

Cyber-Physical Systems in Healthcare: Design, Interoperability and Security Challenges

Emmanuel Nkansah, Micheal Abimbola Oladosu, Moses Adondua Abah, Olaide Ayokunmi Oladosu

Abstract: *Cyber-Physical Systems (CPS), a combination of embedded computing, communication networks, and physical processes, are increasingly reshaping clinical practice, pharmaceutical supply chains, and hospital infrastructure. This review covers key principles of Medical CPS design; major interoperability frameworks such as FHIR (Fast Healthcare Interoperability Resources), IEEE 11073, and DICOM; and critical cybersecurity risks that threaten patient safety and data integrity, including ransomware, man-in-the-middle, denial-of-service, and data injection attacks. A review of the literature from 2020 to the present (2025) shows that architectural fragmentation has continued, that there is a lack of harmonised security-by-design standards, and that there is a lack of regulatory guidance on real-time MCPS deployments. Some promising mitigation strategies, such as blockchain-based trust frameworks, AI-powered intrusion detection, and digital twin validation, are introduced. The paper's conclusion recommends a research agenda for interoperability protocols, context-aware security models, and international regulatory convergence as essential factors for implementing safe and scalable MCPS.*

Keywords: *Cyber-Physical Systems, Medical IoT, Interoperability, Cybersecurity, FHIR, Blockchain, Healthcare.*

Nomenclature:

CPS: Cyber-Physical Systems

RPM: Remote Patient Monitoring

MCPS: Medical Cyber-Physical Systems

IoMT: Internet of Medical Things

FDA: Food and Drug Administration

MEC: Multi-Access Edge Computing

IWMCPs: Wireless Medical Cyber-Physical System

CDA: Clinical Document Architecture

FHIR: Fast Healthcare Interoperability Resources

MQTT: Message Queuing Telemetry Transport

CoAP: Constrained Application Protocol

UBA: User Behaviour Analytics

FL: Federated Learning

Manuscript received on 12 June 2026 | First Revised Manuscript received on 23 June 2026 | Second Revised Manuscript received on 28 June 2026 | Manuscript Accepted on 15 July 2026 | Manuscript published on 30 July 2026.

*Correspondence Author(s)

Emmanuel Nkansah, Department of Accounting, Economics and Finance, School of Business, La Sierra University, Riverside, United States. Email ID: emma.ampofol122@gmail.com, ORCID ID: [0009-0006-6512-644X](https://orcid.org/0009-0006-6512-644X)

Micheal Abimbola Oladosu*, Department of Chemical Sciences, Faculty of Sciences, Anchor University, Ayobo, Ipaja, Lagos, Nigeria. E-mail ID: mikeoladosu@gmail.com, moladosu@aul.edu.ng, ORCID ID: [0009-0000-5098-1247](https://orcid.org/0009-0000-5098-1247)

Moses Adondua Abah, Department of Biochemistry, Faculty of Pure and Applied Sciences, Federal University of Wukari, Wukari, Taraba State, Nigeria. Email ID: m.abah@fuwukari.edu.ng, ORCID ID: [0000-0002-9268-1661](https://orcid.org/0000-0002-9268-1661)

Olaide Ayokunmi Oladosu, Department of Computer Science, Faculty of Science and Technology, Babcock University, Ilishan-Remo, Nigeria Email ID: pinkrosesng@gmail.com, ORCID ID: [0009-0001-8550-5598](https://orcid.org/0009-0001-8550-5598)

© The Authors. Published by Lattice Science Publication (LSP). This is an open-access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

I. INTRODUCTION

Cyber-physical systems are engineered systems with tightly coupled integration between computational elements such as sensors, actuators, and controllers and physical processes, via real-time communication networks. The convergence in healthcare has led to an emerging field called Medical Cyber-Physical Systems (MCPS) that includes medical devices such as wearable biosensors, implantable drug delivery units, surgical robots, intelligent infusion pumps, and smart hospital infrastructure [1, 2]. With the advent of the Internet of Medical Things (IoMT), which is expected to have over 30 billion connected devices by 2030, CPS is now the operational backbone of healthcare delivery today [3].

The clinical and economic potential of MCPS is tremendous. As of 2024, over 60 million patients in the USA alone have been utilizing remote patient monitoring (RPM) systems powered by IoMT, which allow for the ongoing monitoring of patients' vital signs, drug adherence, and disease progression without the need for hospitalization [4]. Closed-loop insulin delivery systems and AI-assisted anaesthesia management are new ways of pharmaceutical treatment, where the dosage of a drug is dynamically adjusted based on the physiological feedback [5]. Likewise, blockchain-based pharmaceutical supply chains are enhancing the integrity of the cold chain and drug traceability, which are major concerns regarding counterfeit drugs.

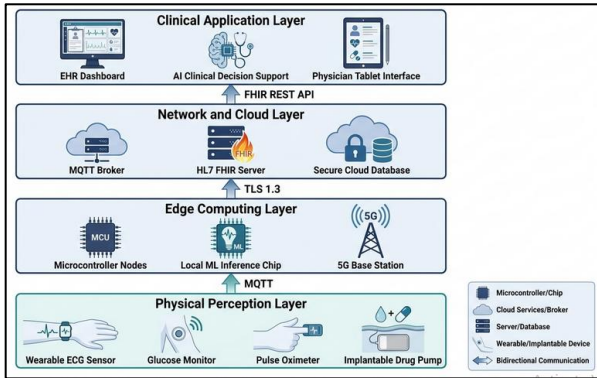
Despite the progress made, there are three interrelated challenges to using MCPS. The first is that the diverse device ecosystems use different communication protocols and data models that make it difficult to realize seamless semantic interoperability [6, 7]. Second, the growing attack surface of network-connected medical devices has placed healthcare at the top of the list of targeted critical infrastructure sectors, as evidenced by 386 reported attacks in 2024 and an estimated 100 million people impacted by the Change Healthcare ransomware attack alone [8]. Thirdly, regulations such as the US Food and Drug Administration (FDA) pre-market cybersecurity guidance and the European Medical Device Regulation (EU MDR) have not caught up with the rate of MCPS innovation, leaving compliance open to interpretation [9].

The goals of this review are to: (i) outline the major design architectures of healthcare CPS; (ii) map out existing interoperability standards and limitations; (iii) list the threats to healthcare CPS; and (iv) discuss new technological and regulatory mitigation strategies.

The need for a common analytical framework to address design, interoperability, and



security in healthcare CPS is an urgent issue identified in several systematic reviews [10,11]. Figure 1 presents the Conceptual architecture of a Medical Cyber-Physical System (MCPS)



[Fig.1: Conceptual Architecture of a Medical Cyber-Physical System (MCPS) Showing the Layered Integration of Physical Sensing Devices, Edge Computing Nodes, Network Communication Protocols, Cloud Services, and Clinical Decision Support Systems]

Sources: Adapted from Conceptual Models in the Literature [2, 12, 13].

II. DESIGN PRINCIPLES OF HEALTHCARE CYBER-PHYSICAL SYSTEMS

A. Architectural Layers

In today's architecture of MCPS, they are considered as multi-layered systems [1, 2]. The perception layer comprises physical sensors such as accelerometers, a pulse oximeter, and implantable glucose monitors that convert physiological parameters into digital signals. Microcontrollers such as the ESP32 and Raspberry Pi can preprocess these signals at the edge, enabling local inference and minimising bandwidth usage and latency. A network layer that sends processed data to cloud platforms where longitudinal analytics, population health modelling and AI-assisted clinical decision support functions take place, increasingly facilitated by 5G network slicing. At the actuation layer, commands are sent back to the physical device to complete the cyber-physical feedback loop [12, 13].

Watson et al. [2] describe MCPS as a different type of IoT deployment, due to the life-critical nature of the actuation commands. A faulty command to an insulin pump or ventilator may harm the patient, with real-time performance, determinism, and fault tolerance requirements that cloud IoT frameworks generally cannot meet.

B. Real-Time and Safety Constraints

One crucial element of the design for MCPS is its real-time response. Different applications have different requirements for latency, such as cardiac defibrillators, which need response windows of less than 100 ms and continuous glucose monitoring systems, which can tolerate updates every few minutes [5,14]. To meet these widely varying latency demands, multi-access edge computing (MEC) architectures have been suggested to decentralize computation to the local base stations and to minimize the round-trip latency to the single-digit millisecond range [13].

Redundancy and graceful degradation are all part of safety-critical design. Alzahrani et al. [14] showed how to use machine learning algorithms in wireless MCPS nodes to detect sensor failures and network anomalies in real time, without disrupting therapy, and automatically switch to backup communication channels. They also developed their Wireless Medical Cyber-Physical System (IWMCPs) framework, which successfully classified 98.3% of attacks on intrusion datasets, demonstrating the dual use of ML for both safety and security.

C. Applications Across Healthcare Domains

Table 1 provides an overview of the main application categories of healthcare CPS, the technologies within the category, selected clinical application examples, and references. Smart hospital infrastructure utilizes CPS sensor networks to track assets, monitor the environment, and predict maintenance needs, minimizing equipment downtime and enhancing infection control [15]. For cold chain compliance of temperature-sensitive drug products and biologics, pharmaceutical supply chains are increasingly implementing CPS-enabled RFID tagging and environmental sensing [16,17]. Table I shows the Application categories of Cyber-Physical Systems in healthcare.

Table I: Application Categories of Cyber-Physical Systems in Healthcare

CPS Category	Key Technologies	Clinical Application	References
Remote Patient Monitoring	Wearable biosensors, IoT gateways, 5G	Chronic disease management, cardiac monitoring	[3, 12, 13]
Smart Drug Delivery	Closed-loop actuators, insulin pumps, infusion systems	Diabetes, oncology, anaesthesia	[5,14]
Medical Imaging & Diagnostics	AI-assisted MRI/CT, edge computing, DICOM	Radiology, pathology, and real-time analysis	[4,10]
Surgical Robotics	Haptic feedback, computer vision, real-time CPS	Minimally invasive surgery, teleoperation	[2, 18]
Emergency & Critical Care	Real-time sensor fusion, alert systems, and ICU networks	Sepsis detection, ventilator management	[15, 19]
Pharmaceutical Supply Chain	RFID, blockchain, temperature/humidity CPS sensors	Drug traceability, cold-chain integrity	[16,17]

MCPS: Medical Cyber-Physical System; IoT: Internet of Things; RFID: Radio-Frequency Identification.

III. INTEROPERABILITY CHALLENGES AND STANDARDS

A. Dimensions of Interoperability

The interoperability of healthcare CPS has four progressive dimensions: technical (physical connectivity), syntactic (data format standardisation), semantic (shared meaning of data

elements), and organisational (cross-institutional governance and policy alignment) [19]. The challenge of achieving semantic interoperability, for example, where a blood pressure reading from a wearable device means the same when viewed by an intensive care unit system as



when viewed by a general practitioner's EHR, is the major unsolved problem [7, 20].

The current state of the art in semantic health data exchange is the Fast Healthcare Interoperability Resources (FHIR) standard, developed by HL7 International and now at Release 5. The FHIR standard has become the preeminent standard for semantic exchange of health data, developed by HL7 International and available in Release 5 [7, 21]. The authors of the systematic review [21] found FHIR's wide adoption in health research and Bossenko et al. [20] showed how to transform legacy HL7 Clinical Document Architecture (CDA) documents to and from FHIR resources in real time using the FHIR Mapping Language, supporting institutional transitions without data loss. However, FHIR was created with a focus on document-oriented data sharing, and does not natively support the high volume, low latency streaming that is essential for real-time MCPS [12].

B. Lightweight Protocols for IoMT

Lightweight application-layer protocols have been widely used to overcome the drawbacks of heavyweight standards such as FHIR and DICOM in resource-constrained IoMT environments. Message Queuing Telemetry Transport (MQTT) is a TCP/IP-based, low-overhead publish-subscribe protocol, and Constrained Application Protocol (CoAP) is a protocol for sending data via UDP. Both of these can be used to communicate low-overhead data from biosensors to a cloud-based broker [12,13]. Falkenheim et al. presented an open-source development framework that was able to successfully acquire biomedical signals in sub-second order using an MQTT-Influx DB-Grafana stack, thus proving that FHIR-compliant real-time IoMT architectures can be implemented without proprietary middleware [12].

Table 2 provides a comparative description of the primary interoperability standards relevant to healthcare CPS, including their scope, their limitations when applied in MCPS environments, and key references.

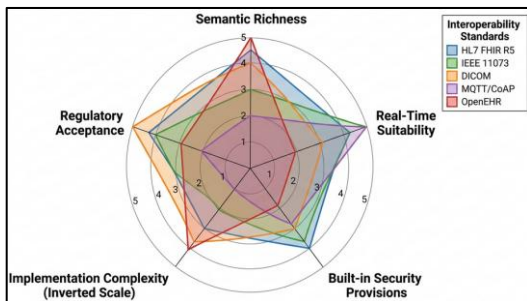
Table II: Interoperability Standards Relevant to Healthcare Cyber-Physical Systems

Standard/Framework	Scope	Limitations in CPS	Reference
HL7 FHIR R4/R5	Clinical data exchange, EHR interoperability	Limited real-time streaming; large payload overhead	[7,21]
IEEE 11073 (x73)	Point-of-care device communication	Scalability challenges in heterogeneous IoMT networks	[6]
DICOM	Medical imaging data exchange	High bandwidth demands; limited CPS edge support	[4]
MQTT/CoAP	Lightweight M2M communication for IoT/IoMT	Lacks semantic interoperability without middleware	[12, 13]
OpenEHR	Archetype-based EHR modelling	Complex implementation; sparse device-level support	[20]
IEC 62443	Industrial CPS cybersecurity framework	Designed for ICS; partial healthcare applicability	[9]

FHIR: Fast Healthcare Interoperability Resources; DICOM: Digital Imaging and Communications in Medicine; MQTT: Message Queuing Telemetry Transport; CoAP:

C. Semantic Gaps and Heterogeneity

One major hindrance to MCPS interoperability is the coexistence of open standards and multiple disjoint device ontologies. However, Adel et al. found that most healthcare institutions with distributed MCPS architectures face semantic mismatches between the data streams generated by the devices and the EHR schema, requiring the development of custom-made middleware solutions that are complex and costly to implement, and therefore can be a target for attack [6]. The 34% of the 158 studies selected for the Internet of Medical Things scoping review by Botsis et al. used FHIR as the sole interoperability layer, while the remaining 66% used a proprietary API or a custom XML schema [19]. Figure 2. Comparative evaluation of interoperability standards for Medical CPS



[Fig.2: Comparative Evaluation of Interoperability Standards for Medical CPS. Radar/Spider Chart Depicting Five Dimensions- Semantic Richness, Real-Time Suitability, Security Provisions, Implementation Complexity, and Regulatory Acceptance, for HL7 FHIR, IEEE 11073, DICOM, MQTT/CoAP, and Open EHR. Higher Scores Indicate Greater Suitability for MCPS Deployment]

Sources: Adapted from references [6, 7, 19].

IV. HEALTHCARE CPS - CYBERSECURITY CHALLENGES

A. The Threat Landscape

Healthcare has been the top target for critical infrastructure sectors for cyberattacks every year. There were 703 incidents of breaches involving 500 or more individuals in 2024, with the number of incidents in 2024 occurring at a lower level than in 2023, but at a much higher level than the number of people impacted by the incident [8]. The BlackCat/ALPHV ransomware group used a double extortion approach to infect an estimated 100 million patient records and wreak havoc on prescription drug processing, clinical authorisations and claims management in thousands of healthcare facilities in the United States [8, 22]. It was a reminder of the fragility of centralised health information intermediaries, as well as the domino effect of a single failure in networked MCPS systems.

Ewoh and Vartiainen's systematic review of healthcare cyberattacks listed the main threat categories: ransomware (which accounted for the majority of attacks), phishing and social engineering, insider threats (which made up a large proportion of the credential harvesting attacks), man-in-the-middle attacks targeting unencrypted device communication, and denial-of-service attacks targeting hospital network infrastructure [22]. The consequences of each of these threat vectors are different for the safety of MCPS: ransomware can break the feedback loop in closed-loop drug delivery; MitM attacks can lead to inaccuracies in sensor data; DoS attacks can cause delays in alarm escalation, particularly in ICUs.



B. Attack Surfaces – Specific to MCPS

Healthcare CPS has a significantly larger attack surface than conventional information systems. Javed et al. have identified three major attack surfaces: (i) wireless communication channels between wearable/implantable devices and gateways are subject to packet injection, blackhole, and greyhole attacks; (ii) cloud and edge computing platforms that store and process patient data; (iii) EHR and clinical decision support systems, which communicate with MCPS outputs [23]. The diversity of device firmware and the fact that many of them are running legacy OS not supported by patching makes them more vulnerable [10,18].

In a pharmaceutical MCPS application, a data injection attack is a potentially more insidious threat. A glucose reading falsification can lead to the administration of an incorrect and dangerous dose of insulin by a closed-loop insulin pump, and falsified temperature sensor data in the pharmaceutical cold chain can mask drug degradation. In the case of the ToN-IoT dataset, Alserhani was able to show that

ML-CCPS could achieve a macro F1 score of 97.8% and an AUC of 99.1% even with noisy telemetry [24].

C. Regulatory and Compliance Dimensions

The regulatory landscape for MCPS security is fragmented, with various jurisdictions controlling specific aspects. The FDA's 2023 guidance on Cybersecurity in Medical Devices requires reporting a Software Bill of Materials (SBOM) and Vulnerability Monitoring Plans for medical devices to be submitted before market and monitored after market, respectively [9]. The EU Medical Device Regulation (EU MDR) and the Medical Device Cybersecurity Guidance provided by ENISA define cybersecurity as one of the General Safety and Performance Requirements; however, the deadlines and enforcement aspects differ significantly from one Member State to another [9, 21]. Specific obligations for MCPS as part of drug manufacturing, clinical trials and supply chain management are placed on them for pharmaceutical applications by 21 CFR Part 11 requirements for electronic records and GxP data integrity guidelines [17]. Table 3 presents the principal cybersecurity threats to healthcare CPS and evidence-based mitigation strategies.

Table III: Principal Cybersecurity Threats to Healthcare CPS and Evidence-Based Mitigation Strategies

Threat Vector	Attack Example	Proposed Mitigation	Reference
Ransomware	WannaCry (NHS 2017); Change Healthcare 2024 (100M records)	Offline backups, network segmentation, MFA	[8, 22]
Man-in-the-Middle (MitM)	Intercepted insulin pump commands	End-to-end TLS encryption, PKI certificate pinning	[18, 25]
Insider Threats	Credential harvesting; unauthorised data access	RBAC, user behaviour analytics (UBA), UEBA	[22, 26]
Routing/Blackhole Attacks	Dropped packets in MCPS wireless networks	Blockchain-enabled Gini index trust framework	[23]
Data Injection / Spoofing	Falsified sensor readings alter clinical decisions	ML anomaly detection, digital twin validation	[11, 24]
Denial of Service (DoS)	Flooding hospital network nodes	Edge computing load distribution, IDS/IPS	[10, 27]

MFA: Multi-Factor Authentication; RBAC: Role-Based Access Control; UEBA: User and Entity Behaviour Analytics; PKI: Public Key Infrastructure; IDS/IPS: Intrusion Detection/Prevention System.

V. EMERGING MITIGATION STRATEGIES

A. Blockchain-Enabled Security Frameworks

To tackle the aforementioned issues of trust, integrity, and auditability in HCP, blockchain technology has come up as a viable architectural solution. The decentralisation, immutability and cryptographic transparency are intrinsic features that overcome the drawbacks of centralised health data storage, as they create a single point of failure [16, 25]. To safeguard EHRs from cyberattacks, Kumar et al. introduced a decentralised blockchain architecture that includes elliptic curve cryptography and biometric authentication for improved data confidentiality and access control, as compared to PKI-only baselines [25]. In the pharmaceutical supply chain, MCPS, blockchain platforms are being used to allow for the inclusion of sensor-derived information for tracking the cold chain, with the inclusion of immutable, distributed ledger entries [16, 17] to record the provenance of high-value biologics with tamper-evident records.

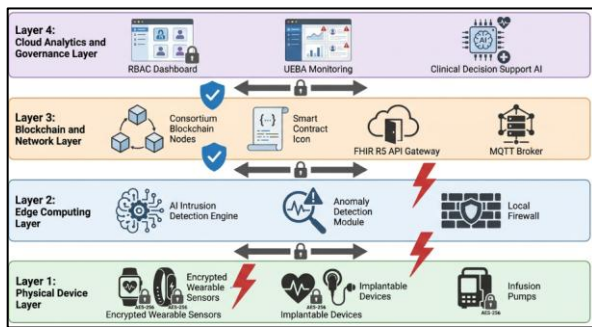
Javed et al. adopted a blockchain approach to the network layer of smart healthcare CPS by designing a blockchain-based trust framework on the Gini index, which claimed to achieve 95.4% detection accuracy with minimal false positive probability for blackhole and greyhole attack nodes in

wireless sensor networks [23]. Consortium blockchain architectures, which rely on trust among a specific group of healthcare organizations, have been suggested to provide a compromise between transparency and confidentiality of patient data [9].

B. Artificial Intelligence and Machine Learning for Intrusion Detection

The volume and type of data generated by the MCPS networks make it impossible for a rule-based IDS to detect intrusions effectively. Anomaly detection models based on AI identification of abnormal network flow and the behaviour of devices provide adaptive and scalable options [11, 24]. To deploy the system to hardware with low computational power, Kumaar et al. successfully implemented a hybrid deep learning IDS framework named ImmuneNet that achieved 99.19% accuracy for the CIC Bell DNS 2021 dataset, with less than one million parameters, outperforming ensemble baseline models [11]. Alserhani's ML-CCPS includes a cognitive loop with feedback, which continuously re-trains the classification models by incorporating residual behavioural trends that adapt to novel attack signatures without manual signature updates [24].





[Fig.3. Proposed Integrated Security and Interoperability Framework for Healthcare CPS. The Diagram Illustrates a Four-Layer Reference Model: (1) a Physical Device Layer with Encrypted Sensor Nodes; (2) an Edge Computing Layer Incorporating AI-Based Intrusion Detection; (3) a Blockchain-Secured Network and data Exchange Layer Supporting FHIR R5 and MQTT; and (4) a cloud Analytics and Clinical Decision Layer with RBAC and UEBA Governance]

Sources: Adapted from References [23, 24, 25, 27].

C. Digital Twins and Federated Learning

Using digital twin technology, which involves creating a real-time virtual replica of physical MCPS components, enables proactive security validation without impacting live clinical systems. Security teams can use the digital twin to simulate attacks on the infusion pump network and identify vulnerabilities in firmware logic and communication protocols before they are exploited. To improve the generalisation of the detection model without compromising patient privacy, federated learning (FL) frameworks have been proposed to allow training collaborative AI models in the distributed CPS environments found in hospitals [14].

VI. DISCUSSION

The review has uncovered a recurring theme in the development of healthcare CPS: the need for clinical functionality and connectivity, interoperability across diverse device ecosystems, and robust cybersecurity in life-critical environments. All three are not mutually exclusive; they must all be satisfied, which means doing security by design rather than patching in place.

HL7 v2, DICOM, and proprietary device protocols demonstrate how healthcare IT has been built over 40 years with a focus on incremental investments and without a plan for a CPS paradigm. The move towards a unified semantics will require harmonised reference architectures (analogous to the EU's European Interoperability Framework) and regulatory obligations specifying minimum interoperability profiles for new devices entering the MCPS market [19, 20, 21].

The industry's continued cybersecurity under-investment, with an estimated 6% of IT spend dedicated to cybersecurity versus 15% for financial services, makes the healthcare sector structurally vulnerable from the security point of view [22]. This lack of investment is now evident in patient safety incidents, including documented clinical deterioration at Ascension hospitals following a 2024 ransomware attack on the company that crippled clinical information systems. One route to adequate resourcing is regulatory frameworks that correlate cybersecurity maturity levels with reimbursement

and/or access to the market, based on models such as IEC 62443 and the NIST Cybersecurity Framework [9].

In the field of pharmaceutical Science, MCPS will create opportunities and pose regulatory challenges. Closed-loop systems for drug delivery in oncology, metabolic disorders, and pain management have the potential to deliver precise doses that cannot be derived from conventional pharmacokinetic models. But, when combined with software-mediated dosing algorithms and physical drug delivery actuators, software failure can have direct toxicological implications that the existing software frameworks do not fully address [5, 14, 17].

VII. CONCLUSION

The operational limits of healthcare and pharmaceuticals are shifting with the advent of cyber-physical systems, which enable closed-loop drug delivery, real-time remote monitoring, smart hospital infrastructure, and blockchain-secured supply chains. As shown in this review, architectural fragmentation (to ensure interoperability), a growing and complex cybersecurity threat environment, and regulatory frameworks that do not keep up with technology are three interconnected challenges that continue to limit the full clinical and economic impact of MCPS.

New solutions, such as AI-powered intrusion detection systems with over 97% accuracy, blockchain-backed trust frameworks for network and data security, federated learning for privacy-preserving model development, and digital twin security validation, offer a viable path to secure, interoperable MCPS. To make this roadmap a reality, coordinated efforts are needed by device manufacturers, the healthcare sector, standards organisations, and regulators to create consistent interoperability profiles, security-by-design requirements, and harmonised post-market cybersecurity surveillance guidelines across the countries where devices will be deployed. Future studies should focus on longitudinal clinical studies of MCPS security frameworks in real hospital environments, regulatory science to facilitate adaptive approval pathways for AI-based closed-loop medical devices, and health-economic modelling of the return on investment of cybersecurity investments in MCPS-dependent care settings.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted objectively and free from external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of



this article are publicly accessible.

- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Yaacoub JA, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. Cyber-physical systems security: limitations, issues and future trends. *Microprocess Microsyst*. 2020; 77:103201. DOI: <http://doi.org/10.1016/j.micpro.2020.103201>
2. Watson A, Park J, Pugh S, Sokolsky O, Weimer J, Lee I. Medical cyber-physical systems: IoMT applications and challenges. In: 2022 56th Asilomar Conference on Signals, Systems, and Computers; 2022. p. 998–1004. DOI: <http://doi.org/10.1109/IEEECONF56349.2022.10052110>
3. Siwicki B. How IoT is transforming remote patient monitoring. *Healthcare IT News* [Internet]. 2024. Available from: <https://www.healthcareitnews.com/news/how-iot-transforming-remote-patient-monitoring>
4. Bossencko I, Randmaa R, Piho G, Ross P. Interoperability of health data using FHIR Mapping Language: transforming HL7 CDA to FHIR with reusable visual components. *Front Digit Health*. 2024; 6:1480600. DOI: <http://doi.org/10.3389/fdgth.2024.1480600>
5. Hermawan D, Dewi Kansa Putri NM, Kartanto L. Cyber-physical system-based smart healthcare system with federated deep learning architectures with data analytics. *Int J Commun Netw Inf Secur*. 2022;14(2):222–233. DOI: <http://doi.org/10.17762/ijcnis.v14i2.5513>
6. Adel E, El-Sappagh S, Barakat S, Kwak KS, Elmogy M. Semantic architecture for interoperability in distributed healthcare systems. *IEEE Access*. 2022; 10:126161–126179. DOI: <http://doi.org/10.1109/ACCESS.2022.3226126>
7. Vorisek CN, Lehne M, Klopfenstein SAI, Mayer PJ, Bartschke A, Haese T, et al. Fast Healthcare Interoperability Resources (FHIR) for interoperability in health research: systematic review. *JMIR Med Inform*. 2022;10(7):e35724. DOI: <http://doi.org/10.2196/35724>
8. Riggi J. A look at 2024's health care cybersecurity challenges. *AHA News* [Internet]. 2024 Oct 7. Available from: <https://www.aha.org/news/aha-cyber-intel/2024-10-07-look-2024s-health-care-cybersecurity-challenges>
9. Ali A, Al-rimy BAS, Almazroi AA, Alsabaei FS, Almazroi AA, Saeed F. Securing secrets in cyber-physical systems: a cutting-edge privacy approach with consortium blockchain. *Sensors*. 2023;23(16):7162. DOI: <http://doi.org/10.3390/s23167162>
10. El-Kady AH, Halim S, El-Halwagi MM, Khan F. Analysis of safety and security challenges and opportunities related to cyber-physical systems. *Process Saf Environ Prot*. 2023; 173:384–413. DOI: <http://doi.org/10.1016/j.psep.2023.03.012>
11. Kumaar MA, Samiyya D, Vincent PMD, Srinivasan K, Chang CY, Ganesh H. A hybrid framework for intrusion detection in healthcare systems using deep learning. *Front Public Health*. 2022; 9:824898. DOI: <http://doi.org/10.3389/fpubh.2021.824898>
12. Adochiei FC, Țoi FA, Adochiei IR, Argatu FC, Seritan G, Petroiu GG. HL7 FHIR-based open-source framework for real-time biomedical signal acquisition and IoMT interoperability. *Appl Sci*. 2025;15(23):12803. DOI: <http://doi.org/10.3390/app152312803>
13. Alasmay H. ScalableDigitalHealth (SDH): an IoT-based scalable framework for remote patient monitoring. *Sensors*. 2024;24(4):1346. DOI: <http://doi.org/10.3390/s24041346>
14. Alzahrani A, Alshehri M, AlGhamdi R, Sharma SK. Improved Wireless Medical Cyber-Physical System (IWMCPs) based on machine learning. *Healthcare*. 2023;11(3):384. DOI: <http://doi.org/10.3390/healthcare11030384>
15. Jamil F, Ahmad S, Iqbal N, Kim DH. Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. *Sensors*. 2020;20(8):2195. DOI: <http://doi.org/10.3390/s20082195>
16. Kunal S, Gandhi P, Rathod D, Amin R, Sharma S. Securing patient data in the healthcare industry: a blockchain-driven protocol with advanced encryption. *J Educ Health Promot*. 2024; 13:94. DOI: http://doi.org/10.4103/jehp.jehp_984_23
17. Yelezhanova S, Seitenov A, Kenzhetgarina A, Kenzhetayev A, Kemel A, Ualiyev N, et al. Comprehensive analysis of blockchain technology in the healthcare sector and its security implications. *Int J E-Health Med Commun*. 2025;16(1):1–45. DOI: <http://doi.org/10.4018/IJEHMC.372423>
18. Harkat H, Camarinha-Matos LM, Goes J, Ahmed HF. Cyber-physical systems security: a systematic review. *Comput Ind Eng*. 2024; 188:109891. DOI: <http://doi.org/10.1016/j.cie.2024.109891>
19. Seth M, Jalo H, Högstedt Å, Medin O, Sjöqvist BA, Candefjord S. Technologies for interoperable internet of medical things platforms to manage medical emergencies in home and prehospital care: scoping review. *J Med Internet Res*. 2025;27: e54470. DOI: <http://doi.org/10.2196/54470>
20. Weber SB, Stein S, Pilgermann M, Schrader T. Attack detection for medical cyber-physical systems: a systematic literature review. *IEEE Access*. 2023; 11:41796–41815. [Authors to verify final DOI directly on IEEE Xplore before resubmission] DOI: <http://doi.org/10.1109/ACCESS.2023.3267804>
21. Rajab RM, Abuhmida M, Wilson I, Ward R. A review of IoMT security and privacy related frameworks. *Proc Eur Conf Cyber Warfare Secur*. 2024;23(1):729–739. DOI: <http://doi.org/10.34190/eccws.23.1.2239>
22. Ewoh P, Vartiainen T. Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. *J Med Internet Res*. 2024;26: e46904. DOI: <http://doi.org/10.2196/46904>
23. Javed M, Tariq N, Ashraf M, Khan FA, Asim M, Imran M. Securing smart healthcare cyber-physical systems against blackhole and greyhole attacks using a blockchain-enabled Gini index framework. *Sensors*. 2023;23(23):9372. DOI: <http://doi.org/10.3390/s23239372>
24. Alserhani F. Intrusion detection and real-time adaptive security in Medical IoT using a cyber-physical system design. *Sensors*. 2025;25(15):4720. DOI: <http://doi.org/10.3390/s25154720>
25. Kumar A, Singh AK, Ahmad I, Singh PK, Verma PK, Alissa KA, et al. A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare. *Sensors*. 2022;22(15):5921. DOI: <http://doi.org/10.3390/s22155921>
26. Pokharel BP, Kshetri N, Sharma SR, Paudel S. blockHealthSecure: integrating blockchain and cybersecurity in post-pandemic healthcare systems. *Information*. 2025;16(2):133. DOI: <http://doi.org/10.3390/info16020133>
27. Mansour RF, El Amraoui A, Nouaouri I, Díaz VG, Gupta D, Kumar S. Artificial intelligence and internet of things enabled disease diagnosis model for smart healthcare systems. *IEEE Access*. 2021; 9:45137–45146. DOI: <http://doi.org/10.1109/ACCESS.2021.3066365>

AUTHORS PROFILE

Emmanuel Nkansah is a seasoned Data Analytics Professional with a Bachelor's degree in Physics and two Master's degrees, including Business Analytics. His academic background includes specialised training in Quantum Physics and Computational Physics, providing a strong foundation in analytical thinking, mathematical modelling, and complex problem-solving. He possesses extensive experience in database management, data collection, data cleansing, data warehousing, SQL development, exploratory data analysis (EDA), machine learning, predictive modelling, and business reporting. Combining technical expertise with strong business acumen, he leverages data-driven insights and advanced analytical techniques to develop innovative solutions, optimise organisational performance, support strategic decision-making, and drive sustainable business growth.



Micheal Abimbola Oladosu is an interdisciplinary researcher with a strong academic and research background. He is the founder of Research Hub Nexus Institute, a platform dedicated to research publication, academic writing support, and mentorship for emerging scholars. He currently lectures in the Department of Chemical Sciences (Biochemistry Unit), Anchor University, Lagos, Nigeria. His research interests span the intersections of the life sciences, biomedical sciences, and technology, and he has actively collaborated on multidisciplinary research projects that have been published in reputable peer-reviewed journals. He is also a reviewer for several academic journals and serves on the editorial boards of multiple international scientific journals and publications.



Moses Abah Adondua is a dedicated biochemist and lecturer at the Department of Biochemistry, Faculty of Biosciences, Federal University Wukari, Nigeria. With a strong academic foundation and research interests in molecular biology, enzymology, and metabolic disorders, he is actively involved in both teaching and research, mentoring undergraduate students and contributing to the development of innovative approaches. research in biochemistry. Currently, he is the Co-Founder of Research Hub Nexus, where he helps advance research, innovation, and academic collaboration. He also participates in scholarly publishing, peer review, and capacity-building initiatives aimed at strengthening scientific research in Africa and globally, respectively.





Olaide Ayokunmi Oladosu (née Ayansiji) is a dedicated technology professional and researcher. She holds a Bachelor's degree in Computer Science from Babcock University, Ilishan-Remo, Ogun State, Nigeria. She also obtained a Postgraduate Diploma in Computer Science from Teesside University in the United Kingdom. Olaide is a Certified Cisco Network Associate (CCNA). Her passion for continuous learning and innovation in the tech space is reflected in her scholarly contributions. She has co-authored several publications in reputable peer-reviewed journals, demonstrating her commitment to academic and professional excellence. She continues to contribute to research, innovation, and capacity building in the globally respected technology community.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Lattice Science Publication (LSP)/ journal and/ or the editor(s). The Lattice Science Publication (LSP)/ journal and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.