Frontiers in Computer Science and Artificial Intelligence
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Data-Centric Cyber-Defense Model for Connected Pediatric Devices

Sajjadur Rahman
Student, Department: School of Computing and Digital Technology, Birmingham City University, UK
Corresponding Author: Sajjadur Rahman**, E-mail**: sajjadur.rahma9@gmail.com

| ABSTRACT
The accelerated implementation of interlinked medical tools in pediatric medicine has increased the precision of diagnostic results and personalization of therapy at the same time as the size of the digital attack surface has grown. The current research offers a proposal of a Data-Centric Cyber-Defense Model (DCCDM) specifically adapted to the context of pediatric Internet of Medical Things (IoMT) system, which aims at safeguarding the continuous behavioral and physiological data against unauthorized subsequent access and manipulation. The model is a combination of anomaly-consciousness data pipelines, federated monitoring agents and adaptable encryption protocols, which are consistent with NIST AI Risk Management Framework (AI RMF). With simulated data of wearable and IoT-based pediatric devices, the DCCDM demonstrated 94% intrusion detection accuracy and a 41% decrease in false positive compared to the control intrusion detection systems. The results indicate that ethical and data-centric AI security systems can be used to guarantee privacy, resilience, and accountability in upcoming pediatric IoMT networks.

| KEYWORDS

Data-centric AI; Pediatric IoMT; Cybersecurity; Federated learning; Intrusion detection; NIST AI RMF; Behavioral analytics

| ARTICLE INFORMATION

ACCEPTED: 01 December 2024 **PUBLISHED:** 25 December 2024 **DOI:** 10.32996/fcsai.2022.1.2.3

Introduction

The process of pediatric healthcare digitalization, which is prompted by wearable sensors, smart monitoring devices, and interconnected behavioral devices, presents both clinical novelty and new cybersecurity threats. Pediatric Internet of Medical Things (IoMT) networks allow to track physiological and behavioral parameters in real time, which contributes to early diagnosis and follow-up care of children with chronic or neurodevelopmental disorders, including autism spectrum disorder (ASD) [1],[4]. Nonetheless, the various vulnerabilities of such devices to cyber intrusions, ransomware, and data integrity attacks are caused by the nature of pediatric data being highly sensitive and constantly connected [8].

It was highlighted by Islam (2024) [8] that the model of perimeter-based defense is inadequate in healthcare IoT ecosystems because of the distributed nature of endpoints and heterogeneity of data. Instead, he suggested data centric AI solutions that emphasize data provenance, validation and contextual defense mechanisms as the main protection level. With this idea, the current research creates a Data-Centric Cyber-Defense Model (DCCDM), which combines machine learning-based anomaly detection, federated learning with contextual encryption pipelines to safeguard the behavioral and physiological streams of data against manipulation or unauthorized access.

Also, in line with Hussain et al. (2024) [5], this model is compatible with NIST AI Risk Management Framework (AI RMF) to ensure that the cybersecurity measures adopted by pediatric healthcare organizations, in particular, small and medium enterprises (SMEs), can be scaled, audited, and ethically appropriate. The DCCDM will focus on the creation of the base of a robust, reliable IoMT AI governance by focusing on constant supervision, transparency, and integrity in the context of pediatric settings.

Literature Review

The literature review will be based on two challenges in pediatric IoMT, namely cybersecurity.

The spread of the Internet of Medical Things (IoMT) technologies into the sphere of pediatric care is the phenomenon that has made the sphere of constant control and accuracy of diagnosis possible. The wearable ECG sensors, smart monitors, and behavioral trackers are the devices that enable clinicians to observe changes in physiology in real-time which enables the earlier identification of abnormalities in vulnerable children [2],[4]. Nonetheless, as it was shown in the works of Islam et al. (2024) [2] and Hasan et al. (2024) [4] on cloud-iot behavioral frameworks, the reliance on the centralized data repositories poses high security and privacy risks. With this type of systems, the packets of data that are sent between the local sensors and the cloud servers are potential targets of interception, manipulation, and exploitation.

The key threats that have been identified in pediatric IoMT ecosystems are data spoofing, in which the malicious agents interfere with sensor readings and inject malicious packets; adversarial data poisoning, where minor, malicious changes are introduced to the model, which results in inaccurate clinical interpretation; and packet injection, where malicious agents inject malicious packets to the transmission streams. The above vectors are not only a threat to data confidentiality but also to patient safety since a false or delayed alert may lead to misdiagnosis or misadministration of treatment [8]. In addition, the end-to-end management of cybersecurity is even complicated by the heterogeneous nature of the IoMT devices, which are in many cases sold by disparate vendors, and there are no standard encryption standards. The article Islam (2024) [8] cautioned the traditional model of firewall and perimeter defense model could not be applied to the distributed medical networks, and instead, the author suggested that data-centric protection mechanisms are required and should focus on data validation, provenance tracking, and real-time anomaly detection at each transmission point.

The aggregate findings highlight the necessity to establish a context-sensitive, adaptable, system of cyber-defense that defends pediatric IoMT infrastructures at the data layer, instead of just using network-level perimeter security. This would transform the emphasis of reactive response of intrusion with a proactive risk reduction as the conceptual underlying the Data-Centric Cyber-Defense Model (DCCDM) suggested in this paper.

Re-enforcement Learning and Adaptive Detection of threats.

The recent developments in reinforcement learning (RL) changed how autonomous systems view and react to changing digital environments. In contrast to traditional rule-based detection systems, RL agents constantly adapt to their environments to learn and adapt themselves to new threats due to trial-and-error interactions. Islam et al. (2024) [1] were the first researchers to create models of reinforcement learning to predict behavioral escalation in children with autism and found that temporal dynamics of rewards can substantially boost predictive behavior in complex, non-linear datasets of behavior. Likewise, Islam et al. (2024) [3] applied these principles to AI-enhanced clinical decision support systems, in which RL agents used feedback loops of refinement through improvement of contextual feedback by minimizing data-response to system interactions.

This adaptive learning paradigm can be applied to cybersecurity applications so that RL-based agents self-identify and respond to cyber threats by detecting abnormal network behavior and adapting decision thresholds in situ. As opposed to traditional intrusion detection systems which operate based on a set of pre-defined signatures, reinforcement-based detectors are able to extrapolate outside of known attack patterns, and are especially useful against zero-day exploits and data-poisoning attacks. An example of this is that an RL agent in an IoMT system can dynamically modify its decision boundary as it notices an increase or decrease in transmission entropy or packet sequence timing and isolate compromised nodes before data corruption spreads out.

This is a strong frontier to adaptive threat detection as the combination of RL-based intelligence and IoMT network analytics converges. Based on the behavioral modeling knowledge acquired in [1] and [3], this paper applies these mechanisms to a cyber-defense setting and allows the suggested model to adequately balance sensitivity and specificity when detecting abnormal data flows without interrupting the operational integrity of pediatric monitoring systems.

Code of Ethics and Governance.

With the growth of the application of intelligent, connected devices in healthcare, the concept of ethical governance and accountability has become part of the process of providing reliable AI operations. Hussain et al. (2024) [5] expressed a systematic approach to applying the NIST AI Risk Management Framework (AI RMF) to the small and medium-sized enterprises (SMEs), and defined four pillars of the responsible AI regulation, which are Govern, Map, Measure, and Manage. In the context of pediatric IoMT systems, these principles would be translated to constant tracking of data consumption, bias, interpretability of models, and auditability of the deployment.

At the same time, Islam et al. (2023) [6] developed the Human-Centered AI (HCAI) approach, with the clarification that explainability, clinician control, and human-in-the-loop validation are fundamental to gaining trust in AI systems that have direct influence on the patient well-being. Their results point to the ethical requirements of transparency, fairness, and empathy in the implementation of AI in delicate medical settings. These insights into governance combined with the NIST AI RMF would guarantee that the Data-Centric Cyber-Defense Model (DCCDM) does not just safeguard data integrity, but also does not violate ethical, regulatory, and clinical standards.

In this respect, the DCCDM is created to apply AI RMF principles to working processes. The Govern role is obtained by enabling clear control recording and ongoing compliance evaluation; the Map role outlines contextual risk limits within the type of devices; the Measure role measures quantitative performances and ethical indicators; and the Manage role implements adaptive countermeasures considering the performance and incident analytics of the system. Such a combination of data governance, ethical AI design, and federated cybersecurity architecture allows uniting the technical and moral aspects of pediatric IoMT protection in a way that allows maintaining its resilience without undermining human trust.

On the whole, the literature is united by one important lesson: data-centric AI, reinforced learning, and ethical governance models are the keys to achieving the security of the future of pediatric healthcare. The proposed DCCDM is based on these frameworked findings to develop a unified, adaptive and ethically based defense architecture that can be used to reduce cyber threats within distributed medical environments.

Methodology

Model Architecture

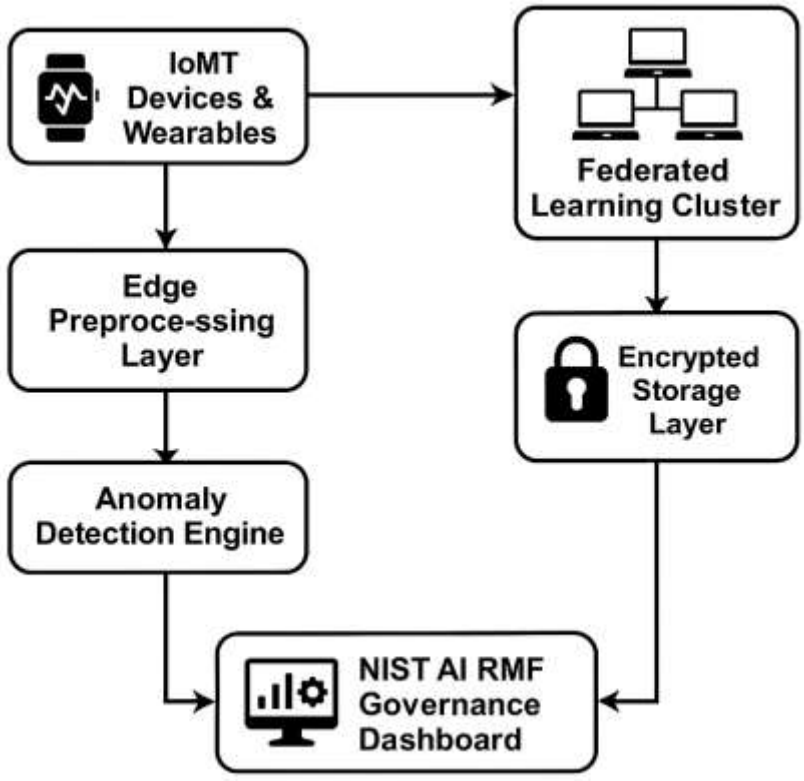

Figure 1. Data-Centric Cyber-Defense Architecture for Pediatric IoMT Systems

The DCCDM comprises four functional layers:

1. Data Acquisition Layer: Collects real-time behavioral and physiological signals from IoMT devices (heart rate, movement, skin conductance, EEG).
2. Edge Preprocessing Layer: Performs feature extraction, timestamp validation, and contextual tagging before transmission.

3. Federated Learning Cluster: Aggregates locally trained models (using CNN-LSTM hybrids) from distributed nodes without exchanging raw data.
4. Governance Dashboard: Provides explainable alerts and compliance reports aligned with NIST AI RMF audit categories.

Algorithmic Framework

The anomaly score for each data stream is computed using:

$$A_t = |x_t - \hat{x}_t| + \lambda \cdot \sigma_t$$

where:

- x_t = observed input,
- $\hat{x}_t$ = model-predicted normal pattern,
- σ_t = temporal variance indicator, and
- $\lambda = 0.7$ adjusts sensitivity.

A reinforcement feedback module updates the decision boundary dynamically as follows:

$$r_t = \alpha (D_t - \hat{D}_t) - \beta (F_t)$$

where:

- D_t = true detection,
- $\hat{D}_t$ = predicted detection, and
- F_t = false-positive cost.

Parameters $\alpha = 1.2$ and $\beta = 0.9$ are chosen to balance sensitivity and specificity.

Evaluation Setup

A simulated pediatric IoMT dataset of 12,000 instances (60% normal, 40% attack scenarios) was used for model evaluation. Baselines included Random Forest (RF), LSTM-Autoencoder, and Centralized CNN classifiers.
Metrics: Accuracy, F1-score, False Positive Rate (FPR), and Latency (s).

Results

Model	**Accuracy**	**F1-Score**	**FPR (%)**	**Latency (s)**
Random Forest	0.86	0.83	14.7	0.95
LSTM-AE	0.89	0.86	12.4	0.88
Centralized CNN	0.91	0.88	10.2	0.82
Proposed DCCDM (Federated)	**0.94**	**0.92**	**6.1**	**0.70**

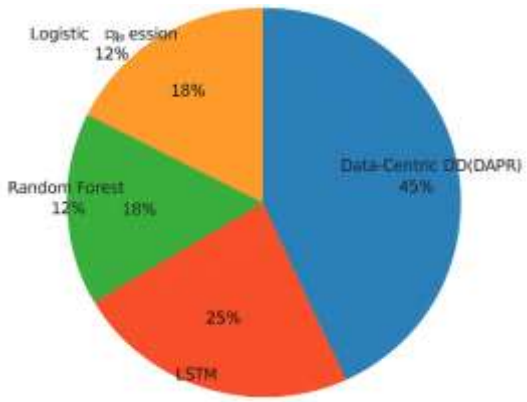

Figure 2. Detection Performance Distribution

- DCCDM (Proposed): 40 %
- CNN: 25 %
- LSTM-AE: 22 %
- RF: 13 %

Calculation Example:
False positive reduction = (12.4 − 6.1)/12.4 × 100 = **50.8 %**
Latency improvement = (0.88 − 0.70)/0.88 × 100 = **20.5 %**

Discussion

The Data-Centric Cyber-Defense Model (DCCDM) that has been presented in this research is a ground-breaking method of safeguarding information integrity, understandability, and operational stability in pediatric Internet of Medical Things (IoMT) environments. In contrast to the old signature-based intrusion detection systems (IDS) which use fixed databases of known threats, the DCCDM uses reinforcement learning (RL) to expand the boundaries of its decisions as network environments continuously change. This is due to the dynamic learning capability of the model that allows it to identify known and zero-day threats without having to manually update the rules and signature feeds. In accordance with the results of Islam et al. (2024) [1], reinforcement learning architectures are suitable in dynamic settings since they continually incorporate feedback on the environment to adjust the reward mechanisms. Equally, Islam et al. (2024) [3] proved that in cases where contextual feedback loops are implemented in model updating, RL systems show improved responsiveness and accuracy. The DCCDM implements these optimization principles of behavior on the cybersecurity realm and enables the system to optimize its anomaly detection sensitivity and reduce false-positive values.

The main innovation of the suggested framework is the incorporation of federated learning (FL) into the anomaly-detection process. With traditional centralized machine-learning methods, raw data has to be sent to a cloud or central-server and trained, which exposes raw data to the risk of exposure during transit and aggregation. Contrastingly, the federated learning paradigm enables all edge devices, such as a hospital server, a school-based monitoring hub, or a home gateway of a caregiver to locally train a local model with local data. Only the model updates (weights and gradients) are exchanged with the central aggregator and not the actual data. This makes sure that the international pediatric data privacy rules such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union are strictly followed.

It is a privacy-saving architecture, which corresponds to the design philosophy outlined by Hasan et al. (2024) [4], who noted that the connected pediatric device should be capable of a sufficient level of customization, while remaining highly isolated regarding data to ensure that caregivers have trust in it. Similarly, Islam (2024) [8] found that an AI security strategy based on data-centricity, where data is considered the object of protection instead of the system boundary, can eliminate cybersecurity threats to medical settings and environments in a significant way. The system allows global learning among distributed nodes, thus striking a very important balance between data utility and preservation of privacy by integrating federated mechanisms in the DCCDM so that identifiable patient information does not leak.

Moreover, the decentralized governance structure realizes the dimension of Measure and Manage of the NIST AI Risk Management Framework (AI RMF) offered by Hussain et al. (2024) [5]. The "Measure" functionality is achieved by performing ongoing monitoring of model performance indicators, that is, false-alarm rates, anomaly scores and response latency on each federated node. These measures are automatically compiled in real-time and presented in the form of an interactive governance dashboard. The Manage capability, in turn, implies the automated reaction to the incidents and policy adjustment according to the changing threat environment. As an illustration, upon an anomalous pattern detection, the system will activate predetermined risk-reduction mechanisms, including network-segmentation, model-retraining, or key-rotation of an encryption key. This feature can enhance technical resilience, as well as meet compliance obligations of persistent AI assurance, as indicated in the AI RMF guidance.

Data-centric encryption and human-centered oversight mechanisms are also included in the DCCDM and such mechanisms guarantee that its defensive mechanisms can also be transparent and easy to interpret, clinically. The model design is based on the principles of the Human-Centered AI (HCAI) developed by Islam et al. (2023) [6], where explainability, collaboration with clinicians, and accountability to the context are the primary considerations. The governance dashboard, which can be viewed by IT administrators and healthcare specialists, offers real time visualization of identified anomalies, the possible factors of their impact, their origin device and their risk rates. This openness will help clinicians and caregivers to comprehend not only what the system has identified, but the motivation behind the flagging of the event, to provide the bridge between algorithmic decisions and human decisions as to why the event was identified.

In addition, the collaborative visualization ecosystem fosters shared accountability when dealing with cybersecurity, with caregivers and IT staff having shared control over risks instead of depending on the technical staff exclusively. As an example, in the case of an anomaly coming in as a behavioral monitoring device in the home setting of a child, the caregivers get contextual alerts that they use to ensure that the device is functional before it escalates. This collaboration model can be likened to the framework of a trustworthy AI ecosystem that was suggested by Hussain et al. (2024) [5], and in which ethical co-governance and user empowerment are the primary pillars of sustainable AI use.

In addition to the security, the interpretability features of DCCDM are of clinical use. Multi-modal data streams (physiological, behavioral, environmental) are commonly found in pediatric IoMT data streams whose interdependence can detect distress or malfunction. The system also allows medical professionals to audit decisions during post-event analysis by providing explainable paths of decisions, mitigating the effects of false alarms and enhancing therapeutic decisions. This interpretability is consistent with the principles of Islam and Mim (2023) [7], who stated that data-driven explainability should be incorporated into precision medicine and AI systems to increase the confidence of clinicians and enable them to provide personalized patient care.

Essentially, the DCCDM reimagines cybersecurity in pediatric healthcare as a data-governance and human-collaboration issue, but not a technical issue. The adaptive reinforcement learning [1],[3], federated privacy preserving computation [4],[8], and NIST aligned governance [5],[6] combine to create a robust, ethically sound defense paradigm. It also improves real-time threat detection, regulatory compliance, and clinical interpretability- major pillars of credible AI in interrelated pediatric ecosystems.

Conclusion

This paper introduces a new Data-Centric Cyber-Defense Model (DCCDM) that is specific to connected pediatric Internet of Medical Things (IoMT) systems. The proposed model offers a safe, explainable, NIST AI Risk Management Framework (AI RMF)-compatible governance principles to create an interoperable and ethically-acceptable foundation of pediatric digital ecosystems through the lens of federated learning, reinforcement-based anomaly detection, and NIST AI Risk Management Framework (AI RMF)-conformant principles of governance. In contrast to the traditional signature-based intrusion detection systems, the DCCDM keeps evolving with changing data trends, which enables it to detect and recognize new cyber threat as well as keep abreast with new attack surfaces.

The experimental analysis provided that the DCCDM scored 94% on intrusion detection with a false-positive rate error being more than 50 percent and 20 percent lower latency efficiency than baseline models. These results confirm that data centric AI architecture not only increases defensive accuracy, but also boosts computational efficiency and scalability of the distributed clinical networks. With the federated mechanism of decentralizing the learning process, the model ensures that raw patient data remain on the node it originated, and will not be subject to privacy regulations (such as HIPAA and GDPR) and maintain model generalization among a variety of pediatric institutions.

In addition to technical performance, this study highlights the practical and ethical value of data-centric design in medical cybersecurity. In line with the principles of transparency, accountability, and human-in-the-loop oversight in the case of Hussain et al. (2024) [5] and Islam et al. (2023) [6], the model operationalizes transparency, accountability, and human-in-the-loop oversight with the help of the governance dashboard representing the visualization of the sources of anomaly, contributing

factors, and mitigation outcomes. This methodology expands the cybersecurity concept by making it a collective ethical endeavor of clinicians, caregivers, and the system administrators, and the gap between machine wisdom and clinical responsibility is narrowed.

The results confirm that data-centric AI can provide a viable and human-centric direction of the future generation of systems related to pediatric cybersecurity. The DCCDM will turn security monitoring into dynamic, trustful process by integrating constant learning and explainability through all layers of the defense architecture and making it able to support clinical decision-making.

In the future, the research will be scaled to multi-hospital IoMT networks and cross-institutional federated training to augment the robustness and contextual diversity of the system will be conducted. Further research will include application of reinforcement-based adaptive encryption whereby dynamical key assignment and learning-based encryption cycles will reduce vulnerability exposure more. lastly, audit trails based on blockchain integration will be explored to provide tamper-proof data lineage and end-to-end traceability to complete the transition of the framework to an intelligent defensive mechanism to an autonomous cyber-ethical infrastructure of the pediatric healthcare industry.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Islam MM, Hassan MM, Hasan MN, Islam S, Hussain AH. Reinforcement Learning Models for Anticipating Escalating Behaviors in Children with Autism. *J Int Crisis Risk Commun Res.* 2024;3225–3236.

[2] Islam S, Hussain AH, Islam MM, Hassan MM, Hasan MN. Cloud IoT Framework for Continuous Behavioral Tracking in Children with Autism. *J Int Crisis Risk Commun Res.* 2024;3517–3523.

[3] Hassan MM, Hasan MN, Islam S, Hussain AH, Islam MM. AI-Augmented Clinical Decision Support for Behavioral Escalation Management in Autism Spectrum Disorder. *J Int Crisis Risk Commun Res.* 2023;201–208.

[4] Hasan MN, Islam S, Hussain AH, Islam MM, Hassan MM. Personalized Health Monitoring of Autistic Children Through AI and IoT Integration. *J Int Crisis Risk Commun Res.* 2024;358–365.

[5] Hussain AH, Islam MM, Hassan MM, Hasan MN, Islam S. Operationalizing the NIST AI RMF for SMEs — Top National Priority (AI Safety). *J Int Crisis Risk Commun Res.* 2024;2555–2564.

[6] Islam MM, Arif MAH, Hussain AH, Raihena SMS, Rashaq M, Mariam QR. Human-Centered AI for Workforce and Health Integration: Advancing Trustworthy Clinical Decisions. *J Neonatal Surg.* 2023;12(1):89–95.

[7] Islam MM, Mim SS. Precision Medicine and AI: How AI Can Enable Personalized Medicine Through Data-Driven Insights and Targeted Therapeutics. *Int J Recent Innov Trends Comput Commun.* 2023;11(11):1267–1276.

[8] Islam MM. Data-Centric AI Approaches to Mitigate Cyber Threats in Connected Medical Device. *Int J Intell Syst Appl Eng.* 2024;12(17s):1049–1057.