcare sector. One of the several methods by which IoT and its healthcare applications improve individuals' lives is as follows: Wireless IoT technologies enable healthcare to reach patients, rather than requiring people to seek healthcare services. The data is safely gathered by an IoT sensor, processed by a compact algorithm, and then sent to healthcare professionals for personalized suggestions. Ongoing surveillance: internet-connected, non-invasive monitoring gadgets gather extensive data on mental health instantaneously. Data storage is administered by gateways and analytics deployed on the cloud.

[2] LITERATURE REVIEW

IoT's enormous effect on modern technology has created new opportunities and hazards in various domains. This research examines major IoT studies on development, security, and technological integration. Kumar et al. (2019) reviewed how IoT may transform technology. They discussed how the IoT may transform healthcare, business, and daily life [1]. An IoT-era cooperative virtual network security paradigm was created by Alabady et al. (2020). They proposed a system to promote IoT device cooperation and preserve data authenticity and privacy, solving important security issues [2]. Atlam et al. (2020) studied IoT security's privacy, safety, ethics, and safety. This work considerably expanded the literature on large-scale data collection and usage ethics and IoT security [3]. Mabodi et al. (2020) proposed a multi-tiered trust-based intelligence architecture to protect IoT against assaults. They detailed how their multi-level security may prevent data corruption and unauthorized access [4]. Bansal et al. (2020) examined all aspects of the IoT ecosystem, including devices, gateways, operating systems, middleware, and communication protocols. The Internet of Things (IoT) architecture and its components have been studied [5]. Kaur et al. examined ML, IoT, and digital twin connections in 2020. They discussed how these technologies may enhance IoT systems by converting data into intelligent analysis [6]. Rachit et al. (2021) summarized current IoT security advancements in their study. This research is essential for keeping up with IoT security developments and adapting to evolving threats [7]. Ashok et al. (2023) statistically examined IoT security models and remote health monitoring applications. They conducted realistic tests of remote health monitoring system security measures [8]. Palattella et al. (2016) examined IoT capabilities, architecture, and business models in their 5G study. They analyzed how 5G's faster connection, lower latency, and more capacity may boost IoT [9]. Islam et al. (2021) developed a secure, long-term ML predictive framework for IoT multimedia services. By predicting and resolving security risks, they built a framework to increase multimedia product durability and safety [10]. Zhang et al. (2020) used blockchain and big data mining to secure IoT-based agricultural applications. Blockchain and BG mining developed more secure and effective agricultural IoT systems [11]. Ayyer et al. (2021) used DL to enhance smart city threat detection and security. KH-AES encryption and IDS increased smart city security and attack resistance [12].

Table 1. Comparison of existing research

Ref	Author(s) & Year	Objectives	Methodology	Techniques	Limitations	Conclusion
[1]	Kumar, S., Tiwari, P., & Zymbler, M. (2019)	Review of IoT advancements and future potential	Literature review of IoT applications and impacts	Review and analysis	Lacks quantitative analysis	IoT holds significant potential for technological advancements in various sectors
[2]	Alabady, S. A., Al-Turjman, F., & Din, S. (2020)	Develop security model for cooperative virtual networks	Design and implementation of a novel security framework for virtual IoT networks	Cryptographic model and cooperative techniques	Limited scalability and practical testing in real environments	Presents an efficient security framework but needs scalability improvements
[3]	Atlam, H. F., & Wills, G. B. (2020)	Examine IoT security, privacy, safety, and ethics	Review of existing IoT security and privacy frameworks	Ethical analysis, privacy risk assessment	Lacks focus on specific applications or industries	Highlights ethical and privacy concerns and the need for balanced IoT security
[4]	Mabodi, K., et al. (2020)	Secure IoT against threats using a multi-level trust-based schema	Development of a cryptographic authentication scheme	Trust-based schema, cryptographic methods	High complexity for low-power IoT devices	Effective for security, but complex for lightweight IoT environments
[5]	Bansal, S., & Kumar, D. (2020)	Survey IoT ecosystem: devices, gateways, OS, middleware	Comparative analysis of IoT components and middleware	Survey and analysis	Does not evaluate real-time performance	Provides a comprehensive overview of IoT ecosystems
[6]	Kaur, M. J., et al. (2020)	Investigate convergence of Digital Twin, IoT, and ML for actionable insights	Examines Digital Twin and ML application on IoT data	Machine learning, Digital Twin	Limited case studies	Potentially transformative for real-time actionable insights
[7]	Rachit, Bhatt, S., & Ragiri, P.	Analyze security trends	Survey of recent IoT security	Comparative study	Lacks implementation	Provides an updated

	R. (2021)	in IoT	trends		examples	perspective on IoT security challenges
[8]	Ashok, K., & Gopikrishnan, S. (2023)	Analyze remote health monitoring IoT security models	Statistical analysis and review of IoT health monitoring models	Statistical methods	Focus on health sector limits broader application	Highlights security requirements specific to IoT health monitoring
[9]	Palattella, M. R., et al. (2016)	Review IoT architecture and business models for 5G	Examination of IoT enablers, architecture, and models in 5G networks	5G communication, business model analysis	Focuses on conceptual frameworks without practical application	Provides foundational understanding of 5G-IoT integration
[10]	Islam, N., et al. (2021)	Develop secure and sustainable framework for IoT-based multimedia	ML-based predictive framework for secure IoT multimedia	Machine learning, security protocols	Limited to multimedia context	Proposes an efficient, secure framework for multimedia in IoT
[11]	Zhang, F., & Zhang, Y. (2020)	Propose security model for IoT in agriculture using blockchain	Integrates blockchain and data mining for IoT security in agriculture	Blockchain, big data mining	High computational demand	Effective for secure agricultural IoT, but computationally intensive
[12]	Duraisamy, M. A., et al. (2021)	Enhance IoT security using deep learning for smart cities	Implementation of KH-AES in IDS for enhanced IoT security	Deep learning, KH-AES algorithm	Limited scalability in broader IoT systems	Effective for detecting attacks in smart cities, but lacks scalability
[13]	Anitha, R., & Raja, B. A. (2020)	Improve IoT data security with deep learning	Deep learning model for data security	Deep learning	Does not address lightweight device compatibility	Offers secure IoT data handling but not suitable for lightweight IoT devices
[14]	Haseeb, K., et al. (2020)	Develop energy-efficient and secure IoT framework for green environment	Big data analysis and energy-efficient framework	Big data analysis, energy-efficient protocols	High energy requirements for continuous data processing	Provides energy-efficient IoT solution with green potential
[15]	Andrea, I., et al. (2015)	Examine IoT security vulnerabilities and challenges	Analysis of IoT security risks and potential mitigation	Risk assessment	Early study; lacks emerging technology perspectives	Identifies early IoT security challenges
[16]	Wang, K.-H., et al. (2017)	Address lightweight security for RFID tags in IoT	Ultra-lightweight authentication protocol	RFID-based authentication	Limited applicability outside RFID environment	Suitable for IoT RFID, but limited to specific use cases
[17]	Schiliro, F., et al. (2019)	Develop IoT-enabled policing processes	Implementation of IoT for law enforcement	IoT policing processes	Ethical and privacy concerns	Effective policing model but needs enhanced privacy safeguards
[18]	Aversano, L., et al. (2021)	Review deep learning for IoT security	Systematic review of deep learning models for IoT security	Systematic review	Lacks practical applications	Highlights deep learning's potential but needs real-world applications

[3] PROBLEM STATEMENT

A primary barrier to the widespread adoption of continuous and accurate health monitoring is the inability of conventional healthcare systems to efficiently process and assess real-time data from a diverse array of physiological sensors. Advanced sensor networks must address several critical challenges to be effective in high-performance health monitoring systems. Challenges include data quality and dependability, energy optimization for extended device battery life, effective management and processing of large data volumes, and stringent privacy and security measures for sensitive health information. The responses must be readily accessible and sufficiently adaptable to accommodate various healthcare environments. The development and optimization of a cutting-edge health monitoring system, including many sensor networks, may effectively

tackle these practical and technological issues, therefore improving patient care, health outcomes, and actionable insights.

[4] PROPOSED Research Methodology

The proposed research aims to examine the function of PSO optimization inside machine learning, specifically concentrating on health monitoring systems that use sophisticated sensor networks. Initially, we will assess the existing literature pertinent to the proposed topic. Examples include efforts on medical, deep learning, and optimization subjects. Subsequently, one considers issues associated with prior investigations. The current healthcare system is susceptible to errors and inefficacious. Furthermore, a scalable system must be established. An optimization procedure is then used to get refined data, therefore excluding less significant healthcare information. Resolving issues related to disease detection performance and accuracy would imply their complete absence. The proposed work is eventually evaluated and contrasted with the traditional way to ensure the model's reliability.

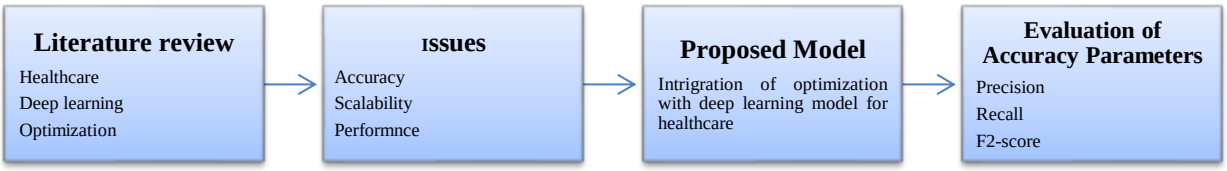


Fig. 1. Research Methodologies

Figure 4 illustrates the execution of the designated original technique, which includes testing on both optimum and suboptimal datasets in addition to training. PSO serves as the optimization technique for the study endeavor. The optimal method for filtering a dataset is achieved using PSO. Subsequently, training and testing are conducted using the filtered dataset. The acquired confusion matrix is analyzed using this classification to determine accuracy requirements. Evaluating the accuracy attributes of the two models will facilitate the selection of a better option.

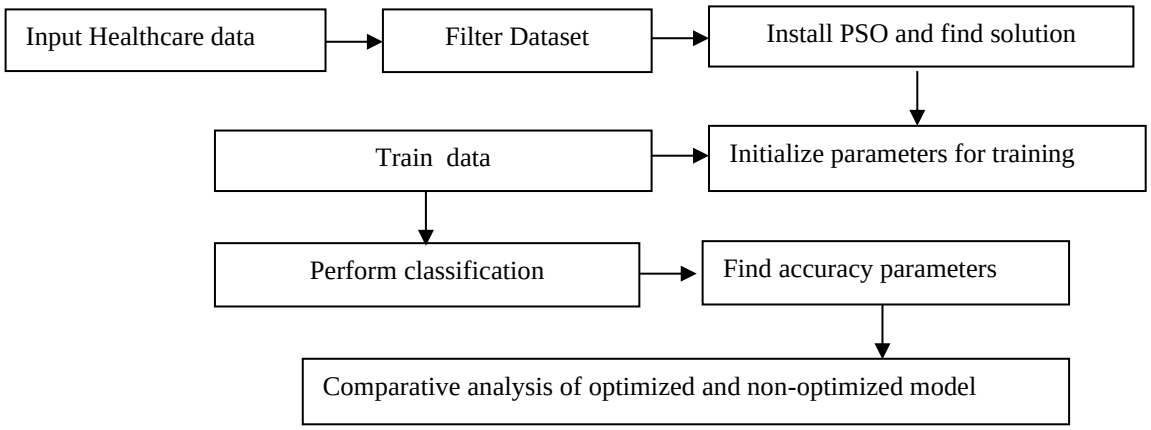


Fig. 2 Flow chart of a Proposed Model

[5] RESULT AND DISCUSSION

Examining the elements influencing the accuracy and performance of the robotics model helps one to grasp its use in different sectors. Different machine learning techniques are under investigation for classification needs; however, it is necessary to incorporate an optimization mechanism all through the process. Robotic services should become more accurate using event classification using a machine learning technique. Among the accuracy tests this study intends to improve, recall value, f-score, and precision are among those ones.

5.1 Confusion matrix for non-optimization model

Below is the confusion matrix for the non-optimized model. It demonstrates the classification performance across six classes.

Table 2 Confusion matrix for non-optimization model

Predicted Class	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6
Class 1	865	30	20	40	25	29
Class 2	15	875	35	10	30	28
Class 3	20	25	895	25	20	10

Class 4	40	15	25	880	30	20
Class 5	35	22	15	25	880	25
Class 6	25	33	10	20	15	888

Results: TP: 5283 and Overall Accuracy: 88.05%

Table 3 Accuracy parameters for non-optimization model

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	1000	1009	95.35%	0.86	0.86	0.86
2	1000	993	95.95%	0.88	0.88	0.88
3	1000	995	96.58%	0.90	0.90	0.90
4	1000	1010	95.83%	0.87	0.88	0.88
5	1000	1002	95.97%	0.88	0.88	0.88
6	1000	991	96.42%	0.90	0.89	0.89

5.2 Confusion matrix for optimization model

With optimization applied, the confusion matrix shows improvement in classification accuracy across all classes.

Table 4 Confusion matrix for optimization model

Predicted Class	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6
Class 1	920	10	10	15	15	19
Class 2	10	940	15	10	15	22
Class 3	15	10	940	15	10	10
Class 4	16	10	10	935	15	15
Class 5	25	15	10	15	935	15
Class 6	17	15	15	10	10	919

Results: TP: 5589 and Overall Accuracy: 93.15%

Table 5 Accuracy parameters for optimization model

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	1000	989	97.52%	0.93	0.92	0.93
2	1000	1012	97.8%	0.93	0.94	0.93
3	1000	1000	98%	0.94	0.94	0.94
4	1000	1001	97.82%	0.93	0.94	0.93
5	1000	1012	97.63%	0.92	0.94	0.93
6	1000	986	97.53%	0.93	0.92	0.93

5.3 Comparison Accuracy Parameters

The following table shows the comparison of key accuracy parameters between the optimized and non-optimized models.

1. Accuracy

Table 6 Comparison of accuracy

Class	Non-Optimization Model	Optimization Model
1	95.35%	97.52%
2	95.95%	97.80%
3	96.58%	98.00%
4	95.83%	97.82%
5	95.97%	97.63%
6	96.42%	97.53%

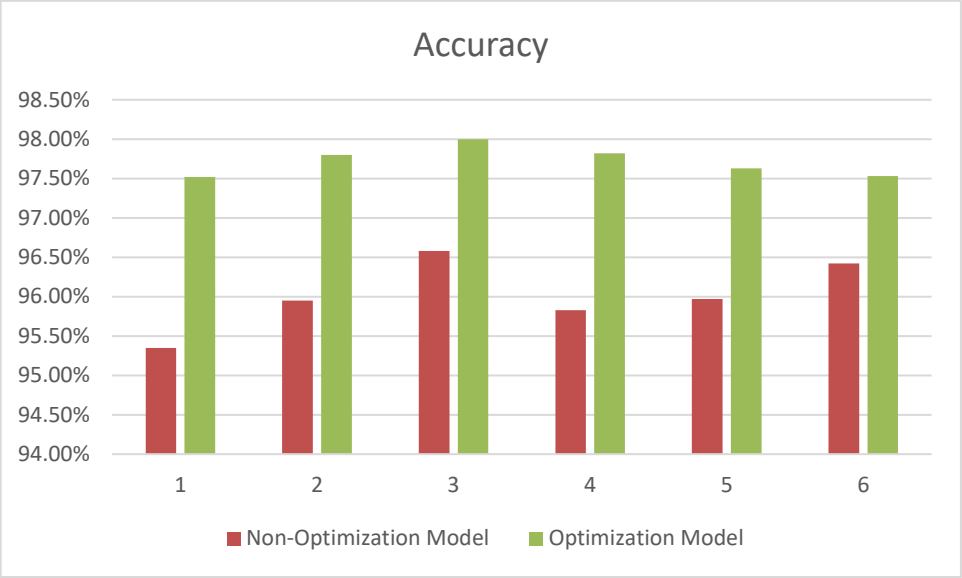


Fig 3 Comparison of accuracy

2. Precision

Table 7 Comparison of precision

Class	Non-Optimization Model	Optimization Model
1	0.86	0.93
2	0.88	0.93
3	0.9	0.94
4	0.87	0.93
5	0.88	0.92
6	0.9	0.93

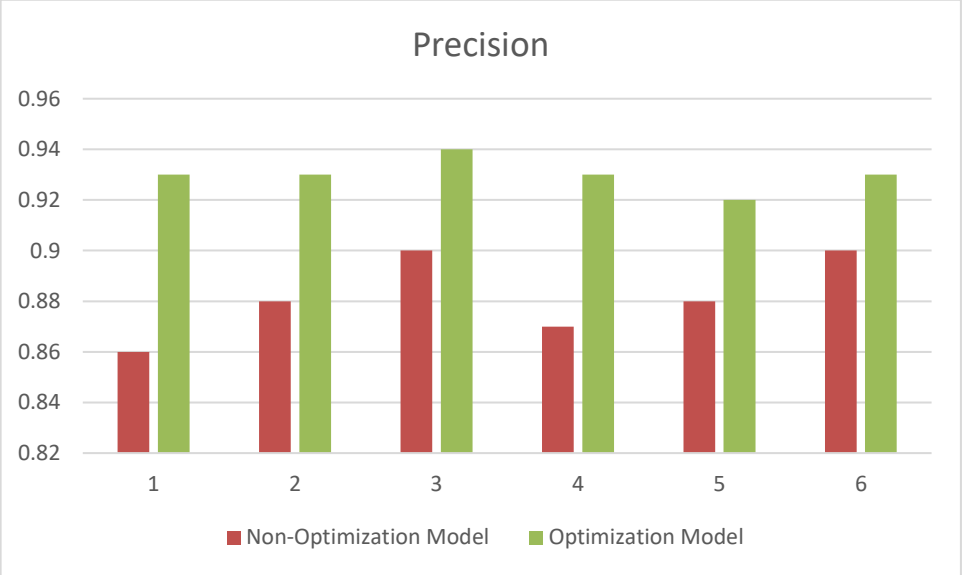


Fig 4 Comparison of precision

3. Recall value

Table 8 Comparison of Recall

Class	Non-Optimization Model	Optimization Model
1	0.86	0.92
2	0.88	0.94
3	0.9	0.94
4	0.88	0.94
5	0.88	0.94
6	0.89	0.92

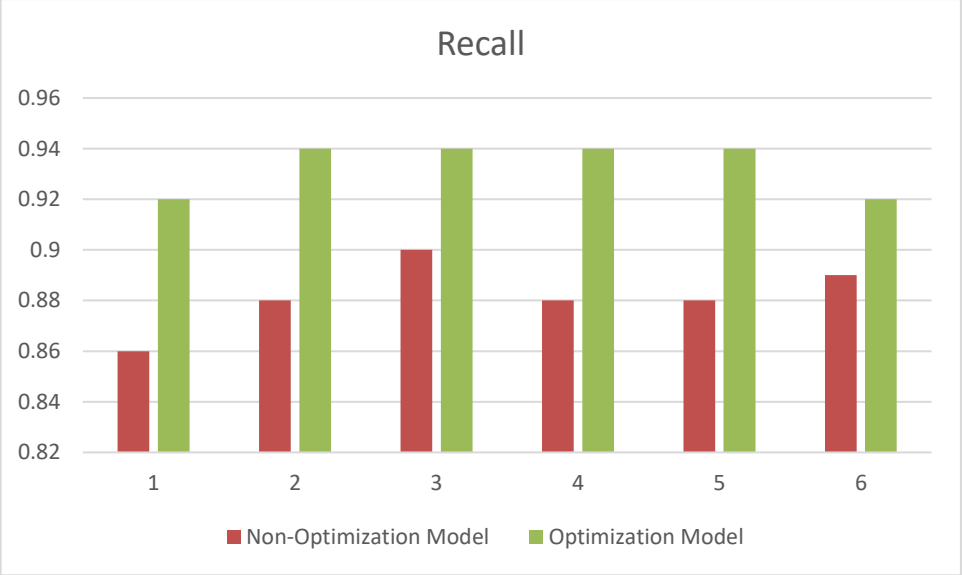


Fig 5 Comparison of recall

4. **F1-Score**

Table 9 Comparison of F1-Score

Class	Non-Optimization Model	Optimization Model
1	0.86	0.93
2	0.88	0.93
3	0.9	0.94
4	0.88	0.93
5	0.88	0.93
6	0.89	0.93

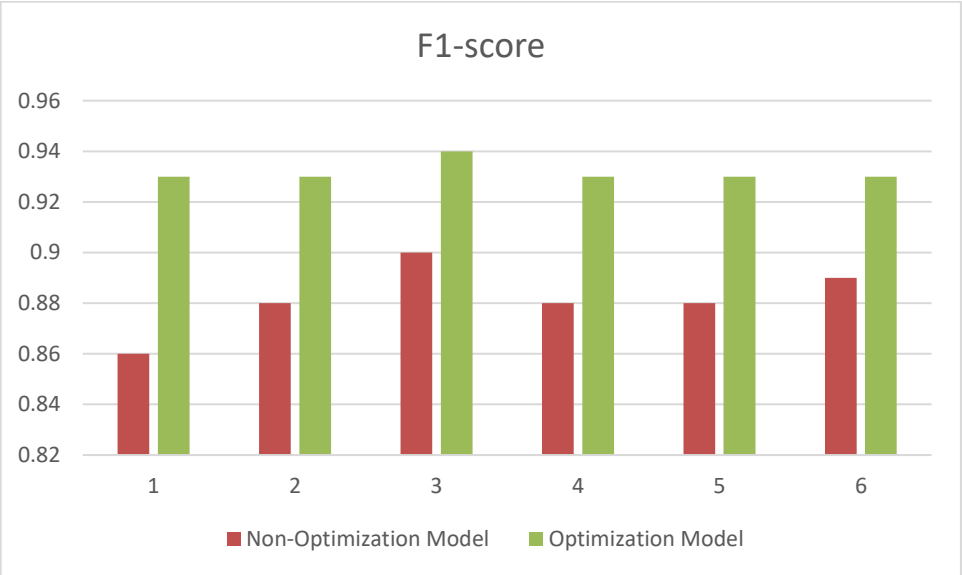


Fig 6 Comparison of F1-Score

5.4 Overall accuracy and error rate with its performance parameters

Table 2 shows accuracy and error rate for both an optimal and non-optimal dataset with six classes taken under consideration. Every class has one thousand components.

Table 10 Comparison of overall Accuracy and Error Rate

	Non optimized Model	Optimized model
Overall Accuracy	88.05%	93.15%
Error rate	11.95%	6.85%

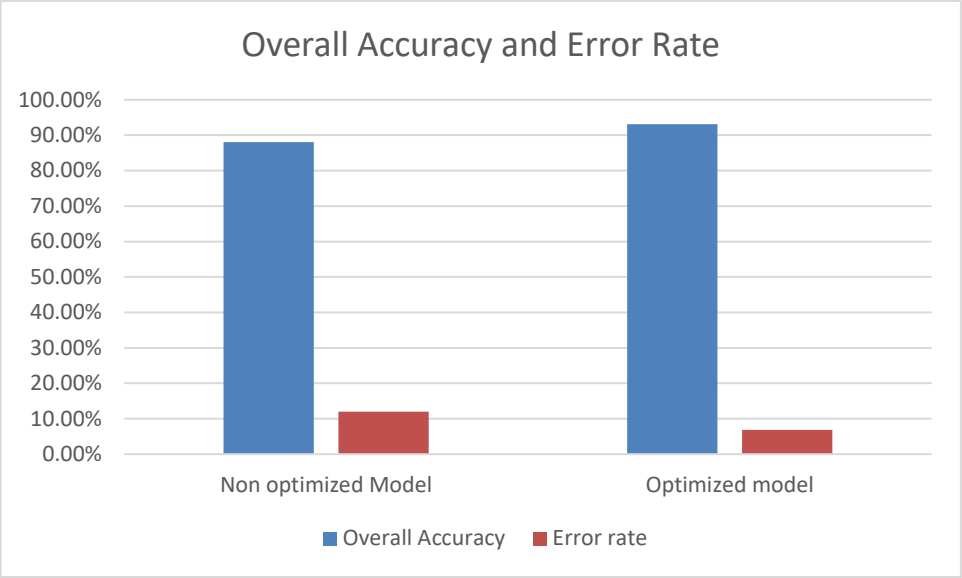
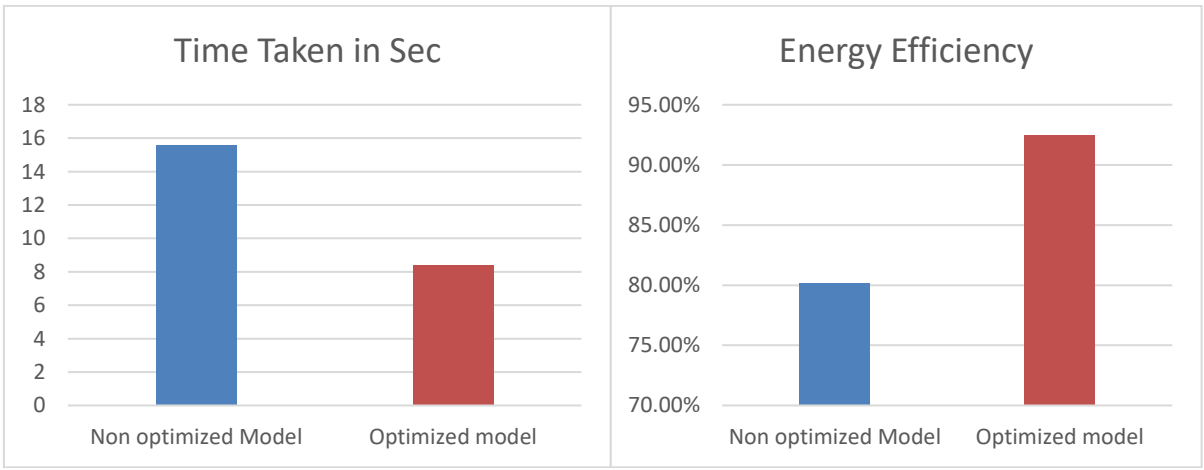


Fig. 7 Comparison of overall Accuracy and Error Rate

Here we will provide the performance figures for the proposed method as well as the conventional model. Table 1 displays the findings of a comparison between the proposed work and the standard model after the testing is over.

Table 11 Comparative Analysis of Performance

	Non optimized Model	Optimized model
Time Taken in Sec	15.6	8.4
Energy Efficiency	80.2%	92.5%



(a) Time taken in sec (b) Energy Efficiency

Fig. 8. Comparative Analysis of Performance

[6] CONCLUSION AND FUTURE SCOPE

High-performance health monitoring systems with sophisticated sensor networks represent a major breakthrough in healthcare IT. Modern systems with unique sensors and powerful network architecture continually and in real time monitor patient vital signs and health data to maximize accuracy, energy efficiency, data management, and security. Real-time data gathering and analysis allow fast interventions and individualized therapies, increasing patient outcomes and safety. Creating strong, scalable, and successful systems requires overcoming fundamental technological and regulatory constraints. These systems depend on modern data processing to handle and evaluate healthcare data. Privacy issues in data processing include anonymizing patient data to protect identities, while encryption technologies like AES safeguard data at rest and in transit. Communication protocols are essential for sensor, device, and central system data transmission. Privacy is protected via secure communication channels like TLS/SSL and security mechanisms including message integrity checks (HMAC) and encryption. Healthcare apps rely on network design, which separates sensitive data for privacy. Firewalls and IDSs prevent illegal access to boost security. Sensor selection prioritizes dependability and security, with data encryption and safe storage preferred. Access

restrictions and sensor firmware updates are also needed to ensure system integrity. Advanced sensor networks improve health monitoring accuracy and efficiency by integrating various sensors. Secure data aggregation and analysis safeguard privacy and assure data accuracy and safety. HIPAA compliance is ensured via privacy protection methods and procedures. Data reduction, purpose restriction, audits, and compliance checks are necessary to comply with privacy rules. These components provide the backbone of a resilient health monitoring system that adapts to current healthcare requirements, improves patient safety and cost reduction, and meets society's developing expectations with strong data security and privacy.

IoT is growing at an exponential rate, driven by the remarkable data exchange and interoperability of today's smart gadgets. The incredible power of modern smart gadgets is directly responsible for this. The healthcare industry is quickly using the Internet of Things as a tool for remote monitoring of patients' severity levels. This is due to its widespread and varied use in many applications worldwide. This technical advancement has impacted people's general quality of life, in addition to problems about people's health and safety. The use of computing, data processing, and storage in the cloud has the potential to enhance the Internet of Things. In addition to its many other applications, this technology also allows users to save geographic data on the cloud, making it accessible from any device. This is something that the majority of cloud storage companies provide.

REFERENCES

[1] Kumar, S., Tiwari, P., &Zymbler, M., “Internet of Things is a revolutionary approach for future technology enhancement: a review”, Journal of Big Data, Vol. 6, Issue no. 1, SN - 2196-1115, 2019.

[2] Alabady, Salah A., Al-Turjman, Fadi, Din, Sadia, “A Novel Security Model for Cooperative Virtual Networks in the IOT Era”, International Journal of Parallel Programming, Vol. 48, Issue no. 2, pp. 280-295, 2020.

[3] Atlam, H. F., & Wills, G. B., "IOT Security, Privacy, Safety, and Ethics", Springer International Publishing, Springer, Cham, pp. 123-149, 2020.

[4] Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L., &Fotohi, R., "Multi-level trust-based intelligence schema for securing of Internet of things (IoT) against security threats using cryptographic authentication", The Journal of Supercomputing, vol 76, issue no. 9, pp. 7081-7106, 2020.

[5] Bansal, S., & Kumar, D., “IOT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware and Communication”, International Journal of Wireless Information Networks, Vol - 27, Issue no. 3 pp. 340 - 364, 2020.

[6] Kaur, M. J., Mishra, V. P., &Maheshwari, P., "The Convergence of Digital Twin, IOT, and Machine Learning: Transforming Data into Action", Springer International Publishing, pp. 3 – 17, January 2020.

[7] Rachit, Bhatt, S., &Ragiri, P. R., “Security trends in Internet of Things: a survey”, SN Applied Sciences, vol 3, issue no. 1, pp. 121, 2021.

[8] K. Ashok and S. Gopikrishnan, "Statistical Analysis of Remote Health Monitoring Based IoT Security Models & Deployments From a Pragmatic Perspective," IEEE Access, vol. 11, no. December 2022, pp. 2621–2651, 2023, doi 10.1109/access.2023.3234632.

[9] Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., &Ladid, L., “Internet of Things in the 5G Era: Enablers, Architecture, and Business Models,” in IEEE Journal on Selected Areas in Communications, vol. 34, no. 3, pp. 510-527, March 2016.

[10] Islam, Naveed, Majid Altamimi, Khalid Haseeb, and Mohammad Siraj, “Secure and sustainable predictive framework for IOT-based multimedia services using machine learning,” Sustainability (Switzerland), 2021, Vol 13, Issues No. 23, ISSN 1–15. https://doi.org/10.3390/su132313128

[11] Zhang, Feng and Zhang, Yongheng, “A Big Data Mining and Blockchain-Enabled Security Approach for Agricultural Based on Internet of Things,” Wireless Communications and Mobile Computing, 2020, Pp: 1-8. 10.1155/2020/6612972.

[12] AyyerDuraisamy, MuthusamySubramaniam, Chinnanadar Ramachandran Rene Robin, “Optimized Deep Learning Based Security Enhancement and Attack Detection on IOT Using IDS and KH-AES for Smart Cities,” Studies in Informatics and Control, 2021, vol 30, issue no. 2, ISSN 121–131.

[13] R Anitha, A Brightlin Raja, “Data Security in IOT Environment using Deep Learning Technique”, International Journal of Creative Research Thoughts, 2020, vol 8, issue no. 6, ISSN 2320–2882. www.ijcrt.org

[14] Khalid Haseeb, Soojeong Lee, Gwanggil Jeon, “EBDS: An energy-efficient big data-based secure framework using Internet of Things for green environment,” Environmental Technology and Innovation, Volume 20, 2020, 101129, ISSN 2352-1864, https://doi.org/10.1016/j.eti.2020.101129.

[15] I. Andrea, C. Chrysostomou and G. Hadjichristofi, “Internet of Things: Security vulnerabilities and challenges,” 2015 IEEE Symposium on Computers and Communication (ISCC), pp. 180-187, 2015.

[16] Wang, K.-H., Chen, C.-M., Fang, W., & Wu, T.-Y., “On the security of a new ultra-lightweight authentication protocol in IOT environment for RFID tags” The Journal of Supercomputing, Vol. 74, Issue No. 1, pp. 65–70, 2017.

[17] Schiliro, F., Beheshti, A., Ghodratnama, S., Amouzgar, F., Benatallah, B., Yang, J., Sheng, Q. Z., Casati, F., &Motahari-Nezhad, H. R., “iCOP: IOT-Enabled Policing Processes”, LNPSE, Vol. 11434, pp. 447-452, 2019.
[18] Aversano, L., Bernardi, M. L., Cimitile, M., &Pecori, R., “A systematic review on Deep Learning approaches for IOT security,” Computer Science Review, Vol. 40, pp. 100389, May 2021.
[19] Saleem, T. J., & Chishti, M. A., "Deep learning for IOT: Potential benefits and use-cases," Digital Communications and Networks, Vol. 7, Issue No. 4, pp. 526-542, November 2021.
[20] Bian, J., Arafat, A. A., Xiong, H., Li, J., Li, L., Chen, H., Wang, J., Dou, D., &Guo, Z., "Machine Learning in Real-Time Internet of Things (IoT) Systems: A Survey," in IEEE Internet of Things Journal, vol. 9, Issue no. 11, pp. 8364-8386, 1 June 2022.
[21] Sanjay V, Dr. N. Suganthi, "Deep Learning Techniques In Internet Of Things (IoT) Security ", International Journal of Aquatic Science, Vol. 12, Issue No. 03, pp. 1453 - 1459, 2021.
[22] Sagu, A., & Gill, N. S., “Securing IOT Environment using Machine Learning Techniques,” International Journal of Engineering and Advanced Technology (IJEAT), Vol. 9, Issue No. 3, pp. 2249-8958, February 2020.