A Secure & Scalable Embedded Systems Framework for Remote Healthcare Monitoring

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

36 sensors layer, secure communication layer, analytics layer and cloud integration layer.
37 This framework aims to establish robust and compliant embedded systems-based
38 healthcare monitoring applications thus contributing to safer and efficient healthcare
39 delivery.

40

41   RELATED WORK

42 Data captured by embedded medical devices is transmitted to the telemetry systems for
43 analysis and response. Early systems focused on monitoring and measuring vital
44 statistics such as ECG, heart rate, glucose levels etc. While these features enabled
45 measurement of vital statistics outside of the hospital (Pantelopoulos&Bourbakis, 2010),
46 they are limited by single – purpose design and lack security measures. It is also not
47 possible to transmit data from such devices to IT systems of hospitals.

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

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

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

70

71

72   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

73

74   METHODOLOGY

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

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

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

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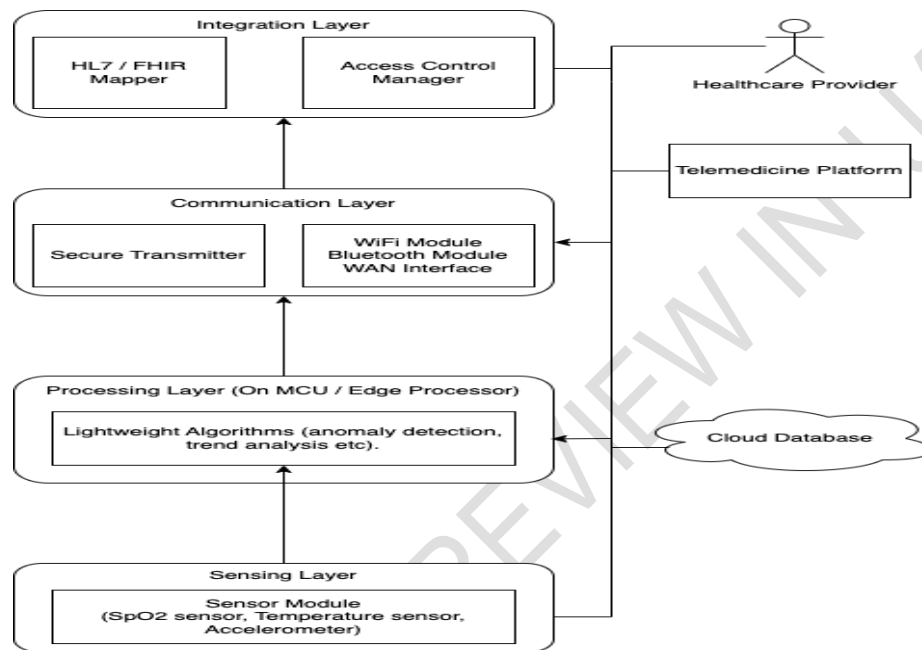100 to interact with the healthcare system.

101

102

103   Figure 1 – Architecture of the Proposed Framework

104

105 To ensure operability, the proposed framework maps to several key international
106 standards in healthcare informatics. These standards include HL7/FHIR, ISO/IEEE
107 11073 Service-Oriented Device Connectivity, ISO/IEEE 11073 Personal Health Device
108 and ISO/IEC 80001-1:2021. In the U.S., it is mandatory to use FHIR standard for
109 regulated medical payers since 2021. In the Integration Layer of the proposed
110 framework, the patients' vitals will be encapsulated using FHIR Device, Patient and
111 Observations resources. This enables integration with the enterprise systems of the
112 hospital (HL7 International, 2023).

113 The ISO/IEEE 11073 Service-Oriented Device Connectivity standard defines a service-
114 oriented architecture for medical device communication (ISO/IEEE, 2020a). The
115 proposed architecture's communication layer will use the standard service profiles and
116 message bindings for communication. The ISO/IEEE 11073-10201:2020 and
117 11073-10101:2020 contain clearly defined information models for data exchange of vital
118 parameters. This is optimized for constrained devices such as embedded systems. The
119 sensing layer which contains various sensors such SpO2, heart rate etc will be mapped

120 to these models to enable lightweight encoding. This will also enhance the
121 interoperability with the processing and communication layers.

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

125

126   EVALUATION

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

134

135

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.

136

CONCLUSION

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

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160 ## REFERENCES

161 1. Pantelopoulos, A., &Bourbakis, N. G. (2010). A survey on wearable sensor-based
162 systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man,*
163 *and Cybernetics, Part C (Applications and Reviews), 40*(1), 1–12.

164   2. Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of Internet-of-
165   Things. *IEEE Transactions on Emerging Topics in Computing, 5*(4), 586–602.

166   3. Bender, D., &Sartipi, K. (2013). HL7 FHIR: An agile and RESTful approach to
167   healthcare information exchange. In *2013 IEEE 26th International Symposium on
168   Computer-Based Medical Systems* (pp. 326–331).

169   4. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security
170   and privacy in electronic health records: A systematic literature review. *Journal of
171   Biomedical Informatics, 46*(3), 541–562.

172   5. Ahmad, M., Rathore, M. M., Paul, A., & Chang, V. (2020). Smart healthcare
173   monitoring framework for COVID-19 patients using deep learning and cloud
174   computing. *Personal and Ubiquitous Computing, 25*, 1–17.

175   6. Chen, D. D., Doumeingts, G., &Vernadat, F. B. (2010). *Architectures for enterprise
176   integration and interoperability: Past, present and future*. Computers in Industry,
177   59(7), 647–659.

178   7. Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). Cyber-physical systems: The
179   next computing revolution. *Proceedings of the 47th Design Automation Conference*,
180   731–736.

181   8. HL7 International. (2023). *FHIR Release 4.0.1 specification* and U.S. CMS Final
182   Rule on Patient Access via FHIR. HL7.org.

183   9. ISO/IEEE. (2020a). *ISO/IEEE 11073-20701: Health informatics — Point-of-care
184   medical device communication — Service-oriented medical device exchange
185   architecture and protocol binding.*

186 10.ISO/IEC. (2021). *ISO/IEC 80001-1: Application of risk management for IT-networks
187   incorporating medical devices — Part 1: Safety, effectiveness and security.*