National Journal of Antennas and Propagation, ISSN: 2582-2659 Vol. 7, No. 2, 2025 (pp. 59-66)
RESEARCH ARTICLE
WWW.ANTENNAJOURNAL.COM

Next Generation Wireless Sensor Networks for Smart Healthcare Applications

Shriya Mahajan[1]*, Shivangi Gupta[2], Shashikant Deepak[3], Anbarasi Jebaselvi[4], Bichitrananda Patra[5], Raghu N[6], Amiya Dhar Dwivedi[7]

[1]Centre of Research Impact and Outcome, Chitkara University, Rajpura- 140417, Punjab, India.
[2]Quantum University Research Center, Quantum University, Roorkee, Uttarakhand, 247667, India.
[3]Assistant Professor, uGDX, ATLAS SkillTech University, Mumbai, India,
[4]Associate Professor, Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Chennai, India,
[5]Professor, Department of Computer Applications, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India,
[6]Associate Professor, Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Ramanagara District, Karnataka - 562112, India,
[7]Assistant Professor, Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Uttar Pradesh, India

KEYWORDS:
Wireless sensor Networks,
Smart healthcare,
Internet of Medical Things,
Edge computing,
Healthcare Data analytics,
Medical Alert Systems

ARTICLE HISTORY:

Received 13-01-2025
Revised 05-03-2025
Accepted 27-05-2025

DOI:
https://doi.org/10.31838/NJAP/07.02.11

Abstract

The fast development of sensor technology and wireless communication has opened the path for next-generation Wireless Sensor Networks (WSNs) to transform creative healthcare environments. Particularly in situations including remote patient monitoring, chronic disease management, and geriatric care, these modern WSNs provide smooth, real-time tracking and data analysis, so enabling proactive healthcare delivery. Innovative healthcare systems can guarantee rapid detection of medical irregularities and help critical decision-making by including intelligent sensors, low-power communication protocols, and edge/fog/cloud computing. The design, main elements, and difficulties of implementing next-generation WSNs in hospital settings are investigated in this work. System design elements include sensor choice, network topology, data aggregation, and intelligent analytics driven by artificial intelligence and machine learning get most importance. Furthermore, the framework of patient-centric data processing covers security, privacy, and energy economy problems. The paper ends by stressing present trends, future lines of research, and the transforming power of WSNs in creating responsive, resilient, and customized healthcare environments.

Author's e-mail id: shriya.mahajan.orp@chitkara.edu.in, shivangi.gupta@quantumeducation.in, shashikant.deepak@atlasuniversity.edu.in, anbarasi.enc@sathyabama.ac.in, bichitranandapatra@soa.ac.in, n.raghu@jainuniversity.ac.in, amiya.dhar@muit.in

Author's Orcid id: 0009-0004-1402-0931, 0009-0005-4285-8974, 0000-0003-0444-6889, 0000-0001-7792-6045, 0000-0001-6414-5389, 0000-0002-2091-8922, 0009-0004-0589-5840

How to cite th is article: Mahajan S, Deepak SGS, Jebaselvi A, Patra B, Raghu N, Dwivedi AD, Next Generation Wireless Sensor Networks for Smart Healthcare Applications, National Journal of Antennas and Propagation, Vol. 7, No.2, 2025 (pp. 59-66).

Introduction

Wireless connectivity, sensor miniaturisation, and computational intelligence have fundamentally changed the healthcare scene and made it possible for smart healthcare systems—personalized, proactive, patient-centric—to arise. Shum, A. (2024) The growth of Next-Generation Wireless Sensor Networks (WSNs), an intelligent network of linked biosensors and devices intended to monitor, gather, and transmit physiological data in real time, drives this change. Kavitha, M. (2024). With patient care started after symptoms show, traditional healthcare systems can rely on reactionary approaches. By means of next-generation WSNs, on

the other hand, vital indicators like heart rate, blood pressure, glucose levels, and oxygen saturation can be continuously monitored noninclusively. While lowering the load on clinical infrastructure, these networks are absolutely essential for remote patient monitoring—especially for managing chronic diseases, post-operative care, and geriatric support. Modern wireless sensor networks (WSNs) are connecting to new technologies like the Internet of Medical Things (IoMT), edge and fog computing, and AI-driven analytics more and more. Abdullah, D. (2024). This lets them respond quickly, find problems intelligently, and make predictions about future illnesses. Cheng, L. W., & Wei, B. L. (2024). Particularly in resource-limited and privacy-sensitive healthcare settings, these systems must also handle important difficulties including energy efficiency, data security, interoperability, and scalability. El-Saadawi.et al.,(2024) The design concepts, communication protocols, and technical enablers of next-generation WSNs specifically for smart healthcare applications are investigated in this work. It also addresses essential implementation issues and shows the future research path towards intelligent and resilient healthcare monitoring systems.

Background Information

Over the past two decades, technology integration into healthcare has acquired momentum; Wireless Sensor Networks (WSNs) are becoming a major enabler of this change. A Wireless Sensor Network is made up of autonomous sensors that are spread out throughout space and gather data and send it to a central processing unit, typically through wireless communication protocols. Often found in wearable or implantable devices, these sensors create Body Area Networks (BANs) or Ambient Assisted Living (AAL) systems in the context of healthcare. Originally designed for military and environmental monitoring, WSNs have recently been modified to fit healthcare environments, enabling remote and real-time patient physiological status monitoring. Growing demand for tailored healthcare, ageing populations, and the necessity to lessen reliance on conventional hospital-based care models have all helped to fuel this change. Smarter, more efficient WSNs have developed faster thanks to the rise of the Internet of Medical Things (IoMT), a subset of IoT especially targeted on medical equipment and applications. These next-generation networks combine low-power communication technologies (such as Bluetooth Low Energy, Zigbee, LoRa), multifarious and tiny sensors, and sophisticated data analytics. Using edge or fog computing, they are meant to gather data and process it locally; they then securely communicate it and support real-time decision-making. WSNs help smart healthcare systems in several respects. Constant monitoring helps to identify health problems early on before they become critical. Mobility and Comfort: lets patients keep their regular activities under observation. Reducing hospital admissions helps to maximise resources by means of cost control. Supporting evidence-based treatments and long-term health management, data-driven care Implementing WSNs in healthcare provides difficulties including energy restrictions, dependable connectivity, security and privacy concerns, and standardising obstacles notwithstanding their possible value. Development of strong and scalable healthcare solutions depends on breaking through these obstacles. Next-generation WSNs will become even more important in enabling intelligent, networked, and patient-oriented medical services as healthcare systems migrate towards predictive and preventive care models.

Key Contribution

- Provides an in-depth architectural design of the technology framework for healthcare WSNs as sensor nodes, edge/fog/cloud layer units, and AI-enabled decision-making modules.
- Discusses the enabling factors IoMT, edge computing, and machine learning add to WSNs for intelligent health monitoring, contributing to dynamic and responsive levels of care.
- Examines energy-efficient policies and WSN routing strategies about health care with an intent to solve a key challenge to WSN implementation.
- Discusses advances in secure data transmission, lightweight encryption, and privacy-preserving models for sensitive health data.
- Ongoing issues of interoperability, lack of standardization, and ethical issues are gaps to be solved in future research and development initiatives.

Various sections follow the research report. Section I describes the introduction of the topic. Section II describes the background information and provides the main objectives of this research. Section III describes the literature review of the previous research. Section IV describes the system architecture. Section V describes the proposed methodology, Algorithms. Section VI describes the results and analysis for authentication of time complexity, the Time complexity for Elgamal key generation, the time complexity of key algorithms, and the discussion part. Section VII summarized the research report and key findings.

Literature Review

Over the past ten years, research on the integration of Wireless Sensor Networks (WSNs) into healthcare has

been somewhat extensively investigated. Many studies have shown their ability to transform medical monitoring and treatment delivery using real-time data collecting, mobility support, and affordable care. WSN Evolution in Healthcare: Early WSN implementations in healthcare mostly concentrated on wearable health monitors for parameters such as mobility tracking, body temperature, and heart rate [Akyildiz et al., 2002]. These systems developed into increasingly sophisticated designs using Body Area Networks (BANs), which let several sensors interact with a central coordinator, usually a smartphone or gateway device [Otto et al., 2006]. The Internet of Medical Things (IoMT) has made WSNs possible to join a larger, linked ecosystem. Research by Islam et al. (2015) and Zhang et al. (2019) underline how IoMT systems combine sensor networks with cloud and edge computing to assist data storage, processing, and diagnosis. By moving computation towards the data source via fog and edge computing, these smart systems also assist reduce the latency and bandwidth restrictions of conventional cloud-based designs. A main obstacle in WSNs for healthcare is power usage. Martinez, R., & Garcia, C. (2024). Many publications, including LEACH protocol and its variants by Heinzelman et al., seek to maximise energy consumption by means of data aggregation and clusterizing. Machine learning is included into recent methods to dynamically optimise routeing and forecast node failures [Al-Fuqaha et al., 2015]. Maintaining patient privacy and data security continues to be a challenge. While new blockchain-based solutions (e.g., by Dwivedi et al., 2020) are under investigation to offer distributed, tamper-resistant medical data records, research by Mahalle et al. (2013) addresses lightweight encryption approaches for limited sensor nodes. Using artificial intelligence and machine learning has improved the analytical power of WSN-based systems. Research on health anomalies, sensor operations optimisation, and illness trend prediction in real time using support vector machines (SVM), convolutional neural networks (CNNs), and reinforcement learning have shown [Chen et al., 2020]. Remote patient monitoring, rehabilitation tracking, and senior care have dominated several experimental projects and deployments. Though scalability and interoperability are still outstanding issues, projects like MobiHealth and CodeBlue have shown that WSNs are feasible in home-based care environments.

System Architecture

Figure 1 shows the smart healthcare relevant application over IoT. A CRN deals with spectrum use more efficiently and mitigates interference. Different two classes of users, primary and secondary, have different hierarchical control privileges over the decommissioned channel. Due to having real-time and critical data transmission and due to considering bandwidth availability most important, primary users have more dominance than secondary users.Xu, X., & Lu, W. (2024). The first stage is to open the bandwidth; spectrum sensing now relies on eviction detection of idle bandwidth information traffic stream. Synchronizing to detect the vacant band, bandwidth access frameworks modify the channel access scheduling of the WBAN. Encompassing such applications as mobile telephony, (DVB), wireless local area networks (Wi-Fi),

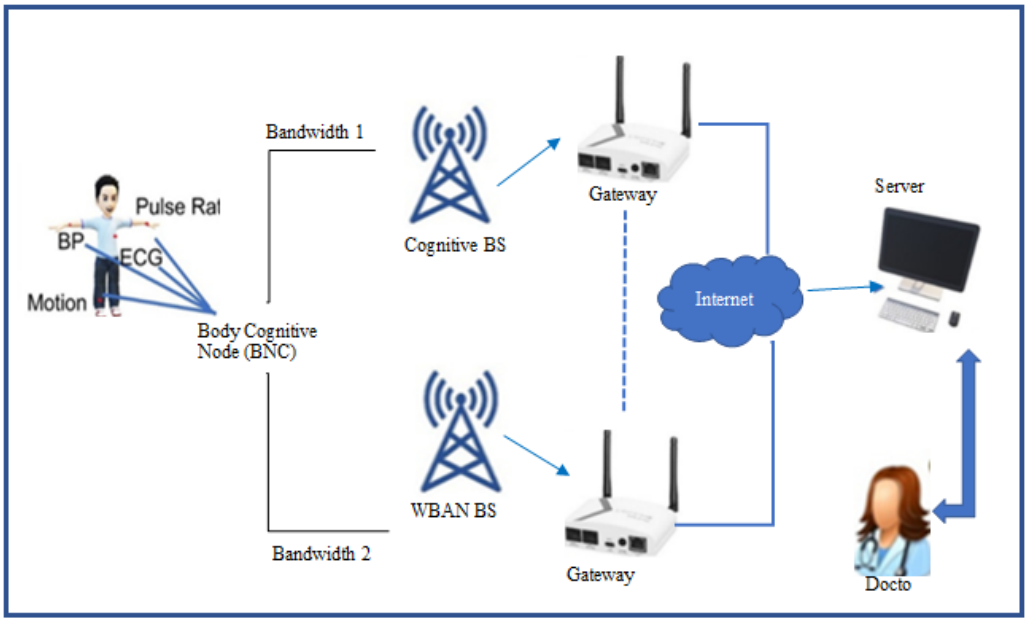


Fig. 1: Smart Healthcare Application

wireless sensor networks (ZigBee) and the internet of things have an immense and ever-increasing demand for radio frequency spectrum. David Winster Praveenraj, et al., (2024). It functions on average time and throughput performance. It opens up extra bandwidth for wireless devices to access opportunistically, thus increasing the overall throughput obtained by these devices, which is its main advantage.

In CRNs, intrusion detection relates to hostile or unauthorized access to computer or network resources. The use of CRNs has enabled better spectrum resource utilization by taking advantage of underused licensed spectrum. Wireless communication systems have applications in cognitive radio, which mitigates spectrum scarcity to a great extent. In mobile cognitive ad hoc networks, secondary users (SU) continuously monitor the activities of primary users (PU) and exploit PU controlled idle channels on a lease basis as per demand. The maintenance of the high quality of communication is directly dependent on workable approaches to the control of interference and efficient use of the temporarily available set of frequency subbands. Moreover, notable is computational complexity in implementation of several analogous systems studied from literature. This complexity increases the total operational price of the system, thus making the system structure difficult to maintain. We study the problem of optimal resource allocation for supportive CRN with unscrupulous licensed range access. Information is transmitted to the server in encrypted form, and the communication protocol used is CRN. Thus, CRN is the most feasible and inexpensive solution for data delivery.

Proposed Methodology

With respect to device and patient authentication, our WBAN-CRN system incorporates the CRN protocol with the DNA based Security Encoding Algorithm (DEA) for data encryption. The data retrieved from the IoT-enabled WBAN system is encoded with DEA, and a key is generated using the ElGamal method. The Biomedical server is sent data in CRN ciphertext form, via wireless transmission. The Nurse body language recognition system employs nano sensor nodes fixed on the patient's body to continuously monitor and record critical health data such as body-temperature, sugar concentration, heart rate (ECG), and blood pressure. The CRN networks guides this data. Multi electromagnetic spectrum methods can be used for transmitting data to the server. The WBAN channel is modified for sensing by discovering idle spectrum. The cognitive network notes the spectrum when data is not being transmitted and idle spectrum allocation. They use fewer computational resources and are more time-efficient during transfers. Also shown are the four parts of the WBAN-CR network: access points, gateways, medical servers, and doctors' owned nodes. BNC nodes serve as sensors. As nomadic authentication is the first line of defense against identity theft, patients and the sensor devices associated with them serve as the first authentication guard. Data collection by the Nano sensors is routed to the gateway for further collection. The patient registers with gateway using their mobile phone which uses Nano sensors. The Civil ID card database captures the registered sensors features. SID serves as a special identifier for the gateway database hosting the mounted sensors for each Nano sensor during the encompassing peripheral sensor registration phase. Upadhyay, N.,et al (2024). The suggested DNA Encryption Algorithm (DEA) uses fewer computing resources and memory. Initially, an encryption key is created through ElGamal method, which is then applied using DEA method to encrypt data. Systems that employ a symmetric scheme use one key for both encryption and decryption, while an asymmetric scheme uses a private key for encoding and public key for decoding. In our proposed method, the symmetric key is derived from the ElGamal scheme to forge a mutual password for shared data. Initially, the participants wishing to initiate one side communication select two common prime numbers P and D. Then, T=(E)^d mod P is generated from T. E is chosen arbitrarily. The figure explains the proposed approach for encrypting our approach. Ciphertext is obtained from a DNA table containing DNA sequences, which is then transformed into binary in the decryption process.

The S-block data is retrieved, and a circular left shift one operation is performed using the outcome data. Each subseque0nt operation produces two portions of four bits; in the case of the first group of four bits, the first portion is employed while the second portion is omitted (because they were incorporated due to the DNA).

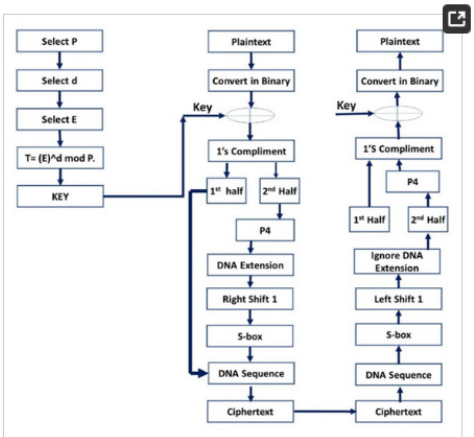


Figure 2. Encryption and Decryption Algorithm.

Algorithm:1 Key Generation and DNA Encryption

Key Generation
Begin
Select Prime Number P
Select Private Key D
Select Public Key E
T=(E)^d mod P
Value of T will be key value
DNA Based Encryption (at WBAN's Sensors)
Begin
for each NS ¤ PD do
sensor node sends authenticated data towards PD through DNA Encryption Securely
Then idle spectrum is being sensed to transfer data
Through the idle bandwidth spectrum,PD transfers data to BS
end for
for each NS¤PD do
if(PD receives data from NS securely),then
encrypted data is ready to transfer over idle bandwidth spectrum
else if (PD does not receive data in given slot from NS) then
Bandwidth is not sensed for idle spectrum
else if (BS receives data from PD successfully)then
Bandwidth is not sensed for idle spetrum
else if (BS receives data from PD successfully)then
data is transferred to cognitive networks BS
end if
end for

DNA Encryption Algorithm (DEA) (Cognitive Networks)
Begin
Bs transmits data to gateway safely encrypted using DEA
Data is transfered from the gateway to the medical server
for each BS GW do
if (BS safely receives data from the spectrum),then
Gateway is used to transport data over clouds
Data is not identified by the Gateway to send over clouds
if (BS does not receive data from any spectrum in specified slot)
End if
if (data from BS to Gateway)is true,then
Gateway clouds deliver data to the medical server
End if
End for

Results and Analysis

For these tests, we simulated cognitive radio networks incorporating MATLAB 2013a. The simulation focused on a field space of 100 by 100 meters. ECG data from the body was captured. The WBAN provided comprehensive data returns and also executed ECG signal recognition of a human heart. The WBAN's data was transferred to the biomedical server using CRN as the routing protocol over bandwidth spectrum. Through a higher energy detector, several antennas are capable of exposing empty spectrum CRNs for. The overview results of the suggested system detail this simulation. There are two evaluation components, assessments and outcomes. Performance assessments is a form of evaluation that monitors the elapsed time required for data encryption or decryption through the algorithm. We analyzed the claimed times which, in this case the times necessary to execute the defined operations within the restricted time windows, were calculated in the reasonable periods. We benchmarked our baseline designs, AES-CTR and ECC, against others.

Analysis of Authentication Time Complexity

We determine the time taken in computing patient and gatekeeper access authentication of the sensors. The response time has been noted to increase as the time for small sensors to register increases; for example, the five microphones take approximately three microseconds when sensor 1 registers at 0.5 microseconds. Overall, it can be observed from figure 7 that, in the case of people, authentication is done faster and more efficiently.

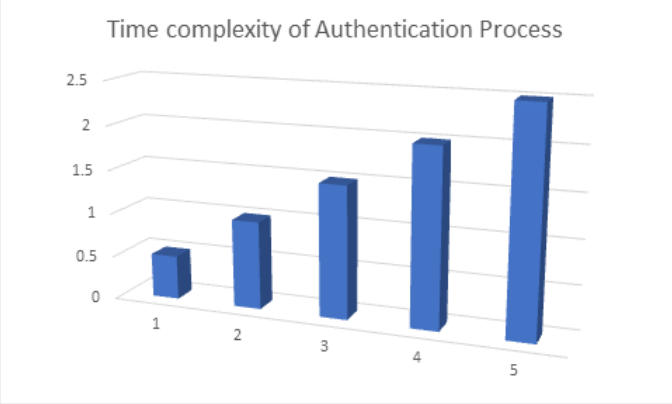
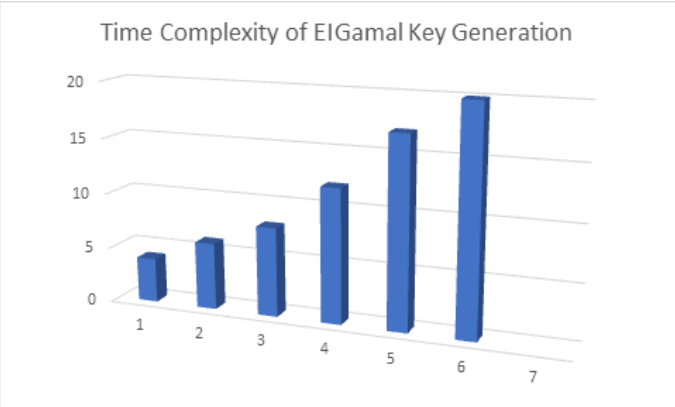


Fig. 2: Time Complexity of ElGamal Key Generation

Time Complexity for Eigamal Key Generation

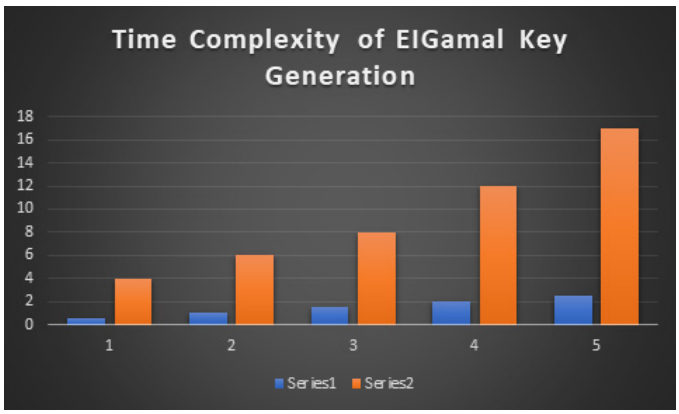
The ElGamal method's computational time is defined as its key generation time; this includes data bytes and elapsed time required during encryption key generation. There is an observable relationship between data byte

count and the time consumed during execution; as data bytes increase, time spent also increases. When calculating the data bits for key production, it takes 9.5 microseconds for 30 bytes and 21 microseconds for 60 bytes.



Time Complexity Comparison for Key Algorithms

The ElGamal Key generating algorithm gives reason to support for the encryption method under discussion which is compared with the Diffie-Hellman Key generating technique. In the figure, it is shown that the time they consumed also grew as the data bytes increased, for example, one data byte took about 2 microseconds in the ElGamal method while in Diffie-Hellman it grew to 5 microseconds at the same level of data byte.



Discussion

As a result of uncontested acceptance of the Internet of Things in the healthcare domain, its implementations through sensors pose numerous challenges, amongst which lies the question of protecting the information. This problem is complicated because of limited memory and energy supply available to the sensors. Though encryption techniques have been attempted, the absence of sufficient operational capacity makes many of them unsuitable for remote sensors. Results of DNA procedures exhibiting data security as defined in Figure 11 are then compared with the proposed DNA based approach. In , DNA-based data verification was used, and DVSSA was applied with a DNA-based approach. Visualization of expenditure on energy and data security for remote sensors illustrates the relationship between security and computational energy spent. Other works are used to secure data over the wireless network. It was shown that the proposed methods based on DNA systems were the most energy efficient compared to previously suggested methods. A new technique was also proposed based on the DEA encryption approach. In this case, we incorporated the ElGamal key generator for additional optimization of the system. The CRN routing protocol uses the unused spectrum for data transmission and therefore operates on the energy-efficient approach. The lightweight proposed algorithm was used to process data extracted from the ECG to enhance the performance of the identified data streams. Following the protocol, the data described by the commanding response network is encrypted according to the described DNAbased scheme.This strategy aids in minimizing security risks and interference. CRN manages the routing for sending the sensor data to the biomedical server via a bandwidth spectrum. Through the use of several antennas, better energy detectors are able to aid CRN's wideband spectrum scavenging. In terms of time complexity, the proposed method is efficient concerning the transfer of data devoid of attacks and intrusion from unwarranted mediators. Illustrating the likenesses, differences, and paradoxes captures the outcomes techniques which are dissected and elaborated from the qualitative reasoning and quantitative logic. Dual-axis graphical representation allows for the analysis of two different data points for outcome comparison. The proposed method has improved results because the approach employs the effective and lightweight DEA algorithm, unlike the current method, which is cumbersome to implement and exceeds execution time. Furthermore, the suggested approach effortlessly illustrates the relationship between the two variables possessing different measurement scales using dual axes.

Conclusion

In developing smart healthcare systems, next-generation wireless sensor networks (WSNs) constitute a transforming technology. These technologies help early diagnosis, preventive care, and better patient outcomes by allowing real-time, continuous, and remote monitoring of patients—all of which help to lower the load on the healthcare infrastructure. Low-power sensors, cognitive data processing via edge and cloud computing, and AI-driven decision-making have substantially increased WSN capabilities outside conventional monitoring. Notwithstanding major progress, some issues affect

energy efficiency, data security, interoperability, and long-term adoption in actual healthcare situations. Furthermore, ethical issues and the necessity of uniform procedures to guarantee fair and safe application of these technologies should be addressed. To fully realise the possibilities of next-generation WSNs, multidisciplinary cooperation among engineers, medical experts, and legislators will be indispensable looking forward. These systems are ready to be crucial in building a more linked, efficient, and patient-centered healthcare ecosystem with ongoing innovation and cautious application.

References

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. Computer Networks, 38(4), 393–422. https://doi.org/10.1016/S1389-1286(01)00302-4
2. Otto, C., Milenkovic, A., Sanders, C., & Jovanov, E. (2006). System architecture of a wireless body area sensor network for ubiquitous health monitoring. Journal of Mobile Multimedia, 1(4), 307–326.
3. Shum, A. (2024). System-level architectures and optimization of low-cost, high-dimensional MIMO antennas for 5G technologies. National Journal of Antennas and Propagation, 6(1), 58–67.
4. Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of Things for health care: A comprehensive survey. IEEE Access, 3, 678–708. https://doi.org/10.1109/ACCESS.2015.2437951.
5. Kavitha, M. (2024). Enhancing security and privacy in reconfigurable computing: Challenges and methods. SCCTS Transactions on Reconfigurable Computing, 1(1), 16-20. https://doi.org/10.31838/RCC/01.01.04
6. Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M., & Alamri, A. (2019). Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. IEEE Systems Journal, 11(1), 88–95. https://doi.org/10.1109/JSYST.2015.2466439
7. Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd annual Hawaii international conference on system sciences (pp. 10-pp). IEEE.
8. Abdullah, D. (2024). Leveraging FPGA-based design for high-performance embedded computing. SCCTS Journal of Embedded Systems Design and Applications, 1(1), 37-42. https://doi.org/10.31838/ESA/01.01.07
9. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095
10. Cheng, L. W., & Wei, B. L. (2024). Transforming smart devices and networks using blockchain for IoT. Progress in Electronics and Communication Engineering, 2(1), 60–67. https://doi.org/10.31838/PECE/02.01.06
11. Mahalle, P. N., Babar, S. D., & Prasad, N. R. (2013). Identity management framework towards internet of things (IoT): Roadmap and key challenges. Communications in Computer and Information Science, 312, 430–439. https://doi.org/10.1007/978-3-642-37985-9_47
12. El-Saadawi, E., Abohamama, A. S., & Alrahmawy, M. F. (2024). IoT-based optimal energy management in smart homes using harmony search optimization technique. International Journal of Communication and Computer Technologies, 12(1), 1-20. https://doi.org/10.31838/IJCCTS/12.01.01
13. Xu, X., & Lu, W. (2024). Digital Preservation and Network Security Protection: A Case Study of Landscape Painting in Ming Dynasty. Journal of Internet Services and Information Security, 14(4), 249-262. https://doi.org/10.58346/JISIS.2024.I4.015
14. Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2020). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 20(2), 357. https://doi.org/10.3390/s20020357
15. Sahu, B. K., & Khan, M. N. (2024). Current Trends and Future Path Analysis of Coral Reef Restoration: A Systematic Review and Analysis. Aquatic Ecosystems and Environmental Frontiers, 2(3), 10-15.
16. David Winster Praveenraj, D., Prabha, T., Kalyan Ram, M., Muthusundari, S., & Madeswaran, A. (2024). Management and Sales Forecasting of an E-commerce Information System Using Data Mining and Convolutional Neural Networks. Indian Journal of Information Sources and Services, 14(2), 139–145. https://doi.org/10.51983/ijiss-2024.14.2.20
17. Chen, M., Ma, Y., Li, Y., Wu, D., Zhang, Y., & Youn, C. H. (2020). Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems. IEEE Communications Magazine, 58(1), 74–81. https://doi.org/10.1109/MCOM.001.1900310
18. Upadhyay, N., Rana, N. S., Hooda, R. C., & Desai, T. (2024). Evaluating the effectiveness of eco-labeling schemes in promoting sustainable fishing practices. International Journal of Aquatic Research and Environmental Studies, 4(S1), 113-118. https://doi.org/10.70102/IJARES/V4S1/19
19. Wood, A., & Stankovic, J. A. (2003). Design of an embedded medical monitoring system. In Proceedings of the Sixth International Conference on Embedded Software (pp. 189–202). Springer.
20. Martinez, R., & Garcia, C. (2024). Integrated Systems Design: A Holistic Approach to Mechanical Engineering. Association Journal of Interdisciplinary Technics in Engineering Mechanics, 2(4), 12-16.
21. Bianchi, G. F. (2025). Smart sensors for biomedical applications: Design and testing using VLSI technologies. Journal of Integrated VLSI, Embedded and Computing

Technologies, 2(1), 53–61. https://doi.org/10.31838/JIVCT/02.01.07

22. Uvarajan, K. P., & Usha, K. (2024). Implement a system for crop selection and yield prediction using random forest algorithm. International Journal of Communication and Computer Technologies, 12(1), 21-26. https://doi.org/10.31838/IJCCTS/12.01.02
23. Anandhi, S., Rajendrakumar, R., Padmapriya, T., Manikanthan, S. V., Jebanazer, J. J., & Rajasekhar, J. (2024). Implementation of VLSI Systems Incorporating Advanced Cryptography Model for FPGA-IoT Application. Journal of VLSI Circuits and Systems, 6(2), 107–114. https://doi.org/10.31838/jvcs/06.02.12
24. Zor, A., & Rahman, A. (2025). Nanomaterials for water purification towards global water crisis sustainable solutions. Innovative Reviews in Engineering and Science, 3(2), 13–22. https://doi.org/10.31838/INES/03.02.02
25. Frincke, G., & Wang, X. (2025). Hardware/software co-design advances for optimizing resource allocation in reconfigurable systems. SCCTS Transactions on Reconfigurable Computing, 2(2), 15–24. https://doi.org/10.31838/RCC/02.02.03