MBNA Publishing House Constanta 2025

Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

Applied Platform in Defense Missions for Health Monitoring via IoT Devices

To cite this article: V. MARASCU, M. I. MIHAILESCU, S. L. NITA, Proceedings of the International Scientific Conference SEA-CONF 2025, pg. 56-63.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-25-006

Applied Platform in Defense Missions for Health Monitoring via IoT Devices

Valentina Marascu [1,2,*], Marius Iulian Mihailescu[1], Stefania Loredana Nita[3]

[1]Faculty of Engineering and Computer Science, Scientific Research Center in Mathematics and Computer Science, SPIRU HARET University, Bucharest, Romania
[2]National Institute for Laser, Plasma and Radiation Physics, 409 Atomistilor Street, RO-77125, Magurele, Ilfov, Romania
[3]Institute for Computers, Bucharest, Romania
*Corresponding author: valentina.marascu@gmail.com

Abstract. The incorporation of Internet of Things technology in defense operations enhances subsystem management and enables the collection of quantitative scientific data. The primary objective of this paper is to provide an appropriate, applicable platform for monitoring personnel's health using IoT sensors. The proposed platform was developed by using the C# language, and dedicated virtual IoT devices were attached. Moreover, the proposed platform can also be used in low-gravity conditions by tracking specific physiological metrics, such as pulse rate/blood pressure, oxygen saturation, body temperature, and carbon dioxide levels. The security of this platform was assured to maintain the integrity of health personnel data.

Keywords: IoT Devices; C# language; Defense missions; Life-support platforms; Education.

1. Introduction

The Internet of Things (IoT) is a transformative paradigm that is becoming increasingly important in many sectors, including advanced sectors such as healthcare, aerospace, and defense. The device used in future military defense plans and space missions helps in managing complex systems and gathering precise scientific information from harsh surroundings. Unique characteristics of IoT systems, such as autonomous data collection, universal connectivity, resilience to extreme conditions, and real-time monitoring, make IoT systems a fundamental tooling solution for the improvement of situational awareness and operational efficiency in remote or high-risk environments (Prashanthi et al., 2024). Within the context of space exploration, IoT devices are massively employed within spacecraft and outer-space habitats to examine system parameters and crew health variables. In demanding environmental conditions (e.g., microgravity, increased radiation, limited communication bandwidth), these systems must operate independently. However, their critical role makes them vulnerable to cyberattacks, signal jamming, and other forms of physical tampering. Security, privacy, and ethical use of sent data should be part and parcel of successfully performing such operations. Securing IoT devices requires advanced encryption protocols, secure boot procedures, and a Zero Trust framework, as well as ethical hacking and penetration testing practices tailored specifically to space missions. These factors increase the resilience of the devices and improve mission reliability, thus promoting global confidence in space activities (Prasad et al., 2023), (Kajornkasirat et al., 2018).

Overall, this study presents a new platform for demonstrating the use of appropriate IoT technology to monitor personnel's physiological status during terrestrial defense and space-like activities. The proposed system was developed using the C# programming language and interfaced with virtual Internet of Things (IoT) devices, thereby enabling real-time collection and analysis of vital indicators such as heart rate, blood pressure, oxygen saturation, body temperature, and carbon dioxide concentration. Because the platform was designed for low-gravity usage, it is not suitable for deployment on other celestial bodies. As per best practices, security measures like data encryption, secure data transmission, and access control ensure the integrity and confidentiality of health-related data. This, in turn, supports the operational needs and ethical frameworks within the modern defense and space medicine field, where data sensitivity and control over human subjects are rapidly changing (Rajesh et al., 2022), (Pahuja et al., 2023).

The main goal of this article is to create, build, as well as validate a secure IoT-based platform suitable for monitoring the real-time health of people involved in the various missions engaged in space exploration or defense. As a result, these types of physicochemical sensors can be supplemented with advanced computational capabilities, sensor networks, localization, and navigation systems and integrated with resilient communication protocols, which define the flavorful business model of future informatics in personalized health management and threat-aware ecological situational inference to improve productivity in ever complex environmental settings.

2. Security Challenges in IoT-Based Health Monitoring Platforms for Defense and Space Missions

The use of cross-involved cyber-physical properties—biometrics data or other sensitive data—and communication systems with a mission-critical characteristic (e.g., controls of spacecraft or scientific instruments) leads to a multi-dimensional attack surface for IoT systems in defense or space medicine (Fernandes et al., 2018). These sorts of platforms can be especially vulnerable to:

- Cyber-attacks that aim to compromise data confidentiality and availability (e.g., eavesdropping, man-in-the-middle, denial-of-service).
- Device tampering or hijacking either prelaunch (supply chain attacks) or in orbit (remote intrusion).
- Insider threats due to the dual-use nature of the data and proximity to sensitive operating environments.
- Physical environment-induced faults — for example, in low-gravity or high-radiation settings, can create data or video streams resembling cybersecurity events or can trigger cybersecurity events.

In order to operate the various countermeasures, the proposed system must be integrated into a multi-layered security architecture designed for:

- Perception Layer Security – Protecting sensors and actuators with encryption and using physical shielding & even embedded security modules from directly accessing sensors and actuators.
- Network Layer Security – Using secure routing protocols, VPN tunnels over satellite relays, and IDS (Intrusion Detection System).
- Application Layer Security – Secure data storage with access control and resilience to web-based vulnerabilities (SQL injection, CSRF, XSS).
- Security Governance Layer – Ensures that technical implementations align with mission policies, compliance standards, and real-time threat intelligence feedback.

To this end, the proposed security framework is structured into four layers (i.e., Perception, Network, Application, and Governance) in a hierarchical form. It creates a strong but modular framework that ensures security rates in non-terrestrial or even contested mission-critical systems. This layered approach aligns with modern best practices in the cyber-physical system's architecture where defense-in-depth should be a design principle. At the Perception Layer level, secrecy is the First Line of Cyber-Physical Defense. This is where the systems that directly interact with both the surrounding or external physical environment and the human crew members corresponding to the perception layer, through sensors and actuators of different kinds, the systems forming the bottom layer of any such system and perhaps also its most exposed frontier. Isolation and protection can be provided by hardware-based security modules, device-level encryption, and physical shields (from direct tampering, environmental disruption (irradiation, microgravity), or adversary access).

However, it is still a quest to implement light encrypting and integrity check mechanisms without draining the constrained resources of (usually) embedded devices. The risk management process must motivate these types of systems (if we are talking about the supply chain of a good or service) to identify these events early on and provide relevant remediation options to the affected party of their good or service, where present such an offer has been part of the infected chain supply if the party has requested it, like making deductions on all of their offers, future to the affected party in case of finding out that exploited offers were indeed exploited and/or their goods/services are exploited in a way that can be quickly remediate some similarities cuts on their goods/service offering available. Therefore, Blockchain or federated trust protocols must be utilized when attesting to supply chains before deploying those supply chains.

Network Layer Security is used to provide Confidentiality and Availability in Hostile Environments. The network layer can provide mechanisms to secure communications from IoT devices out to a central processing or mission control center which is particularly important in satellite-linked or deep-space environments where common networking assumptions cease to be true. The use of VPN tunneling over satellite relays, frequency-hopping schemes, and intrusion detection systems (IDS) helps to mitigate packet sniffing, replay, and denial of service attacks. However, with the factors of latency, packet loss, and the need to support diverse levels of bandwidth as inherent limitations in non-terrestrial networks, implementing delay-tolerant network (DTN) protocols and redundant routing becomes inevitable. In low-bandwidth, high-latency contexts, AI-based anomaly detection in telemetry data is another promising technique to boost detection and isolation capabilities.

The application layer is used for protecting transaction-critical apps and data integrity on this layer. The goal becomes to protect data stored and formulated, secure user entry points, and attack vectors like SQL injections, XSS, and session hijacking. Considering such data collected is medically and operationally sensitive (e.g., biometric indicators), end-to-end encryption, role-based access control (RBAC), and secure coding practices put great emphasis on facilitating them. While these techniques are implemented, there are always zero-day vulnerabilities and the complexity of multi-device integration to contend with. As such, SDLCs for secure software development and automated vulnerability testing (e.g., fuzzing, static code analysis) should be integrated at each stage of development and deployment, especially in environments where systems will be running autonomously for long periods.

The Sovereign Governance layer offers policy alignment, auditability, and resilience engineering. The governance layer is the strategic backbone of this architecture, ensuring technology implementations meet mission-specific, cross-cutting national/international cybersecurity frameworks and ethical constraints. Enhancing this is the layer of adaptive multi-dimensional resilience which utilizes real-time mechanisms for risk assessment and policy enforcement that allows for realignment against both predictive and opportunistic threats. These components must include continuous monitoring systems and audit trails (backed by immutability guarantees) and compliance with something NIST, and so on. Nonetheless, putting this layer into operation in dynamic multi-stakeholder space environments is an inherently challenging proposition. It might necessitate interagency and multinational cooperation and shared threat intelligence platforms to secure situational awareness and unified response processes.

As the projects in space can last a long time, and IoT scenarios can be somewhat critical, it should also incorporate in the design of the system the long-term cryptographic resilience, which is those that use quantum-resistant algorithms (e.g., Lattice-Based Encryption). Moreover, AI-powered anomaly pattern recognition can help proactively detect anomalous behavior on devices and networks, potentially even in zero-trust environments. A formal, multi-layered, and agile method is needed to tackle the security challenges in the IoT-based platforms for the health monitoring of people working in the defense and space domain. The proposed platform utilizes cryptographic best practices, secure-by-design engineering, and continuous threat evaluation to ensure not only the protection of vital physiological data but also mission assurance and ethical compliance. These tenets together act as the foundation for a robust system architecture that can be deployed into the most austere operating environments.

3. Results and discussions

In Figure 1, the component diagram for the defense health monitoring platform can be observed. Herein, the Users check data, configure systems, or dissect trends through UI components. Further on, the state information is pushed to the system via sensors; the IoT Device Manager relays it to the core engine. A prediction module processes the data, stores it securely, and detects anomalies. Hereon, it dispatches alerts through a notification system for mission-critical response. At each stage, in a modular security architecture, authentication and data encryption are managed. With persistence, the data is stored in an encrypted database; the data is visualized in dashboards.

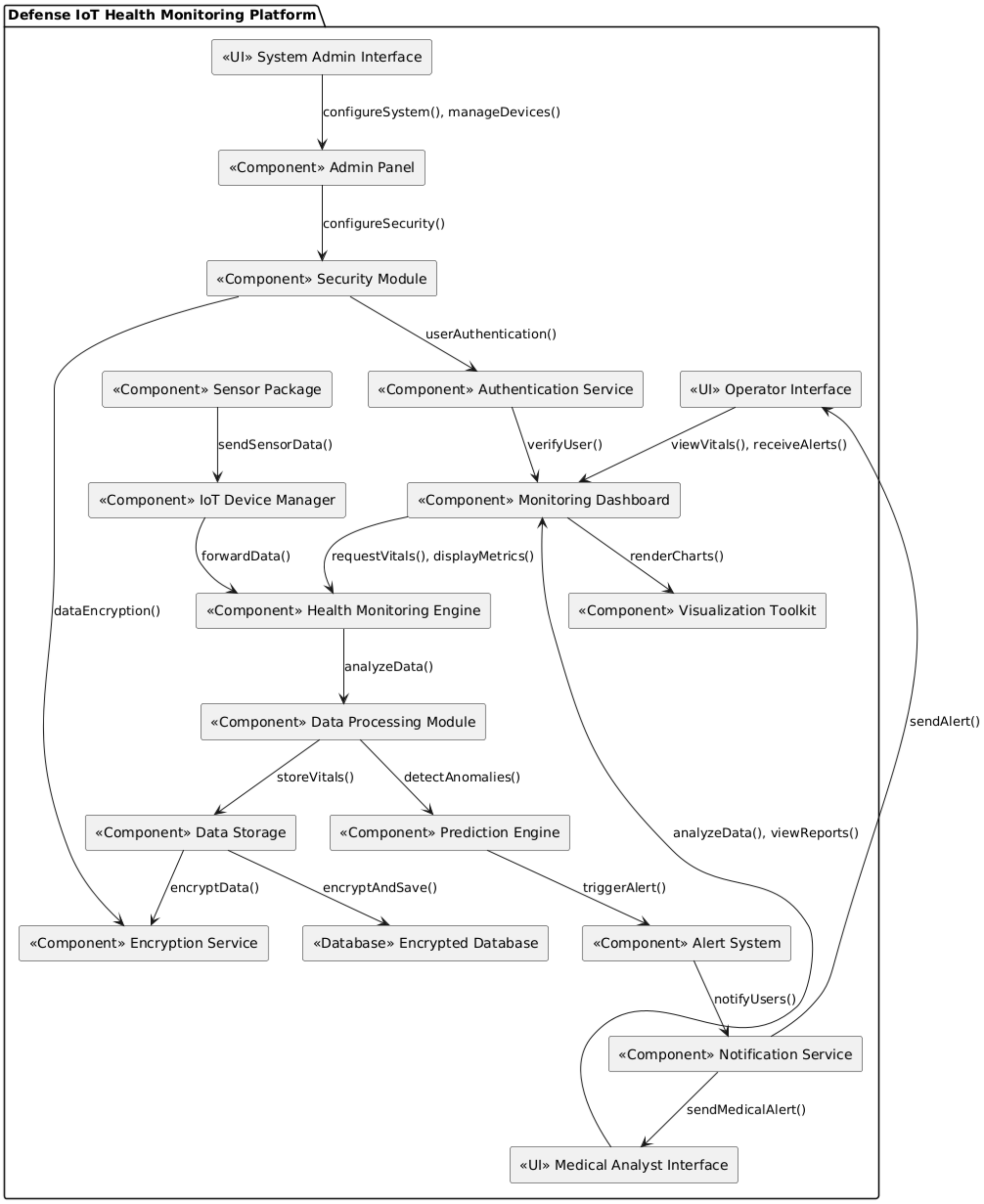
Defense IoT Health Monitoring Platform
«UI» System Admin Interface
configureSystem(), manageDevices()
«Component» Admin Panel
configureSecurity()
«Component» Security Module
userAuthentication()
«Component» Sensor Package
«Component» Authentication Service
«UI» Operator Interface
sendSensorData()
verifyUser()
viewVitals(), receiveAlerts()
«Component» IoT Device Manager
«Component» Monitoring Dashboard
forwardData()
requestVitals(), displayMetrics()
renderCharts()
dataEncryption()
«Component» Health Monitoring Engine
«Component» Visualization Toolkit
analyzeData()
«Component» Data Processing Module
sendAlert()
storeVitals()
detectAnomalies()
«Component» Data Storage
«Component» Prediction Engine
analyzeData(), viewReports()
encryptData()
encryptAndSave()
triggerAlert()
«Component» Encryption Service
«Database» Encrypted Database
«Component» Alert System
notifyUsers()
«Component» Notification Service
sendMedicalAlert()
«UI» Medical Analyst Interface

Figure 1. The Component Diagram for the Defense Health Monitoring Platform

Further on, Figure 2 illustrates the Applied Platform in Defense Mission for Health Monitoring via IoT Devices:

- IoT sensors and devices.
- Health metrics are being tracked.
- Data processing, security, storage (platform components).
- Communication architecture.
- Ability to customize the reporting tailored to end-users (e.g., operator, medical analyst, system admin).

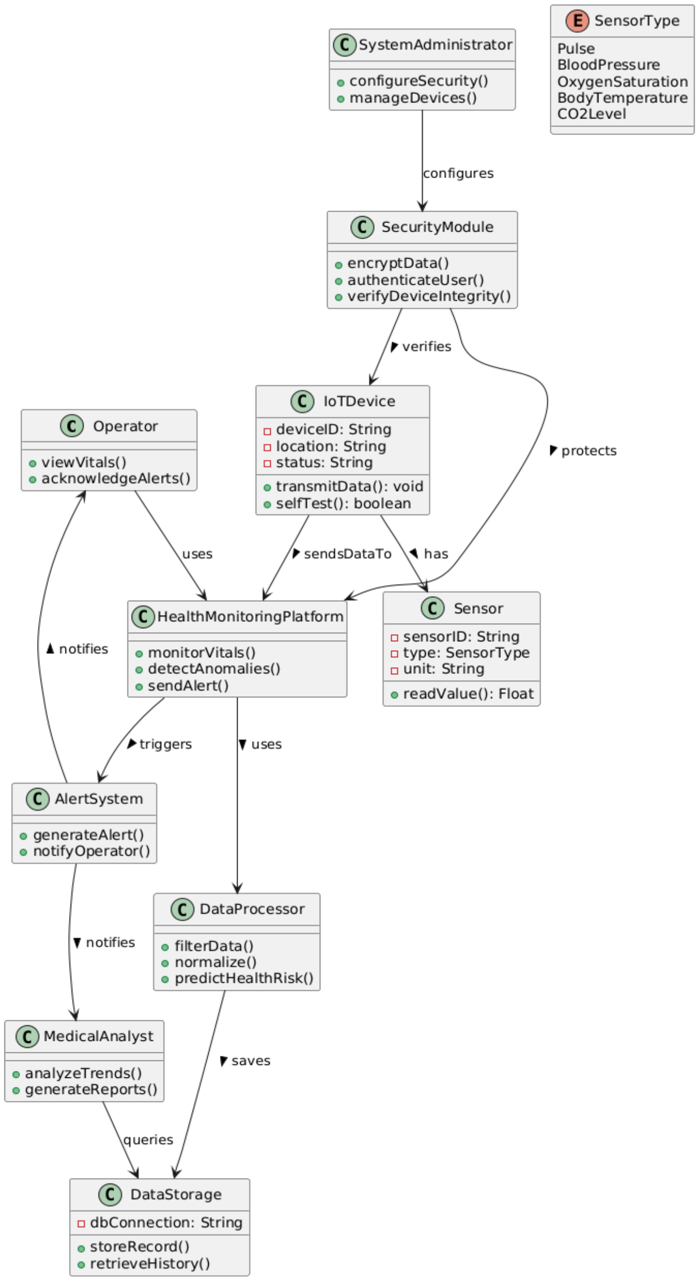

Figure 2. The Class Diagram for IoT Health Monitoring Platform applied to the Defense domain

In Figure 3 we are able to observe the deployment diagram for the proposed IoT health monitoring platform. Herein, IoT sensor and microcontroller hardware (Spacecraft or Ground Defense Unit, referred to as Field Unit). Further, the encrypted sensor data is transmitted via a network link (satellite, radio, or 5G); this also includes computation, security, and persistence, which are handled on the ground servers. Moreover, the operation center includes user interfaces and notification systems for command, analysis, and system administration.

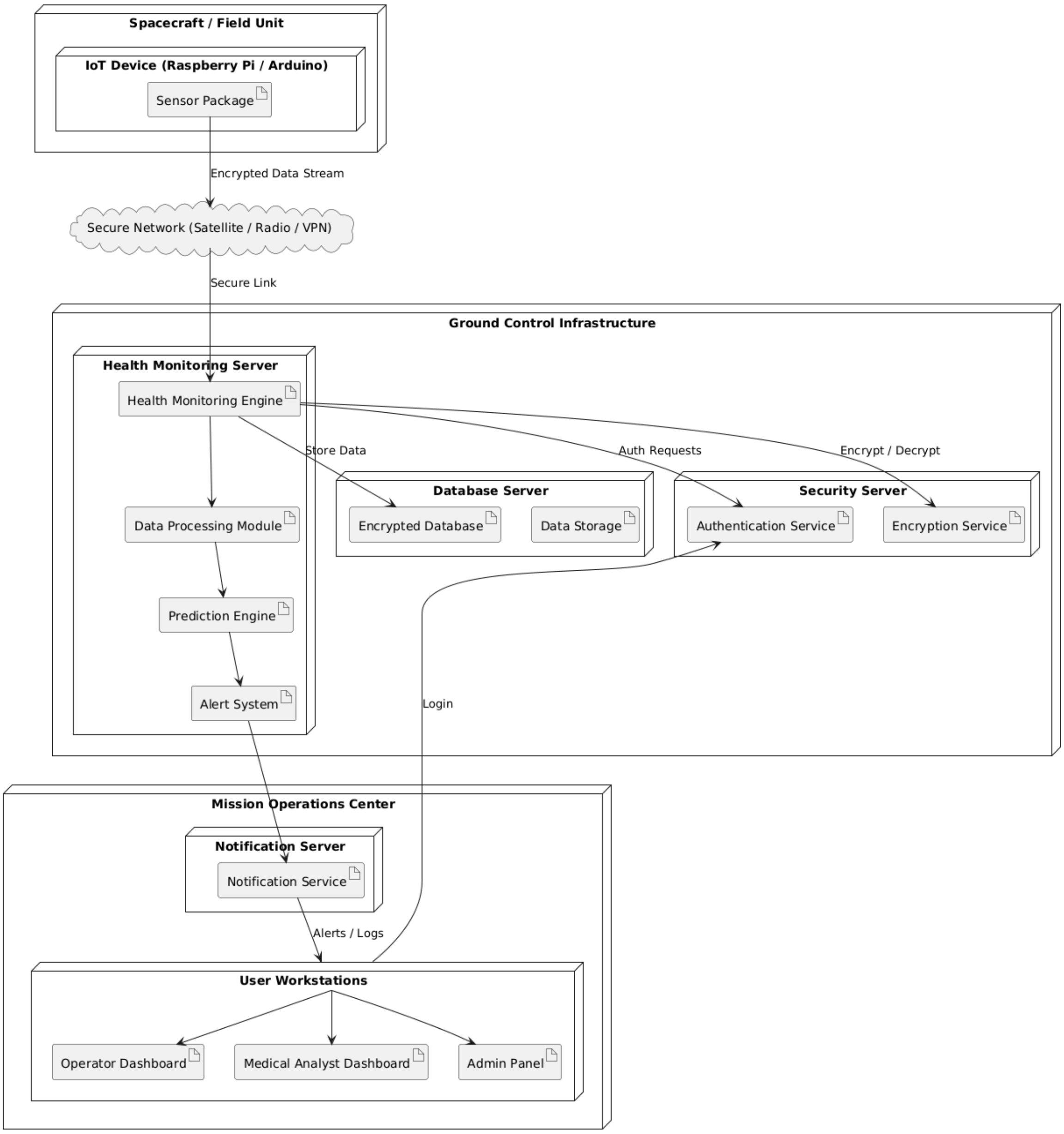

Figure 3. The Deployment Diagram for IoT Health Monitoring Platform applied to the Defense domain

4. Conclusions

In conclusion, a real-time health monitoring IoT platform for defense and space applications would be the step towards bringing cyber-physical systems into mission-critical applications. This paper proposes a platform that utilizes modern sensor technologies, virtualized IoT devices, and secure data acquisition frameworks to fulfill the dual requirements of operational functionality and data protection in hostile or remote environments. A multi-layered security perspective was employed to implement the platform architecture in C#, providing a solid confirmation of engineering security best practices in any system.

The system provides, even in low gravity or intermittent connectivity conditions, confidentiality, integrity, and availability for sensitive physiological data by means of the implementation of encryption protocols, secure boot, role-based access control, and real-time anomaly detection. Finally, the platform's ability to adapt to extreme environments, including microgravity and high-radiation environments in space—demonstrates its potential for use in missions beyond Earth, as well as on Earth for defense operations, through the use for field deployments, humanitarian crises, or remote medical support.

The machine's ability to monitor heart rate, oxygen saturation, blood pressure, and CO_2 levels makes it a vital early warning system for health deterioration. It assists in the preventive medical management of personnel. Industry Perspective — Combating Cybersecurity Threats with Zero Trust-potential Account Protection: From a cybersecurity perspective, the platform provides an extensive threat mitigation framework built on the foundations of Zero Trust, ethical hacking, and compliance with regulatory frameworks. It guarantees the technological soundness of the system while remaining compliant with international data protection rules and operational doctrines across aerospace and defense sectors.

The proposed platform represents a next-generation solution that is flexible and secure enough to work anywhere humans work – where human life, mission success, and national security are inextricably connected. Future improvements must integrate quantum-resistant cryptography, AI-based health analytics, and autonomous reconfiguration capabilities, all of which promise to reinforce the platform as a cornerstone of next-generation aerospace and defense ecosystems.

Author contributions:

- Conceptualization: V.M. and M.I.M.
- Methodology: V.M, M.I.M., and S.L.N.
- Writing original draft: V.M.
- Writing review and editing: M.I.M., and S.L.N.
- Supervision: V.M, M.I.M., and S.L.N.

Funding: This research received no external funding.

Conflict of interest: The Author's declare no Conflict of interest.

References

1. B. Prashanthi, A. Sharma, M. Mahima, K. Navya, R. R. Al-Fatlawy and S. Chidambaranathan, "AI-Driven Smart Health Monitoring System Using Wearable IoT Devices and Predictive Analytics," 2024 International Conference on IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2024, pp. 952-956, doi: 10.1109/ICICAT62666.2024.10923489.
2. C. Gokul Prasad, W. G. Vipshal, O. Leon, A. Thamarai Kannan, B. Sabarinathan and N. Arun Vignesh, "Relating DT Framework in IOT based Heart Rate and Blood Oxygen Monitor with Automatic Data Saving," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1-4, doi: 10.1109/ICCCI56745.2023.10128596.
3. S. Kajornkasirat, N. Chanapai and B. Hnusuwan, "Smart health monitoring system with IoT," 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia, 2018, pp. 206-211, doi: 10.1109/ISCAIE.2018.8405471.

4. T. Rajesh, T. Babu, R. R. Nair and S. Nivedha, "Secure Remote Health Monitoring System and assessment using IOT," 2022 International Conference on Artificial Intelligence and Data Engineering (AIDE), Karkala, India, 2022, pp. 295-300, doi: 10.1109/AIDE57180.2022.10060104.
5. M. Pahuja and D. Kumar, "Several Energy-Efficient Routing Protocols, Design-based Routing Problems and Challenges in IoT-Based WSN: A Review," 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS), Coimbatore, India, 2023, pp. 694-699, doi: 10.1109/ICISCoIS56541.2023.10100555.
6. A. M. Fernandes, A. Pai and L. M. M. Colaco, "Secure SDLC for IoT Based Health Monitor," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018, pp. 1236-1241, doi: 10.1109/ICECA.2018.8474668.