Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/21862
DOI URL: http://dx.doi.org/10.21474/IJAR01/21862

RESEARCH ARTICLE

A SECURE AND SCALABLEFRAMEWORK FOR EMBEDDED SYSTEMS BASED MEDICAL DEVICES

Akshat Bhutiani

Manuscript Info

Manuscript History
Received: 19 July 2025
Final Accepted: 21 August 2025
Published: September 2025

Key words:-
Embedded Systems, Healthcare, IT Systems Integration, Frameworks

Abstract

Embedded systems such as radiology machines, smart thermometers etc. are widely used in hospitals and health centers. These devices collect a large amount of patient data. However, several issues persist around security of the data and integration with other IT systems in the hospitals. This paper proposes a theoretical framework that outlines a layered approach for using secured and scalable healthcare devices. The main focus is on lightweight encryption mechanisms, handling of real-time patient data and integration with other IT systems.

Introduction:-

Embedded systems are small devices that consist of resource constrained hardware and real-time software. This software can either be run directly on the hardware or on an operating system. Embedded Systems have now become integral to medical devices as they can be used easily in collecting patient data. These systems can range from highly complex medical imaging devices all the way down to the simplest of thermometers. The data that these devices collect, can then be transferred to the IT department of a hospital for analysis and decision making by healthcare professionals. It has been observed that the increasing use of embedded systems is associated with reduced hospitalization costs and improved patient outcomes (Pantepolous&Bourbakis, 2010).

However, the deployment of embedded systems within into healthcare devices has raised some questions, particularly relating to security and interoperability. Since embedded systems based medical devices collect a lot of patient data, it is required that they maintain compliance with data privacy standards such as HIPA and GDPR (Mosenia& Jha, 2017). As embedded systems are severely constrained in their hardware and software capabilities, it is difficult to implement standard security protocols on them. Thus, these systems are vulnerable to threats like data interception, unauthorized access etc.

This paper introduces a framework for design and development of secure embedded systems for healthcare monitoring. The proposed framework has 4 layers – embedded sensors layer, secure communication layer, analytics layer and cloud integration layer. This framework aims to establish robust and compliant embedded systems-based healthcare monitoring applications thus contributing to safer and efficient healthcare delivery.

Related Work:-

Data captured by embedded medical devices is transmitted to the telemetry systems for analysis and response. Early systems focused on monitoring and measuring vital statistics such as ECG, heart rate, glucose levels etc. While these features enabled measurement of vital statistics outside of the hospital (Pantelopoulos&Bourbakis, 2010), they

Corresponding Author:-Akshat Bhutiani

are limited by single – purpose design and lack security measures. It is also not possible to transmit data from such devices to IT systems of hospitals.

As more devices become integrated with the internet, securing them becomes increasingly essential. Since embedded systems have limited hardware and software capabilities, some custom intrusion detection schemes have been proposed to accommodate these limitations. However, these schemes fall short when it comes to a multi-device, multi-user scenario. Mosenia and Jha (2017) emphasize that embedded medical systems must be resilient to a broad range of threats—ranging from physical tampering to wireless protocol attacks—and require architecture-level design considerations, not just cryptographic add-ons.

IT software systems in hospitals are built around HL7 and FHIR, however most embedded systems lack native support for these formats. There are approaches proposed such as RESTAPI approach (Bender and Sartipi, 2013). While this may work, implementing it in real-time is still an issue. Further, Fernández-Alemán et al. (2013), also point out that effective health care electronic systems require a comprehensive governance framework to ensure privacy, auditability and compliance with regulations. However, this framework did not consider real-time data analysis that could be performed by these devices.

Recently, Ahmed et.al (2020), proposed a smart healthcare monitoring framework for COVID-19 patients using cloud computing and deep learning. This work emphasizes the role of AI – driven diagnostics and telemedicine during the pandemic. However, it relies heavily on cloud infrastructure and offers limited support for embedded processing on the edge. These gaps point to the need for a unified, scalable and secure framework specifically suited to embedded healthcare systems.

TABLE 1 – Comparative Analysis of Frameworks for Embedded Healthcare Systems

Framework / Study	Year	Security Measures	Interoperability	Embedded Systems Focus
Pantelopoulos&Bourbakis	2010	Basic encryption	No	Yes
Bender &Sartipi	2013	Secure RESTful services	Yes (HL7/FHIR)	Partial
Fernández-Alemán et al.	2013	Privacy / trust models	Limited	No
Mosenia& Jha	2017	Lightweight cryptography	No	Yes
Ahmed et. al	2020	Basic cloud level security	No	No
Proposed Framework	2025	Lightweight + role based	Yes (modular FHIR integration)	Yes

Methodology:-

This paper proposes a 4-layer framework for secure embedded healthcare devices. This framework is based on the main principle of distributed information system design. The 4 layers i.e. Sensing layer, Processing layer, Communication layer, and Integration reflect both technical and information flows in a modern healthcare environment. As shown by Chen.et al, 2008, the layered architecture described above is widely used in Information Sciences design. The framework also supports data acquisition from embedded devices while addressing the challenges of security and interoperability.

The sensing layer will have wearable and implantable embedded systems to acquire body measurements such as heart rate, Sp02 and glucose. Sensor operations shall be optimized through techniques such as adaptive sampling and acquisition triggered by certain events. Validation techniques will be used to ensure that the data is consistent before being encrypted for transmission. This step will make sure that data integrity and security are not compromised. While traditional sensing mechanisms capture raw data, this method will filter the raw data and make it more suitable for transmission.

The processing layer acts as the intermediate layer. It collects raw data and provides data analysis for the collected data. It is possible to implement lightweight algorithms on the micro-controllers. Such algorithms can detect anomalies, perform trend analysis and do event classification. By implementing the processing algorithms directly on the embedded medical device, it prevents the need for processing on centralized servers and reduces communication latency. It also helps in events where critical actions need to be taken such as seizures or heart attacks etc (Rajkumar, et.al 2010).

The integration layer sits between the embedded health care devices and the IT system of the hospital. This layer is responsible for ensuring that there is compliance with regulatory frameworks such as HIPAA and GDPR. It also supports role-based authentication and secure audit trails. This layer can also support API services that seek to interact with the healthcare system.

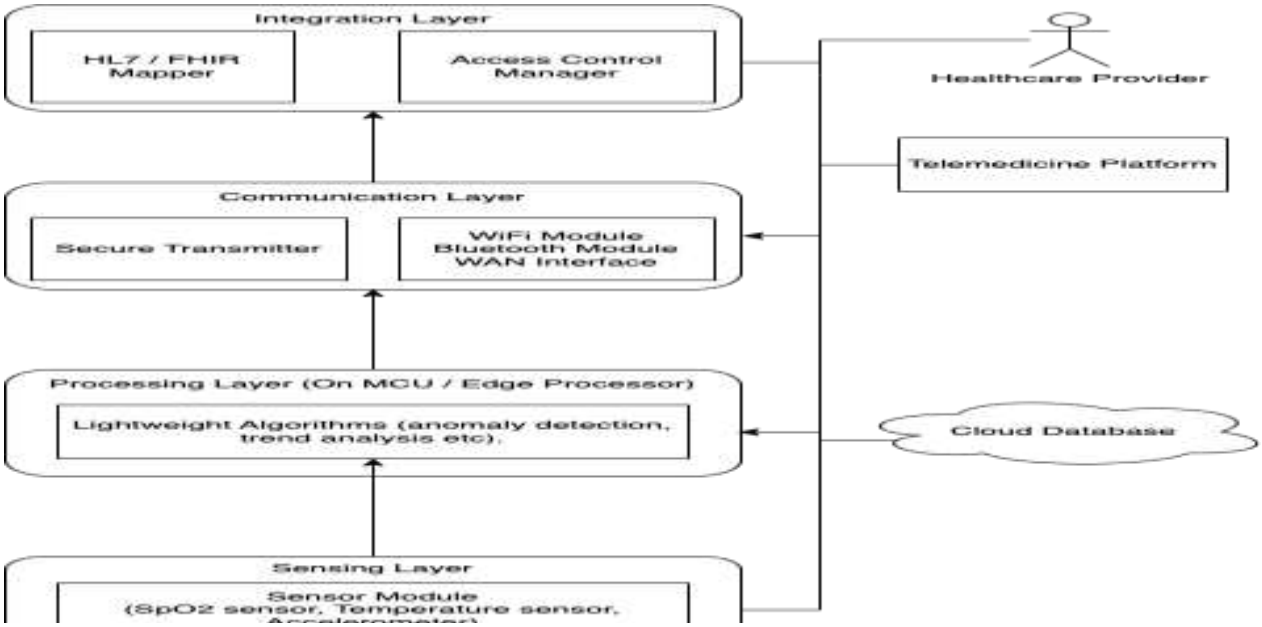

Figure 1 – Architecture of the Proposed Framework

To ensure operability, the proposed framework maps to several key international standards in healthcare informatics. These standards include HL7/FHIR, ISO/IEEE 11073 Service-Oriented Device Connectivity, ISO/IEEE 11073 Personal Health Device and ISO/IEC 80001-1:2021. In the U.S., it is mandatory to use FHIR standard for regulated medical payers since 2021. In the Integration Layer of the proposed framework, the patients' vitals will be encapsulated using FHIR Device, Patient and Observations resources. This enables integration with the enterprise systems of the hospital (HL7 International, 2023).

The ISO/IEEE 11073 Service-Oriented Device Connectivity standard defines a service-oriented architecture for medical device communication (ISO/IEEE, 2020a). The proposed architecture's communication layer will use the standard service profiles and message bindings for communication. The ISO/IEEE 11073-10201:2020 and 11073-10101:2020 contain clearly defined information models for data exchange of vital parameters. This is optimized for constrained devices such as embedded systems. The sensing layer which contains various sensors such SpO2, heart rate etc will be mapped to these models to enable lightweight encoding. This will also enhance the interoperability with the processing and communication layers.

For managing risk to IT networks there is ISO/IEC 80001-1:2021 standard that also covers medical devices. The integration layer in the architecture will use this for compliance focused design.

Evaluation:-

The proposed framework is evaluated using a criteria-based assessment approach. It is evaluated based on its ability to meet requirements from international standards. The criteria are drawn from 80001 (Application of Risk Management for IT Networks Incorporating Medical Devices), HL7 FHIR R4 (Fast Healthcare Interoperability Resources), and IEEE 11073 (Personal Health Device Communication). The evaluation is primarily focused on 5 dimensions – Interoperability, Scalability, Security & Privacy, Standards Compliance and Maintainability.

Dimension	Alignment Level	Justification
Interoperability	Full Alignment	L7 FHIR R4-compliant APIs and IEEE 11073 protocols will be used for communication.
Standards Compliance	Full Alignment	Core design mapped to international standards, with explicit support for risk management and interoperability.
Maintainability	Full Alignment	Layered design with modular components allows isolated upgrades without disrupting the entire system.
Security & Privacy	Partial Alignment	Proposed framework incorporates encryption, authentication and role-based access. However, full alignment requires implementation.
Scalability	Partial Alignment	Modular architecture of the framework supports scaling. However, full alignment requires implementation.

Conclusion:-

The proposed framework for embedded systems based medical devices shows a strong alignment with established standards for interoperability, safety and data protection. The framework of the architecture is divided into processing, integration and communication layers. This ensures that the framework is modular and supports the integration of advanced analytics, real-time data processing and device interoperability. The strong alignment with various established standards shows that the framework is ready to be implemented. Future research in this area will focus on implementing the framework and testing.

References:-

1. Pantelopoulos, A., &Bourbakis, N. G. (2010). A survey on wearable sensor-based systems for health monitoring and prognosis. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 40(1), 1–12.
2. Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of Internet-of-Things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586–602.
3. Bender, D., &Sartipi, K. (2013). HL7 FHIR: An agile and RESTful approach to healthcare information exchange. In 2013 IEEE 26th International Symposium on Computer-Based Medical Systems (pp. 326–331).
4. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3), 541–562.
5. Ahmad, M., Rathore, M. M., Paul, A., & Chang, V. (2020). Smart healthcare monitoring framework for COVID-19 patients using deep learning and cloud computing. Personal and Ubiquitous Computing, 25, 1–17.
6. Chen, D. D., Doumeingts, G., &Vernadat, F. B. (2010). Architectures for enterprise integration and interoperability: Past, present and future. Computers in Industry, 59(7), 647–659.
7. Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). Cyber-physical systems: The next computing revolution. Proceedings of the 47th Design Automation Conference, 731–736.
8. HL7 International. (2023). FHIR Release 4.0.1 specification and U.S. CMS Final Rule on Patient Access via FHIR. HL7.org.
9. ISO/IEEE. (2020a). ISO/IEEE 11073-20701: Health informatics — Point-of-care medical device communication — Service-oriented medical device exchange architecture and protocol binding.
10. ISO/IEC. (2021). ISO/IEC 80001-1: Application of risk management for IT-networks incorporating medical devices — Part 1: Safety, effectiveness and security.