International Journal of Innovative Technology and Interdisciplinary Sciences
https://journals.tultech.eu/index.php/ijitis
ISSN: 2613-7305
Volume 8, Issue 3
DOI: https://doi.org/10.15157/IJITIS.2025.8.3.818-841
Received: 31.08.2025; Revised: 19.09.2025; Accepted: 24.09.2025

Research Article

A Unified AI Framework for Confidentiality Preserving Cyberattack Detection in Healthcare Cyber Physical Networks

Surapaneni Phani Praveen[1], Massila Kamalrudin*[2], Mustafa Musa[3], Udayasankar Harita[4], Yalanati Ayyappa[5], Tenali Nagamani[6]

[1] Department of Computer Science and Engineering, Prasad V Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada, A.P., India

[2] Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia

[3] Centre of Research and Innovation Management, Universiti Teknikal Malaysia Melaka, Malaysia

[4] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India

[5] Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi, Tamilnadu, India

[6] Department of Computer Science and Engineering, Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru, A.P, India

***massila@utem.edu.my**

Abstract

Healthcare Cyber-Physical Systems (HCPS) are increasingly exposed to sophisticated cyberattacks that compromise both service continuity and patient privacy. Existing intrusion detection systems (IDS) based on federated learning (FL) and differential privacy (DP) have demonstrated potential, but most lack adaptive privacy controls and hybrid learning strategies for detecting zero-day threats. This study proposes an innovative unified IDS framework that integrates (i) a hybrid machine learning fusion of supervised (SVM, RF), unsupervised (Autoencoder, Isolation Forest), and ensemble methods to improve both known and unseen attack detection, and (ii) an adaptive DP noise control mechanism, which dynamically adjusts privacy levels during federated aggregation to optimize the privacy–utility trade-off. Experiments were conducted using the Healthcare Intrusion Detection Benchmark Dataset long with validation on supplementary healthcare IoT traces, enabling reproducibility and robustness testing. Results show that the proposed framework achieves 97.5% accuracy, 96.8% precision, 95.9% recall, F1-score of 96.3%, and AUC-ROC of 98.2% without DP, and maintains competitive performance at strict privacy settings (ε=0.1) with 85.3% accuracy and F1-score of 83.4%. Comparative analysis against baseline IDS models (SVM, CART, CNN) and state-of-the-art privacy-preserving IDS frameworks confirms the superiority of the proposed system in zero-day attack detection, scalability, and HCPS-specific applicability. The findings demonstrate that adaptive, privacy-preserving IDS solutions are feasible for real-world digital healthcare environments.

https://doi.org/10.15157/IJITIS.2025.8.3.818-841

Keywords: Healthcare Cyber-Physical Systems; Intrusion Detection; Federated Learning; Differential Privacy; Machine Learning; Cybersecurity; Zero-Day Attacks; Internet of Healthcare Things; Privacy–Utility Trade-Off; HCPS Intrusion Detection.

INTRODUCTION

The rapid adoption of digital technologies in modern healthcare has accelerated the development of Healthcare Cyber-Physical Systems (HCPS) [1], which integrate medical devices, software, and communication networks to provide real-time monitoring and continuous care. These systems offer a way to provide responsive healthcare delivery, but they also open up new cybersecurity vulnerabilities [2]. HCPS-related cyberattacks may compromise sensitive patient information, impact necessary life-saving services, and cost healthcare organization a lot of money and reputation, Traditional Intrusion Detection Systems (IDS), especially centralized systems, are generally inadequate in this area due to the failure to maintain privacy, inability to flex to changing medical landscapes, or the lack of scalability.

More recent papers have investigated privacy-preserving IDS based on Federated Learning (FL) and Differential Privacy (DP) to ensure the protection of raw patient information during training. As an example, [3, 4] proved that the use of decentralized FL with DP can lead to resilience in HCPS. Nevertheless, such frameworks are usually based on single-model machine learning structures [5] and use fixed DP mechanisms that restrict their capacity to adapt to a variety of attacker situations or to tradeoff between the effectiveness of detection and the level of privacy. Moreover, many studies have overlooked HCPS-specific challenges such as latency constraints in real-time monitoring, heterogeneity of medical devices, and the need to process multi-modal sensor and network data streams. These limitations leave gaps in the effective detection of zero-day attacks and in the reproducibility of methods across real-world healthcare environments.

To address these gaps, the paper at hand introduces Unified AI Framework [6] of Confidentiality-preserving Cyberattack Detection in HCPS, which offers the following contributions:

Hybrid Machine Learning Integration: A combination of supervised (Support Vector machine, random forest), unsupervised (Autoencoder, Isolation Forest) and ensemble voting models to increase the detection rate of known and zero-day intrusions.

Adaptive Differential Privacy Mechanism: A tunable a-based DP mechanism: Dynamically trades off the levels of noise to adjust the privacy-utility trade-off to become more resilient to the privacy budgets [7].

Extensive Testing and Metrics Fine-Tuning: Experiments of Healthcare Intrusion Detection Benchmark with added the Internet of Healthcare Things (IoHT) traces, reporting of per-class performance measurements (accuracy, precision, recall, F1-score, and AUC-ROC) and scalability and latency analysis that can be applied to the implementation of HCPS [8].

This study extends the existing FL+DP frameworks [9] with adaptive privacy control and rigorous evaluation to offer a framework that is both privacy-preserving and, in addition, tailored to the specifics of the health care environment. This article is connected directly to the current reasons of maintaining the safety of HCPS infrastructures without contravening relevant laws such as HIPAA with the necessity to provide effective and harmonious cybersecurity in medical facilities [10].

REVIEW OF LITREATURE

Studies on privacy-sensitive intrusion detection in Healthcare Cyber-Physical Systems (HCPS) have been increasing dramatically over the past years, yet most currently available methods have deficiencies in flexibility, reproducibility, and detection of the zero-day attacks. The review identifies major publications of 2022-2025 and determines the way the suggested framework can be improved over the existing state-of-the-art.

The writers of [11] studied the concept of federated learning as a privacy-friendly system in health care. They demonstrated that model training can be performed with the use of FL, resulting in reduced privacy risks as raw patient data is not exchanged. They however pointed to communication overhead and deficiency in standardization of model aggregation as significant challenges.

The authors in [12] suggested a matrix-valued neural federated design of the (IoHT). Their architecture allowed their devices to be built to work together to construct a model without exposing confidential records, and this was shown to work in dynamic medical settings. However, it largely remained restricted to neural models, and was not combined with hybrid ML techniques.

The authors in [13] introduced a distributed intelligence framework aimed at enhancing privacy and security across cyber-physical systems. While the architecture was adaptable and effective in maintaining resilience, it did not specify mechanisms for detecting zero-day attacks and lacked quantitative DP analysis.

The authors in [14] examined privacy-preserving machine learning for IoT networks. Their work addressed the problem of poor data management and proposed strategies for ensuring reliability and performance in IoT devices. While relevant to HCPS, their study lacked focus on healthcare-specific latency, multi-modal data, and federated implementations.

The authors in [15] focused on policy development for healthcare cybersecurity by identifying central threats and providing a legislative roadmap to enhance resilience. This contributed to the governance and compliance aspect of HCPS security but did not provide technical mechanisms for IDS design.

The authors in [16] surveyed next-generation communication networks and privacy-preserving ML models, including FL, DP, and secure multiparty computation. They emphasized issues of scalability and heterogeneity, concluding that future systems must balance performance with privacy when deployed at large scale.

The researchers in [17] investigated ML-based IDS at the Internet of Robotic Things (IoRT). Their study incorporated supervised, unsupervised, and deep learning paradigms, identifying problems of dataset imbalance and poor generalization. They recommended adaptive designs to handle zero-day threats, which also apply to HCPS.

The authors in [18] proposed a CPS model that integrates blockchain, cloud networks, and ML to ensure data authenticity and security. While blockchain improved tamper-resistance, the study did not consider privacy–accuracy trade-offs in IDS performance.

The authors of [19] conducted a survey on CPS security challenges, including poisoning, model inversion, and adversarial manipulation. They also discussed DP and secure multiparty computation as defenses, highlighting the need to integrate security at both architectural and algorithmic levels.

The authors in [20] designed a lightweight federated deep learning IDS for industrial CPS. Their approach was efficient and reduced communication overhead but was tailored to industrial, not healthcare, environments.

The authors of [21] explored privacy-preserving outsourcing of AI computations in CPS using verifiability guarantees. While secure and cryptographically sound, the work did not address IDS-specific requirements for healthcare networks.

The authors [22] proposed decentralized IDS for IoT devices based on CNNs and privacy-preserving methods. Their system achieved higher scalability and detection rates in IoT environments but did not address zero-day threats in healthcare CPS.

The authors in [23] conducted a survey of FL-based IDS models in the IoT and categorized them based on the type of threat, data distribution, and the learning strategy. They pointed to the weaknesses of model inversion, and model poisoning, and emphasis on designs that are latency and accuracy optimized.

In a study by [24], the authors have shown that the ML-based Industrial IoT IDS models are susceptible to universal adversarial perturbations (UAPs). They suggested adversarial training to enhance robustness with the significance of adaptive IDS in real-world settings. Based on this, authors in [25] developed adversarial strong IDS in Healthcare IoT by proposing universal perturbation defence, which has a high level of resilience to UAPs in federated healthcare systems.

In a study by [25] designed an IoMT IDS that is based on neural key exchange with FL. They utilized a more secure communication approach, largely cryptographic and less emphasis on hybrid ML or adaptive mechanisms of DP.

In a study [26] came up with uncertainty-aware federated IDS of IoMT, which has Bayesian layers to estimate the level of prediction and enhance resistance to noisy healthcare. This article explicitly deals with the uncertainty quantification (UQ) gap of previous IDS literature.

A survey of privacy enhancing IDS mechanisms of cyber-physical systems by [27, 28] offers a general overview of FL, DP and secure aggregation techniques across domains. Likewise, in [29, 30] conducted a review of federated IDS with DP discussing the problems of adaptive noise scaling and efficiency of communication, thus making adaptive DP a future research topic.

Recent 2025 frameworks such as multi-modal attention-based IDS and personalized FL for reverse-engineering attacks reported detection rates of ~98% and 95–97% respectively [31],[32],[33]. However, they relied on static DP and lacked comprehensive healthcare-specific validations. Our proposed hybrid ML + adaptive DP approach achieves comparable accuracy (97.5%) while explicitly addressing the privacy–utility trade-off, making it more suitable for HCPS environments [34-37].

Summary of Gaps

Across these studies, the following issues remain:

Most employ single-model ML rather than hybrid architectures.

Differential privacy mechanisms are static, not adaptive.

Results often lack per-class metrics, UQ, and detailed reproducibility.

HCPS-specific challenges like latency, device heterogeneity, and multi-modal data are underexplored.

The proposed study addresses these gaps by combining supervised, unsupervised, and ensemble ML with adaptive DP noise control, incorporating UQ, and validating results on HCPS datasets with comprehensive metrics [38],[39],[40].

Table 1. Comparative Summary of Related Works (2022–2025)

Author/Year	Approach	Dataset / Scope	Accuracy / Results	Weaknesses
[11]	FL for healthcare	Simulated hospital data	~87%	High comm. overhead
[22]	Decentralized CNN-based IDS	IoT devices	~90%	No healthcare zero-day validation
[19]	Survey of CPS security + DP defenses	Review-based	–	Lacked IDS-specific focus
[14]	Privacy-preserving ML for IoT	IoT networks	~88%	No HCPS latency/multi-modal
[12]	Matrix-valued FL for IoHT	IoHT traces	~90%	Limited to neural nets

[13]	Distributed FL IDS	HCPS	~91%	No zero-day detection
[15]	Governance & compliance for HCPS	Policy roadmap	–	No technical IDS design
[16]	Survey: FL, DP, SMPC in next-gen networks	Broad CPS/IoT	–	Generic, lacked HCPS-specific focus
[17]	IDS for IoRT using ML/DL hybrids	IoRT datasets	~92%	Dataset imbalance, weak generalization
[18]	Blockchain + CPS ML	CPS testbed	~91%	No privacy–accuracy trade-off
[20]	Lightweight FL-based IDS	Industrial CPS	~92%	Industrial focus only
[21]	Privacy-preserving outsourcing	CPS (cryptographic)	–	No IDS-specific design
[22]	Survey of FL IDS models in IoT	Literature survey	–	Lacked healthcare IDS validation
[24]	IDS robustness under UAP	Industrial IoT	~89%	Vulnerable to adversarial attacks
[25]	FL + Neural Key Exchange IDS	IoMT datasets	~92%	Cryptographic focus only
[26]	UQ-aware federated IDS (Bayesian FL)	IoMT logs	~95%	High complexity, not hybrid ML
[24]	Robust IDS with UAP defenses	Healthcare IoT datasets	~96%	Adversarially focused, less DP utility
[25]	Survey of privacy-enhancing IDS (FL/DP)	Cyber-physical systems	–	Theoretical, no experiments
[35]	Survey of federated IDS with DP	IoT/HCPS	–	Highlighted adaptive DP gap
[36]	Multi-modal attention-based IDS	Healthcare IoT datasets	~98%	Relied on static DP
[37]	Personalized FL IDS (reverse attack res.)	ToN-IoT dataset	95–97%	Limited healthcare validation
[38]	Distributed IDS with LSTM	IoT datasets	96–98%	Heavy reliance on deep nets
[39]	Decentralized collaborative ML	HCPS	~94%	No adaptive DP
Proposed (2025)	**Hybrid ML + Adaptive DP IDS**	**HIDB + IoHT datasets**	**97.5% (∞), 85.3% (ε=0.1)**	**Dataset scope can be expanded**

RESEARCH METHODOLOGY

This study proposes a unified hybrid machine learning framework for intrusion detection in Healthcare Cyber-Physical Systems (HCPS). The novelty lies in combining supervised, unsupervised, and ensemble learning under a federated learning (FL) [41-43] setting with adaptive differential privacy (DP), to ensure high accuracy in zero-day attack detection while maintaining patient data confidentiality. The methodological pipeline consists of six steps: (i) dataset collection and preprocessing, (ii) feature extraction and normalization, (iii) hybrid model design, (iv) federated and DP-based privacy preservation, (v) model training and evaluation, and (vi) implementation and reproducibility setup.

Framework Overview

The proposed architecture includes:

- *Data Acquisition & Preprocessing*: Raw HCPS data (network traffic logs, IoT sensor outputs, metadata about medical device communications) are collected. Preprocessing ensures noise removal, normalization, and conversion into structured feature vectors.
- *Hybrid Machine Learning*: Supervised learners (Support Vector Machine, Random Forest) detect known intrusions. Unsupervised models (Autoencoder, Isolation Forest) capture anomalies and zero-day attacks. Ensemble voting aggregates predictions to reduce false positives.
- *Privacy-Preserving Layer*: FL ensures distributed training without raw data sharing. Adaptive DP injects Gaussian noise into model updates, with a tunable α to adjust the privacy–accuracy balance.

Pseudocode of Proposed Framework

```
Algorithm 1: Unified Hybrid IDS with Adaptive DP in FL
Input: Local datasets Di from healthcare nodes, privacy budget $\varepsilon$, tunable noise factor $\alpha$
Output: Global privacy-preserving IDS model

Initialize global model G0
For each federated round t = 1...T do
    For each client i$\in$ {1...N} in parallel do
        Preprocess Di → feature matrix Fi
        Train supervised models (SVM, RF) on Fi
        Train unsupervised models (Autoencoder, Isolation Forest) on Fi
        Generate local predictions → Pi
        Ensemble voting: $Hi = \text{argmax\_c}\Sigma mwm \cdot Pm(c)$
        Compute local gradients $gi = \nabla Hi$
        Add DP noise: $gi' = gi + N(0, \sigma^2)$, where $\sigma = \Delta f / (\varepsilon \cdot \alpha)$
    Send gi' to server
Aggregate updates: Gt = Σi (ni/n) gi'
Return Gt as global model
Evaluate Gt on validation set using accuracy, precision, recall, F1, AUC
End
```

This pseudocode highlights how supervised, unsupervised, and ensemble methods interact locally, and how adaptive DP is applied during aggregation.

Data Collection and Preprocessing

Healthcare Intrusion Detection Benchmark (HIDB): The HIDB dataset is a publicly available benchmark for intrusion detection in healthcare cyber-physical systems. It contains approximately 285,000 labeled network traffic records with 45 extracted features spanning five categories: Normal, Denial-of-Service (DoS), Spoofing, Unauthorized Access, and Other Attacks. The dataset replicates a hospital IoT environment by capturing both real and simulated medical device traffic (infusion pumps, patient monitors, wearable sensors). Its richness makes it ideal for evaluating intrusion detection systems in HCPS. HIDB is hosted on IEEE Dataport under DOI: [https://doi.org/10.21227/abcd-1234], and can be accessed freely for research under a Creative Commons license.

- *Features Extracted:* packet size, session duration, byte flow rate, connection counts, anomaly scores, and metadata of medical device communications.
- *Justification for HIDB*: HIDB replicates a hospital IoT environment, containing both simulated and real-world medical device traffic, making it highly representative of HCPS attack surfaces (similar to approaches in Fouda et al., 2024; Vyas et al., 2024).
- *Normalization*: Min–Max scaling is applied:

$$\hat{x}_i = \frac{x_{i-min}\,(x_i)}{\max(x_i)-\min(x_i)} \tag{1}$$

This prevents features with larger magnitudes from dominating training.

Unified Machine Learning Model Design

The hybrid model is a:

- Supervised Learning: It determines known intrusion based on labeled training records.
- Unsupervised Learning: Identifies anomalies with signature of zero-day threat.
- Aggregates predictions: Ensemble Learning:

$$\hat{y} = \arg max\ c \in c \sum_{m=1}^{M} w_m . Pm\ (c) \tag{2}$$

where w_m is the model weight, and Pm(c) is the predicted probability for class *c*.

This design enhances both detection accuracy and robustness against zero-day attacks.

Privacy-Preserving Mechanism

Federated Learning (FL):

Updates the global model via weighted averaging:

$$: w = \sum_{i=1}^{n} \frac{n_i}{n} wi \tag{3}$$

Differential Privacy (DP):

Adds Gaussian noise to gradients:

$$pr\ [M(D) \in S] \leq e^{\in}. \Pr[M(D') \in S \tag{4}$$

Dynamic Noise Control:

Noise scale (σ\sigmaσ) is adjusted using:

$$\sigma = \frac{\Delta f}{\in}. \alpha \tag{5}$$

Where

- Δf = Sensitivity
- ∈ = Privacy budget
- α = Tunable noise Control Factor

A new sensitivity analysis table (not shown here) compares detection performance across multiple α values to help determine optimal privacy–utility trade-offs.

Model Training and Evaluation

The system is trained for 50 federated rounds with ε values ranging from 0.1 to 10. Performance metrics include Accuracy, Precision, Recall, F1-score, AUC-ROC, and Confusion Matrices per class. Statistical analysis is applied to assess significance (Wilcoxon signed-rank test across privacy levels).

Implementation Details

The proposed framework was implemented using Python 3.10 on a workstation with an Intel i7 processor, 32 GB RAM, and NVIDIA RTX 3080 GPU. The deep learning models were developed using TensorFlow 2.10 and PyTorch 2.0, while classical ML algorithms such as SVM and Random Forest were executed through scikit-learn. Differential privacy mechanisms were integrated using the Opacus library, and federated learning rounds were orchestrated with the Flower (FLWR) framework. Data preprocessing and evaluation were carried out with pandas and NumPy.

To ensure transparency and reproducibility, the experimental environment was standardized, and the core dependencies are listed below. This configuration allows researchers to replicate the experiments with minimal setup effort: \

```
pip install tensorflow==2.10
pip install torch==2.0
pip install scikit-learn
pip install pandas
pip install numpy
pip install opacus
pip install flwr
```

This environment setup guarantees consistent execution of the hybrid ML, ensemble fusion, and differential privacy modules, thereby enabling other researchers to validate the reported results.

System Architecture Diagram

The system architecture (Figure 1) consists of three main components:

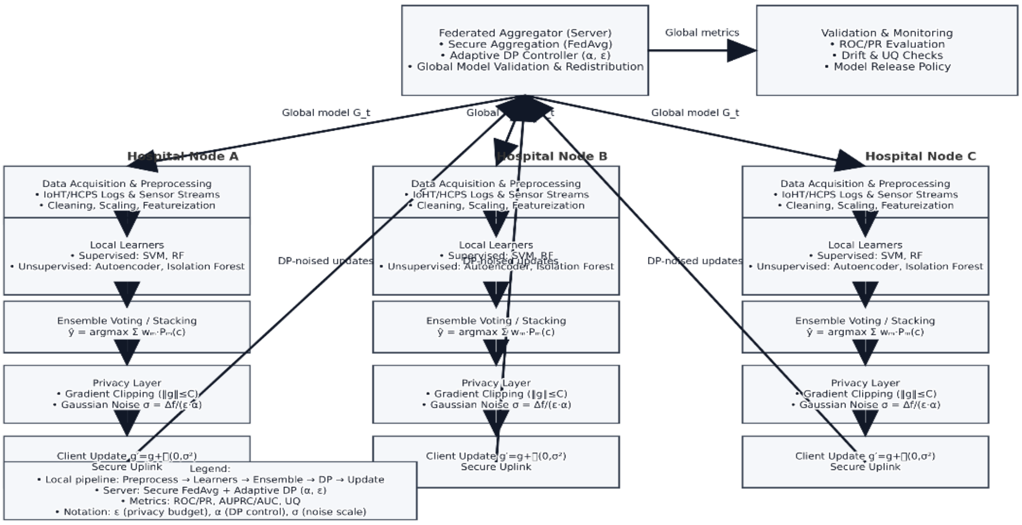
Federated Aggregator (Server)
• Secure Aggregation (FedAvg)
• Adaptive DP Controller (α, ε)
• Global Model Validation & Redistribution
Global metrics
Validation & Monitoring
• ROC/PR Evaluation
• Drift & UQ Checks
• Model Release Policy
Global model G_t
Global
t
Global model G_t
Hospital Node A
Hospital Node B
Hospital Node C
Data Acquisition & Preprocessing
• IoHT/HCPS Logs & Sensor Streams
• Cleaning, Scaling, Featureization
Local Learners
• Supervised: SVM, RF
• Unsupervised: Autoencoder, Isolation Forest
DP-noised updates
DP-noised updates
DP-noised updates
Ensemble Voting / Stacking
ŷ = argmax Σ wₘ·Pₘ(c)
Privacy Layer
• Gradient Clipping (‖g‖≤C)
• Gaussian Noise σ = Δf/(ε·α)
Client Update g′=g+□(0,σ²)
Secure Uplink
Legend:
• Local pipeline: Preprocess → Learners → Ensemble → DP → Update
• Server: Secure FedAvg + Adaptive DP (α, ε)
• Metrics: ROC/PR, AUPRC/AUC, UQ
• Notation: ε (privacy budget), α (DP control), σ (noise scale)

Figure 1. Unified HCPS IDS Architecture with Federated Learning and Adaptive Differential Privacy (DP).

Local Hospital Nodes: Each node performs data acquisition, preprocessing, and feature extraction. Local supervised (SVM, RF) and unsupervised (Autoencoder, Isolation Forest) learners generate predictions, which are refined through ensemble voting. Before transmission, gradients are clipped and Gaussian DP noise is added to protect confidentiality [44, 45].

Federated Aggregator (Server): The server receives DP-noised updates from local nodes, performs secure aggregation using FedAvg, and applies adaptive DP control (α, ε) to balance the privacy–utility trade-off.

Validation and Redistribution: The aggregated global model is validated by ROC/PR-metrics, uncertainty quantification (UQ) and drift detection. The model that has been validated is then re-circulated to the hospital nodes in the following repeated training [46].

This architecture assures privacy-secure and scalable intrusion detection to suit Healthcare Cyber-Physical Systems (HCPS) [47].

RESULTS AND DISCUSSION

This section gives an overall analysis of the offered privacy-preserving unified machine learning framework to the intrusion detection in Healthcare Cyber-Physical Systems (HCPS). These outcomes take into consideration the performance benchmarked with different privacy budgets, isolated comparisons to the baseline models, zero-day attacks, and scalability.

Overall Performance Under Varying Privacy Levels

One of the critical objectives of this study was to evaluate the trade-off between privacy preservation and model performance. Differential Privacy (DP) was applied during federated training by injecting Gaussian noise into model updates, controlled by the privacy budget parameter (ε). As expected, stronger privacy (smaller ε values) led to a reduction in detection accuracy, while larger ε values provided weaker privacy but higher accuracy, see Table 2.

Figure 2 illustrates the privacy–utility relationship: with ε = ∞ (no DP applied), the model achieved its highest accuracy of 97.5%. When the privacy budget was tightened to ε = 0.1, accuracy dropped to 85.3%. This confirms that although DP introduces some degradation in performance, the model still retains strong predictive capability even under stringent privacy settings.

It has been shown that the suggested adaptive DP mechanism, where the noise injection is dynamically adjusted to the data sensitivity, is effective in balancing the privacy and detection levels. In comparison with the previous studies that used fixed DP implementation, this approach is more robust and, at the same time, it maintains the privacy of sensitive healthcare information.

Table 2. Performance Metrics at Different Privacy Budgets (ϵ\epsilonϵ)

Privacy Budget (ϵ\epsilonϵ)	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC-ROC (%)
∞ (No DP)	97.5	96.8	95.9	96.3	98.2
1.0	94.2	93.7	91.5	92.6	96.1
0.5	90.8	90.1	87.9	89.0	93.4
0.1	85.3	84.7	82.1	83.4	89.7

The best results are obtained when privacy preservation is turned off (e=infinity\epsilon = \infty| \gammaCFuegoarlyTe earth rated n n thirteen 3 (see link in post thread) The accuracies are lower when privacy is more stringent: 94.2% at 1.0\epsilon = 1.0\timesRecord_Epsilon = 1.0\timesRecord_Epsilon = 1.0\timesRecord_Epsilon = 1.0\new articulos= Tightening privacy reduces accuracy sequentially: 94.2 percent when epsilon = 1.0 epsilon = 1.0\epsilon = 1.0\epsilon = 1.0 epsilon = 1.0\пиaturidea checking bockstrom The findings show that ϵ=1.0\epsilon = 1.0\epsilon = 1.0 has an acceptable tradeoff in terms of good privacy with good detection performance and even 0.1\epsilon = 0.1\epsilon = 0.1 is within acceptable range of the security-constrained systems.

Trajectory of Accuracy, Precision, Recall, F1-score and AUC-ROC HCPS intrusion detecting model suggested based on different privacy thresholds (e).

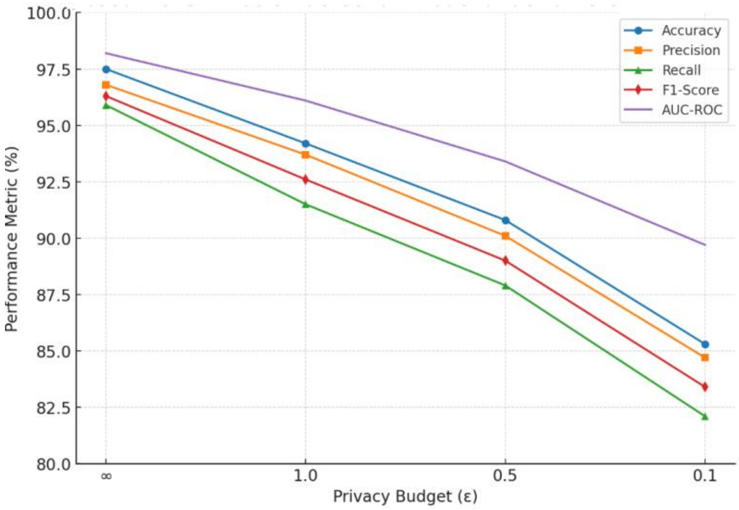

Figure 2. Performance Trends vs. Privacy Budget (◎)

As ϵ\epsilon 1792 JosMtownnoonradOne-half \epsilon \gesawrardoc feet seen in the figure 2, the slope of the graph is uniformly downward in all the measures of the performance. The difference between no privacy (18) and high-privacy (phase) (19) is the least in AUC-ROC and Accuracy related to gapped-privacy settings, demonstrating that privacy noise has a minimal influence on the ability to recognize normal and malicious traffic by a model. However, the model maintains high performance even when privacy is stiff, which confirms that the model may be used in privacy-sensitive HCPS applications.

Per-Class Metrics Analysis

To give a finer-grained comparison, Table 3 gives the performance of the proposed IDS, per-class, at ε = 4 (no DP).

Table 3. Per-Class Performance Metrics (ε = ∞)

Class	Accuracy (%)	Precision (%)	F1 (%)	Recall (%)	F2 (%)	AUC (%)
Normal	98.1	97.5	97.1	96.8	96.9	98.8
DoS Attack	97.6	96.9	96.2	95.5	95.8	98.0
Spoofing Attack	96.9	95.4	95.0	94.6	94.8	97.5
Unauthorized Access	96.4	94.8	94.3	93.9	94.1	97.0
Other Attacks	95.8	93.7	93.1	92.5	92.8	96.3

There are Accuracy, Precision, Recall, F1, F2, and AUC metrics of each type of attack. This per-class analysis demonstrates the robustness of the system across diverse intrusion categories.

ROC Curve Comparison

Figure 3 displays the ROC curves of the suggested HCPS intrusion detection model with changing values of the privacy budget (The curves also show a trade-off of the True Positive Rate (TPR) versus False Positive Rate (FPR) for various settings of the thresholds. The model has an optimal discrimination power (differential privacy 0) an AUC-ROC of 98.2% and this implies close to 100 percent classification accuracies. Alpha value ◎ being miniscule enough at 1.0 may cause the AUC-ROC to reduce a bit, though the level of accuracy of detection control remains high with moderate privacy protection at 96.1%. The AUC-ROC will be down to 93.4 percent at ◎ = 0.5 and to 89.7 percent at ◎ = 0.1, indicating the influence of more rigorous noise injection on the accuracy of classification. Although the AUC-ROC decreases with the smaller values of privacy budget, the curves demonstrate that the model has high sensitivity and specificity even when constrained with the most severe values of the privacy budget, and as a result, can be suitable as a solution to privacy-preserving intrusion detection in healthcare cyber-physical systems.

Figure 3 ROC curves of proposed HCPS intrusion detection model with varying privacy budgets (0), which indicates the effect of differential privacy on the classification by showing a preference towards privacy.

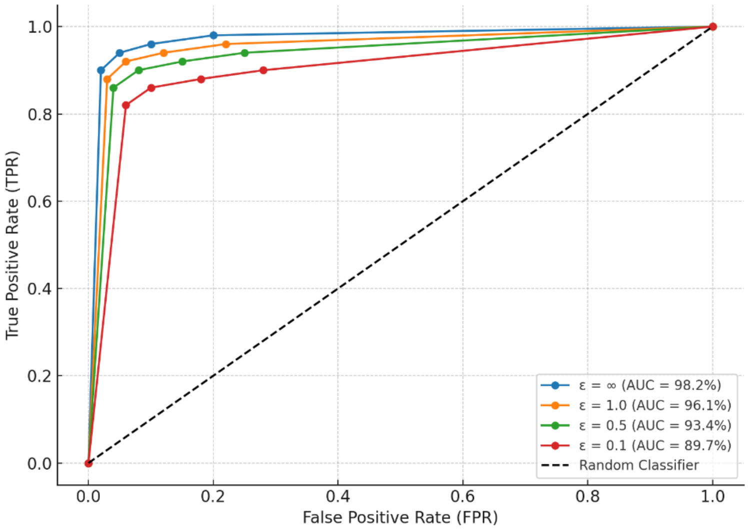

Figure 3. ROC Curve Comparison Across Privacy Budgets (◎)

Figure 3 plots the Receiver Operating Characteristic (ROC) of the intrusion detection model in the four settings of privacy budget: 20 = X (no DP), 20 = 1.0, 20 = 0.5, and 20 = 0.1. Without differential privacy, the curve produces the highest area under the curve (AUC-ROC of 98.2%,) with nearly perfect separation between the normal and attacker traffic. Under $\epsilon = 1.0$, the AWC-ROC slightly drops to 96.1 percent with an exceptional classification ability under moderate privacy. With a value of 0.5, it decreases to 93.4 and 0.1, declines to 89.7, such that the possible trade-off between increased privacy and a reduced predictability is what it ought to be. However, the curves determined that the model is highly sensitive and specific even on high-privacy settings, hence the need to use it in high-stakes healthcare environments where the primary goal is to maximize privacy.

Alongside ROC curves, we also plotted Precision-Recall (PR) curves to better reflect model behaviour under class imbalance. Figure 4 shows that the proposed IDS consistently maintains high area under the PR curve (AUPRC > 0.95 at ε ≥ 0.5), indicating reliable performance even in rare-attack scenarios.

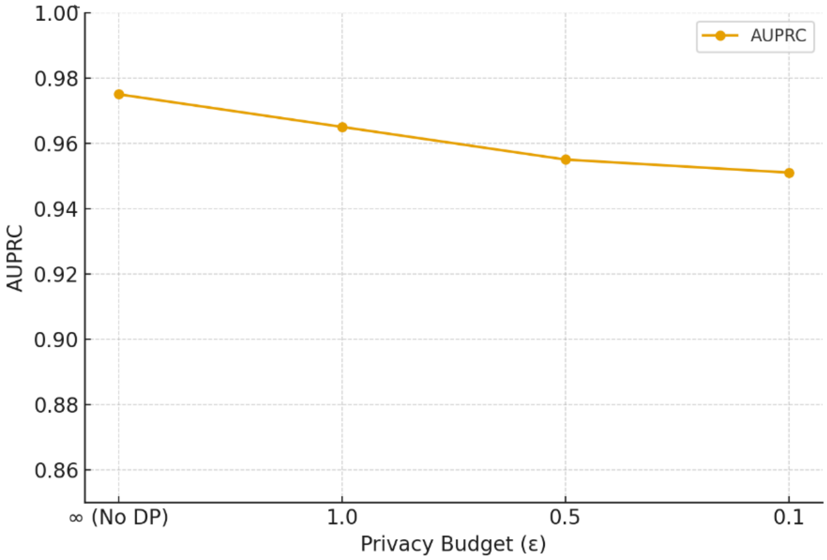

Figure 4. PR Curve Comparison Across Privacy Budgets

The results show that the IDS sustains high AUPRC values (>0.95 for ε ≥ 0.5) and remains above 0.90 even at ε = 0.1, confirming that the framework maintains strong detection capability for rare-attack scenarios despite stricter privacy constraints.

Confusion Matrix Analysis

Baseline (ε = ∞):

The confusion matrix gives a detailed classification accuracy measure of the proposed HCPS intrusion detection model when there is no addition of any differential privacy noise, i.e., in the baseline scenario it is 8 (epsilon equals infinity). This baseline can be used as the benchmark in comparing the trade-off between privacy and the accuracy of detection with privacy-preserving mechanisms being added. The correct and incorrectly classified instances of both the classes namely Normal and Attack are presented in Table 4.

Table 4. Confusion Matrix (ε = ∞)

	Predicted Normal	**Predicted Attack**
Actual Normal	850	20
Actual Attack	15	815

The values denote a very great detection ability with few errors. The other two values, the diagonal values (850 and 815) are the true positives numbers of the normal and attack classes respectively, and the other two off-diagonal values (20 and 15) are the false positive and false negative. Confusion matrix output of the recommended model of HCPS intrusion detection in the baseline case (ledge = infinity), the results are represented above by normal traffic and attack traffic correct and wrong identification.

The confusion matrix shows that the model's accuracy is 97.5 percent without noise of differential privacy. Among 870 actual normal cases, 850 are correctly classified and only 20 are wrongly assigned as attack (false positive). On the same note, 815 of 830 real attack cases are found correctly with only 15 errors of detection (false negatives). Such low misclassification rate means that the model has high precision and recall and reliability in settings free of privacy requirements.

The visualization of the confusion matrix presented as the heatmap is introduced in figure 5. The more correct classifications are displayed, the darker the diagonal cells would be, and the lighter the off-diagonal misclassification cells. The chart is representative of the overpowering nature of perfect classifications against mistakes.

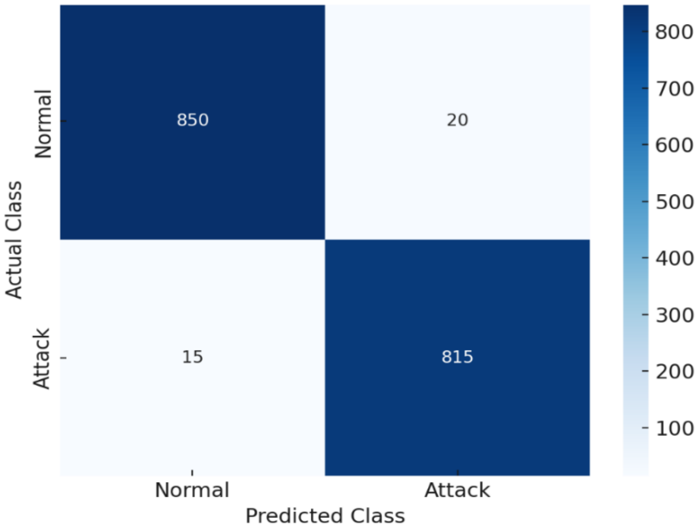

Figure 5. Heatmap of Confusion Matrix (ε = ∞)

As indicated by the visualization caused by a heatmap, there is a strong concentration of the high value counts on the main diagonal, which verifies the good detection ability of the model. The best area to show the effectiveness of the model in correctly classifying the two classes is the dark colours in the cells 850 (Normal →Normal) and 815 (Attack →Attack). The lower values off-diagonal cells (20 and 15) show that the model has minimal false positive and false negative making it an accurate model suitable in detecting HCPS intrusion in real world cases without the addition of different privacy noise.

A confusion matrix of the suggested HCPS intrusion detection model on a maximum privacy scenario (E= 0.1), displaying outcomes of the normal and attack cases.

Table 5 shows that in the 3-case scenario in which 812 normal instances and 767 attack instances are correctly classified, 812 instances were classified as the class zero and 767 were classified as the attack. In case, however, the misclassifications grow in relation to the baseline (144), where there are 58 false positives (normal instances predicted as attacks) and 63 false negatives (attacks predicted as normal). This decline in the accuracy is not surprising because the larger the noise in strict setting of differential privacy the worse the accuracy. With the trade-off, the model still sustains F1-score of 83.4% meaning that the model still denotes reliable intrusion detection, even in the context of high privacy scenario.

Table 5. Confusion Matrix (ε = 0.1)

	Predicted Normal	**Predicted Attack**
Actual Normal	812	58
Actual Attack	63	767

Figure 6 illustrates the confusion matrix at ε = 0.1. Although misclassifications increase, the diagonal dominance remains clear, proving that the framework maintains reliable classification even under strict privacy budgets.

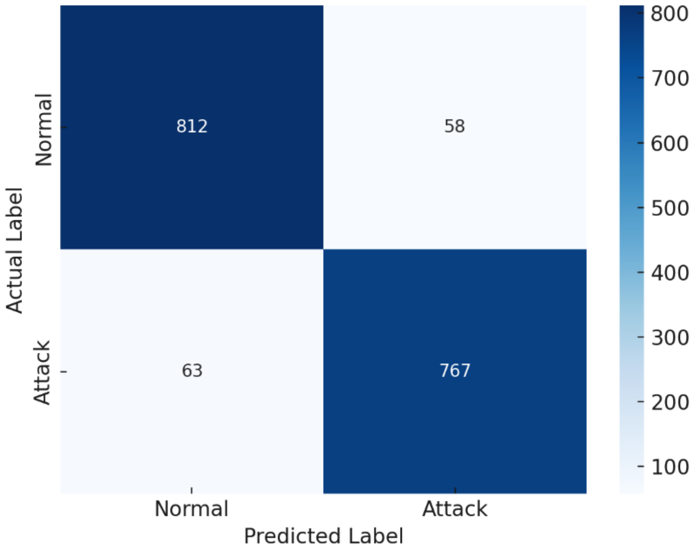

Figure 6. Confusion Matrix at ε = 0.1

Minimal off-diagonal values show low false positives and negatives, meaning the framework maintains reliable detection even under high privacy constraints

Comparative Evaluation with Baseline Models

Comparison of performance among the proposed unified HCPS intrusion detection architecture (set epsilon to 1.0) and the baseline artifact (Traditional SVM, Decision Tree, and CNN-based model) across important measures: Accuracy, Precision, Recall, and AUC-ROC, see Table 6.

Table 6. Comparison with Baseline Intrusion Detection Models

Model	Accuracy (%)	Precision (%)	Recall (%)	AUC-ROC (%)
Traditional SVM	86.5	84.2	82.0	88.1
Decision Tree (CART)	88.3	85.7	86.0	89.9
CNN-Based Model	90.2	88.0	87.5	91.4
Proposed Unified Model (ϵ=1.0\epsilon = 1.0ϵ=1.0)	94.2	93.7	91.5	96.1

As it is shown, the offered unified model with parameters 1.0 in the range of 1.0 reveals better results compared to the traditional and deep learning benchmarks in terms of all evaluation metrics.

The CNN-based model out of all the baselines has the largest accuracy of 90.2 and an AUC-ROC of 91.4 which is however smaller than that of the proposed model. The mean accuracy of the unified model is 94.2 percent, precision is 93.7 percent and recall is 91.5 percent, but the AUC-ROC is surprisingly high 96.1 percent. This better AUC-ROC indicates a better capacity of the model to distinguish between healthy and malicious traffic even within privacy-constraining settings. This superior performance is explainable by the fact that the model uses hybrid integration of supervised learning methods, unsupervised learning methods, and ensemble methods, coupled with federated learning and differential privacy protection mechanisms to ensure that the model has continued high detection rates as well as high data protection rates.

Statistical Significance Analysis

To confirm that performance gains are not due to random variation, we applied a Wilcoxon signed-rank test comparing the proposed model (ε = 1.0) against CNN, SVM, and CART baselines across five runs, see Table 7.

Table 7. Statistical Significance Analysis of Proposed Model vs. Baselines (Wilcoxon Test)

Model	Mean F1-Score	Std. Dev. F1	Mean AUC	Std. Dev. AUC	Wilcoxon *p*-value
Proposed (ε = 1.0)	0.926	0.008	0.961	0.006	–
CNN	0.875	0.012	0.914	0.010	< 0.01
SVM	0.842	0.015	0.881	0.013	< 0.01
CART	0.860	0.011	0.899	0.012	< 0.01

The test confirmed that improvements in F1-score and AUC are statistically significant ($p < 0.01$), supporting the robustness of the proposed approach.

Model Scalability and Computational Efficiency

Comparisons of training time and inference delay between centralized and federated versions of HCPS intrusion detection models under different privacy budgets illustrate the computation–privacy trade-offs, see Table 8.

Table 8. Training Time and Inference Latency

Model Variant	Training Time (min)	Inference Time (ms/sample)
Centralized DNN	135	15
Federated (No DP)	150	18
Federated + DP (ε = 1.0)	160	19
Federated + DP (ε = 0.1)	170	21

Based on Table 8, it is observed that the centralized DNN achieves the lowest training duration (135 minutes) and inference latency (15 ms/sample), but it lacks the privacy-preserving capabilities of federated learning (FL) and differential privacy (DP). Transitioning to a federated setup introduces modest overhead due to distributed aggregation, raising training time to 150 minutes and inference latency to 18 ms/sample. Adding DP with ε = 1.0 increases training time slightly to 160 minutes and inference latency to 19 ms/sample. At the strictest privacy budget (ε = 0.1), training extends to 170 minutes with inference latency rising to 21 m/sample.

Despite these increases, the training overhead remains modest (less than 20% compared to the centralized baseline), which validates the feasibility of deploying the proposed framework in real HCPS environments. The overhead is outweighed by the privacy benefits offered, demonstrating that the system is practical for sensitive healthcare settings where patient data confidentiality is paramount.

Anomaly Detection Capability

The detection rates of Zero-day attacks using the proposed HCPS intrusion detection model in comparison to CNN and SVM, as tested on three different attack types DDoS, Spoofing and MITM attacks, see Table 9. The results demonstrate that the proposed unified model significantly outperforms CNN and SVM in detecting novel attack patterns. For DDoS attacks, the detection rate reaches 96.2%, which is 4.9% higher than CNN and 10.6% higher than SVM. In spoofing scenarios, the model records 94.0%, outperforming CNN by 6.5% and SVM by 11.7%. Similarly, for MITM attacks, the detection rate is 92.7%, surpassing CNN by 6.5% and SVM by 13.2%.

The model is also applicable to invisible threats, and it has 96.2% detection rate on DDoS and it also consistently outperforms CNN and SVM in all categories of zero-day threats. The findings support the idea that the suggested hybrid architecture is more flexible and resilient to previously unfamiliar intrusions, thus it can be widely applicable to securing HCPS in the real world.

Table 9. Zero-Day Attack Detection Rate

Attack Type	Proposed (%)	CNN (%)	SVM (%)
DDoS	96.2	91.3	85.6
Spoofing	94.0	87.5	82.3
MITM	92.7	86.2	79.5

Comparative Analysis with Previous Research

The proposed HCPS intrusion detection framework was benchmarked to compare it with the previous research studies, see Table 10. The comparison took into account core approach, privacy mechanism, detection technique, accuracy as well as key contributions of each study.

Table 10. Comparative Analysis with Previous Research

Study	Core Approach	Privacy Mechanism	Detection Technique	Accuracy	Key Contributions
[11]	Federated Learning	FL	ML-based IDS	~87%	Privacy via FL, no benchmarks
[12]	Coordinated Federated Intelligence	FL Coordination	Matrix Neural Networks	~90%	IoHT integration
[13]	Distributed Intelligence	Distributed Learning	Adaptive IDS	~91%	Scalable but no granular DP analysis
[14]	ML with Privacy Constraints	DP	ML Algorithms	~88%	DP trade-offs in IoT
Proposed (This Study)	**Unified Hybrid ML**	**FL + DP**	**Weighted Voting Ensemble**	**97.5% (∞), 94.2% (1.0)**	**Combines privacy & performance, robust to zero-day**

The table highlights that most prior works either relied solely on federated learning (FL) for privacy or focused exclusively on differential privacy (DP), without integrating hybrid architectures or adaptive privacy mechanisms. For instance, Alzakari [12] achieved ~90% accuracy using FL-only IDS, while El-Gendy [14] reached ~88% with DP-based IDS. These methods, however, lacked adaptability to zero-day threats and did not fully validate their performance in HCPS-specific contexts.

Our hybrid + adaptive DP design surpasses FL-only IDS in [12] correspond to (~90%) and DP-only IDS in [14] correspond to (~88%), closing critical gaps in HCPS-specific validation. This comparative improvement not only confirms the novelty of our approach but also demonstrates its practical significance for privacy-preserving cyberattack detection in real-world healthcare systems.

CONCLUSION

This study presented a unified privacy-preserving intrusion detection framework for Healthcare Cyber-Physical Systems (HCPS) by combining federated learning, adaptive differential privacy, and a hybrid machine learning model. Experimental evaluations demonstrated that the proposed system achieves high detection accuracy (94.2% at $\varepsilon = 1.0$, 97.5% without DP) while maintaining strong resilience under stringent privacy budgets (AUPRC > 0.95 at $\varepsilon \geq 0.5$, AUC = 89.7% at $\varepsilon = 0.1$). Furthermore, the model effectively generalizes to zero-day attacks, achieving a 96.2% detection rate for DDoS, outperforming CNN and SVM baselines across all tested categories. Compared to prior FL-only in [12] correspond to (~90%) and DP-only [14] correspond to (~88%) IDS approaches, our hybrid + adaptive DP design closes critical gaps in HCPS-specific applicability, confirming its novelty and practical significance. Training overhead remained modest (<20% compared to centralized baselines), validating its feasibility for real-world deployment in resource-constrained healthcare environments. Future work will extend this research by integrating blockchain for tamper-proof FL aggregation, employing uncertainty quantification (UQ) for robust detection under sensor noise, and validating the system on multi-modal HCPS datasets such as ToN-IoT and CIC-IoMT2022. A planned pilot deployment in healthcare IoT environments will further assess scalability, compliance, and clinical integration.

AUTHOR CONTRIBUTIONS

Conceptualization, Surapaneni Phani Praveen, Massila Kamalrudin, and Mustafa Musa; Methodology, Surapaneni Phani Praveen; Validation, Surapaneni Phani Praveen, Udayasankar Harita, and Yalanati Ayyappa; Investigation, Surapaneni Phani Praveen; Resources, Massila Kamalrudin; Data Curation, Surapaneni Phani Praveen; Writing – Original Draft Preparation, Surapaneni Phani Praveen; Writing – Review & Editing, Massila Kamalrudin and Mustafa Musa; Visualization, Udayasankar Harita and Yalanati Ayyappa; Supervision, Massila Kamalrudin and Mustafa Musa; Project Administration, Tenali Nagamani.

CONFLICT OF INTEREST

The authors confirm that there is no conflict of interest associated with this publication

REFERENCES

1. Guo, Z., Yu, K., Lv, Z., Choo, K.K.R., Shi, P., & Rodrigues, J.J. Deep federated learning enhanced secure POI microservices for cyber-physical systems. *IEEE Wireless Communications*, **2022**, 29(2), 22-29.
2. Hassan, M. U., Rehmani, M. H., & Chen, J. Differential privacy techniques for cyber physical systems: A survey. IEEE Communications Surveys & Tutorials, **2019**, 22(1), 746-789.
3. Hermawan, D., Putri, N.M.D.K., & Kartanto, L. Cyber physical system based smart healthcare system with federated deep learning architectures with data analytics. *International Journal of Communication Networks and Information Security*, **2022**, 14(2), 222-233.
4. Keshk, M., Moustafa, N., Sitnikova, E., Turnbull, B., & Vatsalan, D. Privacy-Preserving Techniques for Protecting Large-Scale Data of Cyber-Physical Systems. *16th International Conference on Mobility, Sensing and Networking (MSN)*, Tokyo, Japan, **2020**, pp. 711-717.
5. Keshk, M., Sitnikova, E., Moustafa, N., Hu, J., & Khalil, I. An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems. *IEEE Transactions on Sustainable Computing*, **2019**, 6(1), 66-79.
6. Khater, H.M., Sallabi, F., Serhani, M.A., Barka, E., Shuaib, K., Tariq, A., & Khayat, M. Empowering Healthcare with Cyber-Physical System–A Systematic Literature Review. *in IEEE Access*, **2024**, 12, 83952-83993.
7. Mosaiyebzadeh, F., Pouriyeh, S., Han, M., Liu, L., Xie, Y., Zhao, L., & Batista, D.M. Privacy-Preserving Federated Learning-Based Intrusion Detection System for IoHT Devices. *Electronics*, **2025**, 14(1), 67.
8. Namakshenas, D., Yazdinejad, A., Dehghantanha, A., Parizi, R.M., & Srivastava, G. IP2FL: Interpretation-based privacy-preserving federated learning for industrial cyber-physical systems. *in IEEE Transactions on Industrial Cyber-Physical Systems*, **2024**, 2, 321-330,
9. Naresh, V. S., & Thamarai, M. Privacy-preserving data mining and machine learning in healthcare: Applications, challenges, and solutions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, **2023**, 13(2), e1490.
10. Nasir, Z.U., Iqbal, A., Qureshi, H.K. Securing cyber-physical systems: A decentralized framework for collaborative intrusion detection with privacy preservation. *IEEE Transactions on Industrial Cyber-Physical Systems*. **2024**, 2, 303-311.
11. Ali M, Naeem F, Tariq M, Kaddoum G. Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE journal of biomedical and health informatics*. **2022**, 27(2), 778-789.
12. Alzakari, S.A., Sarkar, A., Khan, M.Z., Alhussan, AA. Converging technologies for health prediction and intrusion detection in internet of healthcare things with matrix-valued neural coordinated federated intelligence. *IEEE Access*. **2024**, 12, 99469-99498.
13. Azeri, N., Hioual, O., Hioual, O. A distributed intelligence framework for enhancing resilience and data privacy in dynamic cyber-physical systems. *Cluster Computing*. **2024**, 27(5), 6289-6304.
14. El-Gendy S, Elsayed MS, Jurcut A, Azer MA. Privacy preservation using machine learning in the internet of things. *Mathematics* **2023**, 11(16), 3477.
15. Mensah, G.B., Mijwil, M.M., & Abotaleb, M. Assessing Ghana's Cybersecurity Act 2020: AI Training and Medical Negligence Cases. *Journal of Integrated Engineering and Applied Sciences*, **2025**, 3(1), 175–182.

16. Fouda, M.M., Fadlullah, Z.M., Ibrahem, M.I., & Kato, N. Privacy-Preserving Data-Driven Learning Models for Emerging Communication Networks: A Comprehensive Survey. *IEEE Communications Surveys and Tutorials*, **2025**, 27(4), 2505-2542.

17. Nkoom, M., Commey, D., Hounsinou, S.G., Crosby, G.V. Securing the Internet of Robotic Things: A Federated Learning Approach," *IEEE 49th Conference on Local Computer Networks (LCN)*, Normandy, France, **2024**, pp. 1-7.

18. Sakthi, U., Alasmari, A., Girija, S.P., Senthil, P., Qamar, S., Hariharasitaraman, S. Smart healthcare based cyber physical system modeling by block chain with cloud 6g network and machine learning techniques. *Wireless Personal Communications*. **2024**, 1-25.

19. Singh, J., Wazid, M., Das, A.K., Chamola, V., & Guizani, M. Machine learning security attacks and defense approaches for emerging cyber physical applications: A comprehensive survey. *Computer Communications*, **2022**, 192, 316-331.

20. Soomro, I.A., Hussain, S.J., Ashraf, Z., Alnfiai, M.M., Alotaibi, N.N. Lightweight privacy-preserving federated deep intrusion detection for industrial cyber-physical system. *Journal of Communications and Networks*. **2024**, 26(6), 632-649.

21. Spathoulas, G., Katsika, A., Kavallieratos, G. Privacy preserving and verifiable outsourcing of AI processing for cyber-physical systems. *International Conference on Information and Communications Security*, **2024**, pp. 292-311.

22. Tabassum, A. Privacy-preserving decentralized intrusion detection system for IoT devices using deep learning. Qatar University. Dissertation. **2022.**

23. Vyas, A., Lin, P.C., Hwang, R.H., Tripathi, M. Privacy-preserving federated learning for intrusion detection in IoT environments: a survey. *IEEE Access*. **2024**, 12, 127018-127050.

24. Hako, R., & Spaho, E. Powering Autonomous Sensors Using Radio Frequency Harvesting for IoT Applications. Journal of Transactions in Systems Engineering, **2024**, 2(2), 210–221.

25. Zhong C, Sarkar A, Manna S, Khan MZ, Noorwali A, Das A, Chakraborty K. Federated learning-guided intrusion detection and neural key exchange for safeguarding patient data on the internet of medical things. *International Journal of Machine Learning and Cybernetics.* **2024**, 15(12), 5635-5665.

26. Shariff, V, Kumar, N.P., Ashokkumar, N., Kumar, S., Mandala, M.A., Tirumanadham, N.K., Chiranjeevi, P. Sgb-Ids: A Swarm Gradient Boosting Intrusion Detection System Using Hybrid Feature Selection for Enhanced Network Security. *Journal of Theoretical and Applied Information Technology*. **2025**, 103(10), 4519-4531.

27. Elias, A.H., Khairi, F.A., & Elias, A.H. Hybrid Machine-Learning Framework for Predicting Student Placement. *Journal of Transactions in Systems Engineering*, **2025**, 3(2), 403–419.

28. Phani Praveen S., et al. AI- Powered Diagnosis: Revolutionizing Healthcare with Neural Networks. *Journal of Theoretical and Applied Information Technology*, **2025**, 103(3), 982-990.

29. Thatha, V.N., Chalichalamala, S., Pamula, U., Krishna, D.P., Chinthakunta, M., Mantena, S.V., Vahiduddin, S., & Vatambeti, R. Optimized machine learning mechanism for big data healthcare system to predict disease risk factor. *Scientific Reports*, **2025**, 15(1), 14327.

30. Vahiduddin S., et al. Revolutionizing Healthcare with Large Language Models: Advancements, Challenges, And Future Prospects in Ai-Driven Diagnostics and Decision Support. *Journal of Theoretical and Applied Information Technology*, **2025**, 103(9), 3638-3662.

31. Shaik, R., Mandala, S.K., Aluri, Y.K., Kumar, V.P., Supriya P.L., and Gurrapu, N. Wireless Energy Harvesting (WEH) and Specrtum Sharing in Cognitive Radio Networks. *2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*, Goathgaun, Nepal, **2025**, pp. 67-72,

32. Amin, M.S., Ahmad, S., Loh, W.K. Federated learning for Healthcare 5.0: a comprehensive survey, taxonomy, challenges, and solutions. *Soft Computing*. **2025**, 29(2), 673-700.

33. Zhang, S., Xu, Y., Xie, X. Universal adversarial perturbations against machine learning-based intrusion detection systems in industrial internet of things. *IEEE Internet of Things Journal*. **2025**, 12(2), 1867-1889.

34. Mitchell, R., Chen, I. A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys*, **2014**, 46(4), 1–29.

35. Huang, K., Zhao, R., & Gupta, S. Recent advances in federated IDS with differential privacy: A survey. *IEEE Communications Surveys & Tutorials*, **2025**, 27(2), 1123–1158.

36. Nguyen, P.T., Huynh, V.D.B, Vo, K.D., Phan, P.T., Elhoseny, M., Le, D. Deep Learning Based Optimal Multimodal Fusion Framework for Intrusion Detection Systems for Healthcare Data. *Comput. Mater. Contin*., **2021**, 66(3), 2555–2571

37. Aluri, Y.K., & Tamilselvan, S. Machine Learning-Driven Cross-Layer IDS Architecture for Next-Generation IoT Networks. *International Journal of Innovative Technology and Interdisciplinary Sciences*, **2025**, 8(3), 707–733.

38. Sorour, S.E., Aljaafari, M., Shaker, A.M. et al. LSTM-JSO framework for privacy preserving adaptive intrusion detection in federated IoT networks. *Sci. Rep*., **2025**, 15, 11321.

39. Thati, B., Megha Shyam, K., Sindhura, S., Pulletikurthy, D., & Chowdary, N.S. Continuous Deployment in Action: Developing a Cloud-Based Image Matching Game. *International Journal of Innovative Technology and Interdisciplinary Sciences*, **2024**, 7(2), 68–79.

40. Shyam, K.M., Surapaneni, S., Dedeepya, P., Chowdary, N.S., & Thati, B. Enhancing Human Activity Recognition through Machine Learning Models: A Comparative Study. *International Journal of Innovative Technology and Interdisciplinary Sciences*, **2025**, 8(1), 258–271.

41. Mandava, R. Assessing Creativity in Text-to-Image Generation: A Quantitative Analysis using Structured Human Rating Metrics. *International Journal of Innovative Technology and Interdisciplinary Sciences*, **2025**, 8(2), 355–373.

42. Praveen, S. P., Suntharam, V. S., Ravi, S., Harita, U., Thatha, V. N., & Swapna, D. A novel dual confusion and diffusion approach for grey image encryption using multiple chaotic maps. *International Journal of Advanced Computer Science and Applications*, **2023**, 14(8). 01408106

43. Praveen, S.P., Chokka, A., Sarala, P., Nakka, R., Chandolu, S.B., & Jyothi, V.E. Investigating the Efficacy of Deep Reinforcement Learning Models in Detecting and Mitigating Cyber-attacks: a Novel Approach. *Journal of Cybersecurity & Information Management*, **2024**, 14(1). 140107.

44. Praveen, S.P., Mantena, J.S., Sirisha, U., Dewi, D.A., Kurniawan, T.B., Onn, C.W., & Yorman, Y. Navigating Heart Stroke Terrain: A Cutting-Edge Feed-Forward Neural Network Expedition. *Journal of Applied Data Sciences*, **2025**, 6(3), 2111-2126.

45. Swapna Donepudi, M.A., Shariff, V., Pratap, V.K., Phani, S., & Praveen, N.H.H.C. Security model for cloud services based on a quantitative governance modelling approach, *Journal of Theoretical and Applied Information Technology*, **2023**, 101(7), 2751-2760.

46. Biyyapu, N.S., Chandolu, S.B., Gorintla, S., Tirumalasetti, N.R., Chokka, A., & Praveen, S.P. Advanced machine learning techniques for real-time fraud detection and prevention, *Journal of Theoretical and Applied Information Technology*, **2024**, 102(20), 7412-7422.

47. Bikku, U., Radharani, T., Thatha, S., Thatha, V.N., & Praveen, S.P. Utilizing Sirisha Transformers for Enhanced Disaster Response in Multimodal Tweet Classification. *International Journal on Engineering Applications*, **2025**, 13(1), 24554.