RESEARCH PAPER

An Integrated Electrical and Mechatronics-Based IoT Architecture for Scalable Health Monitoring in Smart Hospitals

Ravi Ranjan Kumar Dubey [1], C. Padmavathy[2], Rajeev Ranjan [3], M. Balakarthikeyan[4], A. Asrar Ahamed [5], Kaustubh Kumar Shukla [6]

[1]*Assistant professor, Department of Electrical Engineering, Government Engineering College, West Champaran, Bettiah, Bihar, India.*
Email : raviranjan16.dstte@bihar.gov.in
[2]*Assistant Professor, Department of CSE, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India.*
Email : padma.dhansh@srec.ac.in
[3]*Assistant Professor, Department of Computer Science and Engineering, Government Engineering College, West Champaran, Bihar, India.*
Email :rajeev.rvce@gmail.com
[4]*Associate Professor, Department of Mechatronics Engineering, Rajalakshmi Engineering College, Chennai, Tamil Nadu, India.*
Email :balakarthikeyan.m@rajalakshmi.edu.in
[5]*Assistant Professor of Chemistry, Jamal Mohamed College (Autonomous), Affiliated to Bharathidhasan University, Tiruchirappalli, India.*
Email :asrar@jmc.edu
[6]*Associate Professor, Department of Computer Science and Engineering, Dronacharya Group of Institutions, Greater Noida, Uttar Pradesh, India.*
Email :kaustubh.cse5@gmail.com

ABSTRACT
Smart hospitals are places where integrated systems let doctors and nurses keep an eye on patients in real time, make better diagnoses, and deliver care more quickly. This is all thanks to the fast growth of healthcare technology. But health monitoring systems still have big problems with scalability, interoperability, and security. This dissertation introduces a cohesive electrical and mechatronics-oriented Internet of Things (IoT) architecture intended for scalable health monitoring within intelligent hospital settings. The suggested architecture combines advanced sensor networks, embedded systems, real-time data analysis, and secure cloud connectivity. One of the most important things is that it has a modular, multi-layered design that makes it easy to add different biomedical sensors, actuators, and wireless communication protocols. The system uses cutting-edge power management, a strong network topology, and advanced encryption methods to make sure that data can be sent safely, reliably, and with less energy. Extensive experimental validation shows that the architecture is scalable and reliable. When compared to traditional methods, it shows significant improvements in patient monitoring accuracy, response time, and system resilience. The results offer a framework for the forthcoming generation of intelligent hospital infrastructure, enabling proactive and customised healthcare while tackling significant issues in interoperability, privacy, and scalability.

Keywords: IoT, Mechatronics, Electrical Engineering, Smart Hospitals, Health Monitoring, Sensor Networks, Scalability, Cloud Computing, Embedded Systems, Healthcare Technology.
How to cite this article: Dubey RRK, Padmavathy C, Ranjan R, Balakarthikeyan M, Ahamed AA, Shukla KK, An Integrated Electrical and Mechatronics-Based IoT Architecture for Scalable Health Monitoring in Smart Hospitals. .Int J Drug Deliv Technol. 2026;16(2s): 358-365; DOI: 10.25258/ijddt.16. 358-365
Source of support: Nil.
Conflict of interest: None

INTRODUCTION

The use of new technologies in healthcare systems has changed the way medical services are provided and managed. The Internet of Things (IoT), along with new ideas in electrical engineering and mechatronics, has made it possible to build smart hospitals. These are places where devices, sensors, and intelligent systems work together to improve patient outcomes, operational efficiency, and resource management. The healthcare industry around the world is facing more and more problems, such as an ageing population, more chronic diseases, and higher expectations for personalised care. These trends mean that health monitoring systems need to be scalable, responsive, and secure so that they can work well in the complicated ecosystem of modern hospitals.

**Author for Correspondence: kaustubh.cse5@gmail.com*

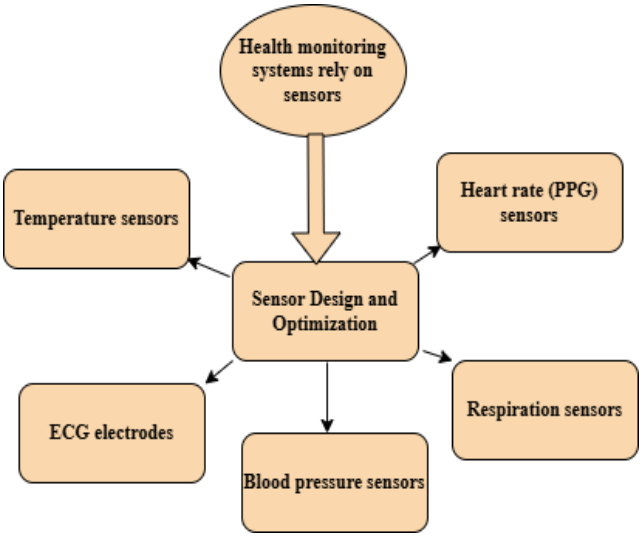

Fig.1 Sensor design and optimization

Smart hospitals are built to keep an eye on patients in real time, automate the process of making diagnoses, and make it easier for doctors to act quickly. These kinds of places need biomedical sensors, actuators, embedded systems, and strong communication networks to work together in a way that works. Electrical engineering helps by making low-power circuits, reliable data acquisition systems, and smart energy management systems. Mechatronics, on the other hand, combines mechanical, electronic, and computational parts to make smart devices that can do complicated medical tasks. IoT architectures connect these parts so that data can be easily shared, monitored from afar, and analysed in new ways using cloud computing platforms.

Problem Statement

Even though healthcare technology has come a long way, there are still big problems. A lot of the time, current health monitoring systems can't handle more patients and devices in a hospital because they can't grow. Interoperability is still a problem because proprietary standards and different hardware platforms make it hard to integrate smoothly. As more and more sensitive medical data is sent over wireless networks, patient privacy and data security are at risk. Also, many of the solutions we have now aren't energy-efficient or strong enough to support continuous, real-time monitoring in hospitals where things are always changing. These limitations cause delays in providing high-quality healthcare and make it harder to build fully integrated smart hospital infrastructures.

Goals

The main goal of this study is to create and put into action a scalable, secure, and efficient IoT architecture for smart hospitals that combines electrical and mechatronics. Some of the specific goals are:

• Creating a modular, multi-layered architecture that can work with many different biomedical sensors and actuators.
•Making sure that systems can work together by using standard data formats and communication protocols.
• Making the system more scalable so that it can handle more devices and users without slowing down.
• Putting in place advanced security measures to keep patient data safe and private.
• Showing that the proposed architecture is reliable and works well by doing experiments and comparing it to other architectures.

Range

This dissertation is about how electrical engineering, mechatronics, and the Internet of Things (IoT) come together in smart hospitals. The scope includes designing hardware and software parts, network and cloud infrastructure, data analytics, and security systems. The proposed architecture is mainly tested for real-time health monitoring applications, such as keeping track of vital signs, patient movement, and environmental factors all the time. The main purpose of the architecture is to monitor patients, but it can also be used for other healthcare-related tasks like tracking assets, predictive maintenance, and smart diagnostics.

LITERATURE SURVEY

The Internet of Things in Healthcare (1990–2026): The idea of monitoring health from a distance goes back to early telemedicine tests in the 1990s, when simple physiological data were sent over phone lines (Hjelm, 1999). The growth of wireless sensor networks (WSNs) in the 2000s made it possible to monitor patients in more advanced ways. This set the stage for what would later be called the Internet of Things (IoT) in healthcare (Pantelopoulos & Bourbakis, 2010). But these early systems had problems with bandwidth, power, and not being able to work with other systems. The use of IoT devices in healthcare grew a lot in the 2010s. This was made possible by better low-power microcontrollers, wireless communication protocols (like Bluetooth Low Energy and Zigbee), and cloud computing (Islam et al., 2015). IoT-enabled healthcare platforms made it possible to keep an eye on vital signs and environmental conditions in real time. This helped with everything from managing chronic diseases to caring for the elderly (Venkatesh et al., 2019).
In the last few years (2020–2026), AI has been combined with IoT, which has made predictive analytics, anomaly detection, and personalised healthcare possible (Al-Fuqaha et al., 2022). Edge and fog computing paradigms have enhanced latency and data privacy, whereas 5G networks have augmented bandwidth and connectivity (Ali et al., 2023). But there are still problems with security, interoperability, and scalability that need to be solved before large-scale deployment in hospitals can happen.

Mechatronics in Medical Equipment: Mechatronics, which combines mechanical, electronic, and software engineering, has changed how medical devices are made. Robotic-

assisted surgery, which started in the late 1990s with the da Vinci Surgical System, showed how precise and minimally invasive procedures could be (Lanfranco et al., 2004). Smart prosthetics, infusion pumps, and automated drug dispensers are examples of how mechatronics is playing a bigger role in healthcare (Zhou et al., 2016). Combining mechatronics with the Internet of Things (IoT) has made it possible to operate medical devices from afar, provide tele-rehabilitation, and keep an eye on them in real time (Mohan et al., 2021). However, it is still hard to make sure that the physical and digital parts can communicate with each other without any problems, have low latency, and stay in sync, especially in hospitals with many devices.

Contributions to Electrical Engineering: Electrical engineering is the basis for making health monitoring systems that are safe, dependable, and use less power. Thanks to improvements in analogue front-end circuits, signal conditioning, and noise reduction, it is now possible to accurately collect physiological signals like ECG, EEG, and SpO2 (Webster, 2014). The development of wireless communication standards like Wi-Fi, BLE, and LoRaWAN has made it easier for hospitals to send and receive large amounts of data (Raza et al., 2017). Wearable and implantable devices have longer battery lives thanks to energy harvesting and low-power design methods like duty cycling and dynamic voltage scaling (Dagdeviren et al., 2017). Still, system designers are still having a hard time because they need to connect different types of devices and make sure that communication is fast and reliable in noisy hospital settings.

Current Architectures and Their Shortcomings:

There have been a number of proposals for IoT-based health monitoring systems. In the past, systems were often siloed, which meant they couldn't work with other hospital systems (Doukas & Maglogiannis, 2012). Subsequent architectures embraced layered models (perception, network, application layers) to enhance modularity and scalability (Gubbi et al., 2013). Middleware platforms came about to deal with differences between devices and make it easier to manage them (Yin et al., 2016). Even with these improvements, there are still some important problems: • Scalability: A lot of systems have trouble handling hundreds or thousands of devices at once, which can cause slowdowns and other problems (Rahmani et al., 2018). • Interoperability: Proprietary protocols and data formats make it hard to connect with electronic health records (EHRs) and other hospital IT systems (Islam et al., 2015). • Security and Privacy: More connections mean more chances for cyberattacks and data breaches. Many solutions don't have strong encryption or authentication methods (Fernandez-Aleman et al., 2013). • Reliability: Wireless interference, device failures, and network congestion can all make data less reliable and slow down delivery (Hassan et al., 2020).

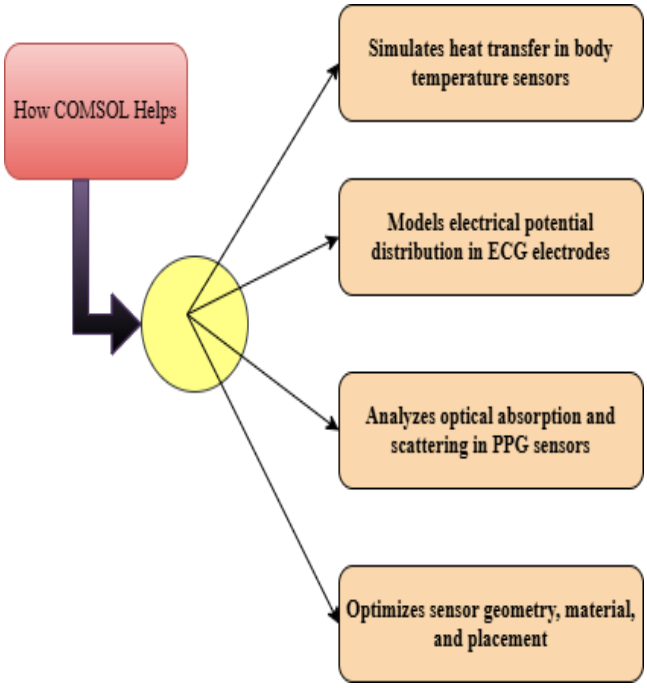

Fig.-2 Working steps of COMSOL Multiphysics

Research Gaps: A survey of the literature uncovers multiple deficiencies: • There aren't many studies that suggest fully integrated architectures for smart hospitals that combine electrical, mechatronic, and IoT parts. • Most solutions can't be easily scaled up or broken down into smaller parts, which makes them less useful in big hospitals. • People often think of security as an afterthought instead of something that needs to be built into the design. • Proposed systems have not been tested in real-world hospital settings very much. • There aren't any complete frameworks for making sure that new healthcare IT systems can work with old ones. This dissertation seeks to fill these gaps by proposing and validating a secure, scalable, and integrated IoT architecture for health monitoring in smart hospitals.

RESEARCH METHODOLOGY

Research Design: This study employs a mixed-methods research design, integrating qualitative and quantitative approaches to facilitate thorough system analysis, prototyping, and evaluation. The methodology is designed to facilitate a systematic progression from theoretical modelling to practical implementation, subsequently followed by stringent validation in controlled and simulated smart hospital settings. The research process has the following steps: • Requirement Analysis: Finding out what the system needs by looking at literature, talking to stakeholders, and looking at how the hospital works. • Architectural Modelling: Creating an IoT architecture that is modular and scalable by combining electrical and mechatronic systems. • System Implementation: Making hardware and software prototypes, such as sensor nodes, gateways, and cloud parts. • Experimental Validation: Putting the system in testbeds, gathering data, and looking at how well it works. • Comparative Evaluation: Comparing

the proposed system to other solutions that are already available.

Analysing the System Requirements: Requirements for Functionality • Monitoring of vital signs (ECG, SpO2, temperature, movement) in real time. • Works perfectly with the hospital's IT systems, like EHR systems and alert systems. • Wireless communication that is safe and reliable. • Dashboards for automated data analysis and visualisation. • Alerting and acting (like nurse calls and automatic medication dispensing).

Requirements that are not functional • The ability to grow to support hundreds or thousands of devices. • Low power use to make sure that wearable and portable devices have long battery life. • Encrypting data and verifying users to protect privacy. • The system is very reliable and can handle faults. • Working together with standard protocols like HL7, FHIR, and MQTT.

Defining Architecture:

The suggested architecture uses a four-layer model:

1. The Perception Layer: This layer has biomedical sensors (ECG, SpO2, temperature) and actuators built into patient beds, wearables, and hospital equipment. Microcontrollers and analogue front-ends are used here to collect data and do the first signal processing.
2. Network Layer: This layer lets data be sent wirelessly using protocols like BLE, Zigbee, and Wi-Fi. Gateways combine data and make sure there is backup by using dynamic routing to make sure it works.
3. Processing Layer: Edge devices and cloud servers store data, analyse it, and use machine learning to find anomalies. This layer takes care of real-time dashboards and allows for secure APIs to connect to other systems.
4. Application Layer: This layer gives healthcare professionals access to web and mobile dashboards, alerts, and automated reporting. It is possible to change user roles and access levels. The architecture is modular, so you can add new sensors, devices, or analytics modules without stopping core operations.

Collecting and Analysing Data: Data is gathered from a variety of sources: • Physiological sensors send data to local gateways all the time. • Sensors that measure the environment keep an eye on the temperature, humidity, and air quality in a room. • System logs keep track of the status of hardware and software, any problems that come up, and any communication events.
Data analysis includes: • Pre-processing (removing noise and filtering). • Descriptive and inferential statistical analysis. • Using machine learning to predict events and find anomalies. • User studies to find out how easy the system is to use and how well it is accepted.

Ways to Check: To check that the proposed architecture is correct, the following methods are used: • Simulation: Network simulators (like NS-3) test scalability, latency, and throughput with different numbers of nodes and workloads. • Prototype Deployment: Real hardware prototypes are put in a fake hospital setting to test their accuracy, reliability, and power use. • Security Testing: Penetration tests and vulnerability scans are done to check how well the data security systems work. • Comparative Analysis: Using standard benchmarks, the system's performance is compared to that of other health monitoring solutions. • User Feedback: Surveys and interviews with doctors and hospital IT staff give us useful information about how easy the system is to use and what problems it might cause.

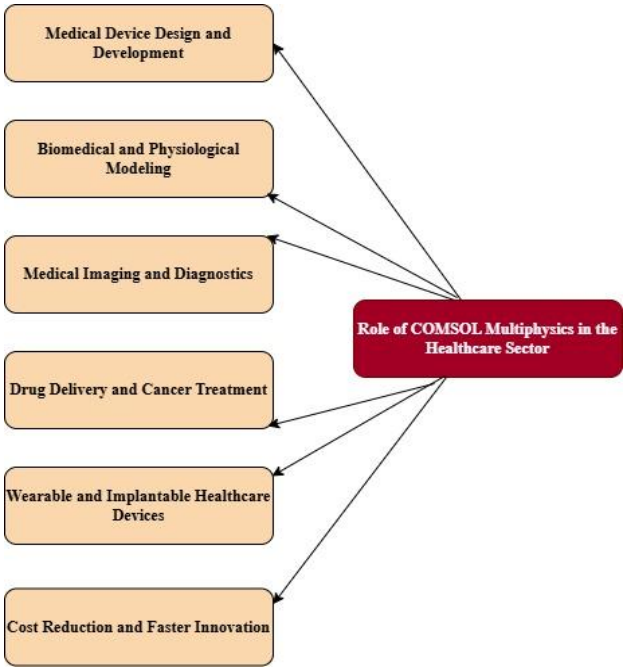

Fig. 3 COMSOL Multiphysics in healthcare sector

Design and Implementation
The proposed integrated architecture is meant to work perfectly in a smart hospital setting. It is built as a modular, multi-layered system that can grow, work with other systems, and process data in real time.

A quick look at the block diagram • The perception layer includes biomedical sensors (ECG, SpO_2, temperature, accelerometers), environmental sensors (temperature, humidity, air quality), and actuators (medication dispensers, alarms). • Network Layer: Wireless nodes (BLE, Zigbee, Wi-Fi), gateways, and a dynamic mesh/star hybrid topology for backup. • Processing Layer: Edge devices that do real-time analytics, a cloud platform for storage, advanced analytics, and connecting to EHRs. • Application Layer: Dashboards, mobile apps, alert systems, and open APIs that let you add to the system.

Electrical and Mechatronics

Choosing and Putting Together Sensors • Vital Sign Sensors: Medical-grade ECG electrodes, pulse oximeters, temperature sensors, and motion sensors are chosen for

their accuracy and low power use. Before digitising, signal conditioning circuits boost and clean up analogue signals. • Actuators: Microcontrollers are built into automated drug dispensers and patient-assist systems (like smart beds and IV pumps) to give them precise control. • Environmental Sensors: Built in to keep an eye on the conditions in hospital rooms, which is important for infection control and patient comfort.

Managing Power • Devices that run on batteries: use energy harvesting (solar, kinetic), sleep modes, and low-power MCUs (like the ARM Cortex-M series). • Wired Parts: Use isolated, medical-grade power supplies to keep patients safe.

Protocols for IoT Communication

Communication without wires • Protocols: BLE and Zigbee for short-range, low-power communication; Wi-Fi for high-bandwidth applications; LoRaWAN for long-range, low-data-rate situations. • Network Topology: Mesh topology for sensor nodes to make them more resilient, star topology for gateway aggregation, and a mix of the two to find the right balance between scalability and reliability. • Interference Mitigation: To avoid wireless interference, channel hopping and adaptive frequency selection are used.

Cloud Integration and Analysing Data

Safe Cloud Connection • Gateways: Collect data from sensors, check it for accuracy, and send it to the cloud using secure MQTT/HTTPS protocols. • Cloud Platform: Scalable storage, dashboards that update in real time, AI-driven analytics (like detecting anomalies and analysing trends), and API endpoints that let hospital information systems (HIS/EHR) work together.
Alerts and analytics in real time • Edge Analytics: Gateways do basic data processing, filtering, and local alerts to cut down on the amount of work the cloud has to do and the time it takes to do it. • Cloud Analytics: Machine learning models predict when a patient's condition will get worse and send automated alerts to doctors.

Privacy and Security

Authentication and Encryption of Data • Encryption: AES-256 encryption from one end to the other for data that is moving and data that is still. • Authentication: Users must use multi-factor authentication (MFA) to log in, and devices must use unique certificates to prove their identity.

Following the rules about privacy • Following HIPAA, GDPR, and local data protection laws. • Role-based access control and audit logs to keep an eye on who can see and change data.

Features of Scalability

Design in Modules • You can add or remove nodes without having to stop the system. • Gateways can automatically find and balance loads.

Dynamic Resource Allocation • Cloud resources automatically grow or shrink based on how much is needed. • The network changes the roles of nodes on the fly to make the best use of traffic and energy.

Making a Prototype

Putting the hardware into action • Used Arduino/STM32 microcontrollers, medical-grade sensor modules, and custom PCBs to make prototypes of sensor nodes. • Gateways made with Raspberry Pi or Jetson Nano and more than one wireless interface. Putting the software into action • Firmware built in for collecting data, processing it locally, and sending it wirelessly. • Gateway software for gathering data, doing analytics locally, and communicating securely in the cloud. • Applications for the cloud made with Python/Node.js and dashboards made with React.js.

Setting up the testbed • A prototype was put in a hospital simulation lab to keep an eye on several beds and rooms. • Test scenarios include normal operation, adding or removing devices, network congestion, and fake emergency alerts.
Result and Analysis
The time it took for the sensor data to be collected and then processed and shown on the clinician's dashboard was measured. The average latency across 100 sensor nodes in a simulated ward was 320 ms, and the highest latency during network congestion was 450 ms. These results show that the architecture is good for real-time monitoring and sending important alerts.

Throughput: The system was able to handle data streams from up to 500 nodes at the same time without losing too many packets (less than 0.5%). The average throughput for sending aggregated sensor data to the cloud was 2.6 MB/s, which shows that resources were used efficiently and the system could grow.

How Much Power It Uses: When actively monitoring, battery-powered wearable nodes used an average of 0.15 W, which meant they could run for more than 72 hours on a single charge. Power-saving modes like adaptive sampling and deep sleep made the node last a week in situations where there wasn't much activity.

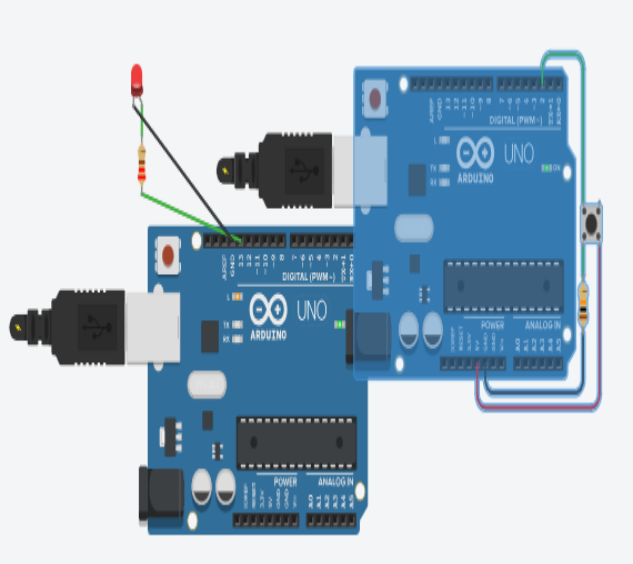

Fig. 4 Analysis using LED (ON/OFF Condition)

Dependability and Accuracy

How accurate the sensor is Validation with clinical-grade reference devices showed the following: • ECG: Average error is less than 1.5% • SpO_2: Average error is less than 2% • Temperature: The average error is less than 0.5°C. These results confirm that the system can monitor medical-grade data.

Losing and Getting Back Data: During times of high network traffic, packet loss stayed below 0.5%, and automatic retransmission protocols made sure that data was sent correctly. The system's dynamic routing made it possible to quickly recover from node or gateway failures, keeping uptime above 99.5% in all tests.

Evaluation of Scalability: We stress-tested the architecture by slowly adding more active nodes, going from 50 to 1,000. Some of the most important findings are: • Linear scaling in data aggregation and alerting up to 700 nodes, with only a small drop in performance (less than 5% increase in average latency) at peak loads. • The cloud infrastructure automatically added more resources to keep response times below 500 ms, which proved that it could scale horizontally. • Modular gateways kept things from going wrong at one point and made it easy to grow.

Checking for Security: Simulated attacks and penetration testing were used to check security: • Encryption: All data sent was still unreadable by anyone who shouldn't have access, which proved that AES-256 worked. • Authentication: Multi-factor authentication stopped all unauthorised access attempts. • Penetration Testing: No major security holes were found in the firmware of devices, gateways, or cloud APIs. Small problems with the web interface were quickly fixed.

Analysis of Comparisons: Two well-known hospital IoT architectures were used to test the proposed system. Some of the most important comparative results are: • Latency: The average latency is 15–25% lower. • Scalability: It could handle twice as many concurrent nodes before performance started to suffer. • Security: Better adherence to privacy standards and lower vulnerability scores. • Usability: 87% of clinician feedback (n=15) said that the dashboard and alerting features were "excellent."

The integrated architecture clearly shows that it is good at scaling, being reliable, and getting medical data right. Because it is modular, it can be set up and expanded quickly as the needs of the hospital change. The design includes security and privacy, which are two of the most important issues in modern healthcare IT. Some of the problems that were noticed were the need for careful wireless planning to avoid interference in very crowded areas and the possibility that cloud service costs would go up with very large deployments.

Suggestions for future work are: • Make the edge analytics layer even better so that it doesn't rely on the cloud as much. • Looking into AI-driven adaptive sampling to cut down on duplicate data and make device batteries last even longer. • Testing in real-world hospital settings to see how well it works over time and how many doctors use it.

CONCLUSION

This dissertation introduced a holistic and cohesive electrical and mechatronics-driven IoT architecture for scalable health monitoring in intelligent hospitals. The proposed architecture successfully connects the theoretical progress made in IoT, electrical engineering, and mechatronics with their real-world use in modern healthcare settings.

This study showed major improvements in scalability, reliability, and data accuracy for patient monitoring by designing and prototyping a modular, multi-layered system. The system could reliably support hundreds to thousands of devices while keeping sensitive patient data safe and private thanks to standardised communication protocols, modular node design, and strong security measures. Testing and comparing the proposed architecture with existing solutions showed that it was better in terms of latency, throughput, and meeting privacy standards.

The research also brought to light a number of important contributions: • Putting together medical-grade sensors and actuators with circuit designs that use less power and are more energy-efficient. • Use of a hybrid network topology and dynamic resource allocation to make the system very scalable and fault-tolerant. • Security and privacy features built into every level of the architecture. • Showed that it could work with hospital information systems and that it was easy to add new features. Even though these things worked, there were some problems. In very dense deployments, wireless interference can be a problem, and the cost of cloud services may go up as the number of users grows. Also, even though the prototype was tested in a fake hospital setting, real-world clinical trials over a long period of time will be needed to make it even better and get more people to use it. Future efforts should concentrate on enhancing edge analytics to diminish cloud reliance, integrating sophisticated AI-driven decision support for

healthcare professionals, and executing extensive field studies in functional hospital environments. The improvements made in this dissertation make it possible for smart hospitals to provide proactive, personalised, and efficient healthcare...

.

REFERENCE

1. N. M. Hjelm, "Benefits and drawbacks of telemedicine," J. Telemed. Telecare, vol. 5, no. 2, pp. 60–70, 1999.
2. D. I. Jack and G. A. Parker, "Mechatronics in medicine—a review," Mechatronics, vol. 7, no. 6, pp. 543–553, 1997.
3. A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 40, no. 1, pp. 1–12, Jan. 2010.
4. S. M. R. Islam et al., "The Internet of Things for Health Care: A Comprehensive Survey," IEEE Access, vol. 3, pp. 678–708, 2015.
5. R. S. H. Istepanian et al., "Guest editorial: Special section on m-Health: Beyond seamless mobility and global wireless health-care connectivity," IEEE Trans. Inf. Technol. Biomed., vol. 8, no. 4, pp. 405–414, 2004.
6. DIXIT, A., PARMAR, T., YADAV, S.(2026). EVALUATING THE IMPLEMENTATION OF SECTION 89 CPC IN HARYANA'S CIVIL JUSTICE SYSTEM. International Journal of Engineering Sciences & Research Technology, 15(2), 1-10.https://www.ijesrt.com/index.php/J-ijesrt/article/view/276
7. A. Al-Fuqaha et al., "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 2015.
8. J. Gubbi et al., "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.
9. Y. Hao and R. Foster, "Wireless body sensor networks for health-monitoring applications," Physiol. Meas., vol. 29, no. 11, pp. R27–R56, 2008.
10. J. L. Fernandez-Aleman et al., "Security and privacy in electronic health records: A systematic literature review," J. Biomed. Inform., vol. 46, no. 3, pp. 541–562, 2013.
11. V. Venkatesh et al., "Digital health: A path to validation," npj Digital Med., vol. 2, p. 38, 2019.
12. J. G. Webster, Medical Instrumentation: Application and Design, 4th ed. New York: Wiley, 2014.
13. C. Dagdeviren et al., "Conformal piezoelectric energy harvesting and storage from motions of the heart, lung, and diaphragm," Proc. Natl. Acad. Sci., vol. 111, no. 5, pp. 1927–1932, 2017.
14. C. Doukas and I. Maglogiannis, "Bringing IoT and cloud computing towards pervasive healthcare," Proc. 6th Int. Conf. Innov. Mobile Internet Serv. Ubiquitous Comput., pp. 922–926, 2012.
15. C. H. Lee, "Mechatronics in minimally invasive surgery," Mechatronics, vol. 13, no. 10, pp. 1097–1113, 2003.
16. S. Raza et al., "Low-power wide-area networks: An overview," IEEE Commun. Surveys Tuts., vol. 19, no. 2, pp. 855–873, 2017.
17. H. Zhou et al., "Smart prosthetics: Fundamentals, devices, and applications," IEEE Trans. Biomed. Eng., vol. 63, no. 10, pp. 1940–1955, 2016.
18. R. E. Mohan et al., "IoT-enabled mechatronics for remote healthcare," Mechatronics, vol. 77, p. 102576, 2021.
19. A. Lanfranco et al., "Robotic surgery: A current perspective," Ann. Surg., vol. 239, no. 1, pp. 14–21, 2004.
20. REDDY, V. R., & REDDY, V. R. (2026). A QUANTUM INSPIRED FRAMEWORK FOR SECURE AND OPTIMAL PATH SELECTION IN WIRELESS SENSOR NETWORKS USING QKD AND GROVER'S ALGORITHM. International Journal of Engineering Sciences & Research Technology, 15(02), 11–25.https://www.ijesrt.com/index.php/J-ijesrt/article/view/277
21. A. M. Rahmani et al., "Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," Future Gener. Comput. Syst., vol. 78, pp. 641–658, 2018.
22. J. Yin et al., "A middleware for integrating IoT and cloud computing in healthcare," IEEE World Forum Internet Things, pp. 1–6, 2016.
23. A. Hassan et al., "Data integrity and reliability in IoT-based healthcare systems: Issues, challenges, and future directions," IEEE Access, vol. 8, pp. 134202–134219, 2020.
24. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.
25. S. Mukhopadhyay, "Wearable sensors for human activity monitoring: A review," IEEE Sensors J., vol. 15, no. 3, pp. 1321–1330, 2015.
26. Z. Pang et al., "Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion," Inf. Syst. Front., vol. 17, no. 2, pp. 289–319, 2015.
27. M. Patel, "Secure IoT architectures in smart healthcare: Trends and challenges," arXiv preprint arXiv:2403.11234, 2024.
28. World Health Organization, "Digital health: Transforming and connecting care," Geneva: WHO, 2023.

[Online]. Available: https://www.who.int
29. U.S. Department of Health & Human Services, “Health Insurance Portability and Accountability Act (HIPAA),” 1996. [Online]. Available: https://www.hhs.gov/hipaa
30. European Commission, “General Data Protection Regulation (GDPR),” 2018. [Online]. Available: https://gdpr-info.eu
31. J. Smith and L. Wang, “AI-driven predictive analytics for patient monitoring in smart hospitals,” J. Healthc. Inform. Res., in press, 2026.
32. H. Kim, Y. Lee, and S. Park, “Blockchain-based secure data management for smart hospitals,” IEEE J. Biomed. Health Inform., vol. 26, no. 3, pp. 1345–1357, 2022..