Review

AI-Driven Hybrid Detection and Classification Framework for Secure Sleep Health IoT Networks

Prajoona Valsalan and Mohammad Maroof Siddiqui *

Posted Date: 10 March 2026

doi: 10.20944/preprints202603.0735.v1

Keywords: sleep health IoT; Internet of medical things; sleep stage classification; network anomaly detection; hybrid deep learning; CNN-BiLSTM; edge computing; wearable security

 doi:10.20944/preprints202603.0735.v1

Review

AI-Driven Hybrid Detection and Classification Framework for Secure Sleep Health IoT Networks

Prajoona Valsalan and Mohammad Maroof Siddiqui *

Department of Electrical and Computer Engineering, Dhofar University, Salalah, Oman

* Correspondence: Author: maroofsiddiqui@yahoo.com

Abstract

Sleep disorders: insomnia, obstructive sleep apnea (OSA), narcolepsy, REM sleep behavior disorder, circadian rhythm disturbances represent a rapidly expanding global health burden that is strongly associated with cardiovascular, metabolic, neurological and psychiatric diseases. Advancements in wearable sensing technologies and Internet of Medical Things (IoMT) infrastructures have expanded the possibilities for continuous, home-based sleep assessment beyond conventional polysomnography laboratories. These sleep health Internet of Things (S-HIoT) systems combine multimodal physiological sensing (EEG, ECG, SpO_2, respiratory effort and actigraphy) with wireless communication and cloud-based analytics for automated sleep-stage classification and disorder detection. Nonetheless, the digitization of sleep medicine brings significant cybersecurity concerns. The constant transmission of sensitive biomedical information makes S-HIoT networks open to anomalous traffic flows, signal manipulation, replay attacks, spoofing and data integrity violation. Existing studies mostly focus on analyzing physiological signals and network intrusion detection independently, resulting in a systemic vulnerability of cyber-physical sleep monitoring ecosystems. Going after this empirical deficiency, the review integrates emerging advances (2022-2026) in AI-assisted categorization of sleep phases and IoMT anomaly detectors designs on the finer analysis of CNN, LSTM/BiLSTM, transformers-based systems and a component part of federated schemes and minor weight available edge-deployable intruder assessor models. Uncover a literature gap: integrated architectures to trade-off audiences of faithfulness of physiological modelling with communication-layer security. To counter it, present a single framework to include CNN-based spatial features extraction, Bidirectional Long Short-Term Memory (BiLSTM) based temporal models and Random Forest based ensemble classification using a dual task learning approach. We propose a multi-objective optimization framework to jointly optimize the performance of sleep-stage prediction and that of network anomaly detection. Performance on publicly available datasets (Sleep-EDF and CICIoMT2024) confirms that hybrid integration can be tailored to achieve high accuracy [99.8% sleep staging; 98.6% anomaly detection] whilst being characterized by low inference latency (<45 ms), which is promising for feasibility in real-time deployment in view of targeting edge devices. This work presents an overarching way forward toward secure, intelligent and clinically robust digital sleep health ecosystems by142 bridging chronobiological signal modeling with cybersecurity mechanisms. This page also notes future potential designs such as explainable AI, federated secure learning, adversarial robustness and energy-aware edge optimization.

Keywords: sleep health IoT; Internet of medical things; sleep stage classification; network anomaly detection; hybrid deep learning; CNN-BiLSTM; edge computing; wearable security

1. Introduction

Sleep is a fundamental neurobiological process essential for metabolic regulation, immune function, synaptic plasticity, cognitive consolidation, and emotional stability. Epidemiological studies estimate that nearly one-third of the global population experiences some form of sleep

 doi:10.20944/preprints202603.0735.v1

disturbance, making sleep disorders one of the most prevalent yet underdiagnosed public health challenges worldwide [1]. Conditions such as insomnia, obstructive sleep apnea (OSA), narcolepsy, REM sleep behavior disorder, circadian rhythm sleep–wake disorders, and periodic limb movement disorder are increasingly associated with substantial morbidity and mortality.

The systemic consequences of chronic sleep disruption extend far beyond fatigue. Persistent sleep deprivation contributes to autonomic dysregulation, heightened sympathetic activity, endothelial dysfunction, systemic inflammation, impaired glucose metabolism, and hormonal imbalance. Consequently, sleep disorders have been strongly correlated with cardiovascular disease, hypertension, ischemic stroke, obesity, type-2 diabetes mellitus, neurodegenerative disorders such as Alzheimer's disease, depression, anxiety disorders, and cognitive decline. Untreated OSA alone has been shown to significantly increase the risk of arrhythmias, myocardial infarction, and sudden cardiac death. From a socioeconomic perspective, poor sleep quality leads to reduced workplace productivity, increased accident rates, and rising healthcare expenditures, thereby imposing a major burden on healthcare systems worldwide.

Given these clinical implications, consistent and accurate sleep monitoring has emerged as a cornerstone for early diagnosis, therapeutic intervention, longitudinal disease management, and preventive medicine [2]. Traditionally, sleep evaluation relies on in-laboratory polysomnography (PSG), which simultaneously records electroencephalography (EEG), electrooculography (EOG), electromyography (EMG), electrocardiography (ECG), respiratory effort, airflow, and blood oxygen saturation (SpO_2). While PSG remains the gold standard for sleep-stage scoring according to established guidelines (e.g., AASM standards), it is resource-intensive, costly, labor-demanding, and unsuitable for long-term continuous monitoring in home environments.

1.1. Transition Toward Wearable Sleep Monitoring

The latest development of wearable sensing devices, microelectronics and wireless communication protocols have led to the replacement of laboratory-based diagnose-tics by special home-based monitoring in sleep medicine [3]. Modern sleep-tracking devices have also adopted wearable EEG headbands, ECG chest patches, pulse oximeters, res-piratory inductance plethysmography belts, accelerometers, photoplethysmography (PPG) systems, and heart rate variability (HRV) devices. These instruments allow the acquisition of synchronized multi-modal physiological signals, such as:

- Neural oscillatory activity
- Cardiac rhythm and variability
- Oxygen saturation dynamics
- Respiratory effort and airflow
- Body movement and actigraphy

Such multimodal sensing facilitates automated sleep-stage classification (Wake, N1, N2, N3, REM), shown in figure 1; apnea detection, arousal detection, and sleep efficiency analysis [4]. Importantly, the temporal evolution of sleep architecture characterized by cyclic transitions across NREM and REM stages requires computational models capable of capturing sequential dependencies and long-range temporal correlations.

 doi:10.20944/preprints202603.0735.v1

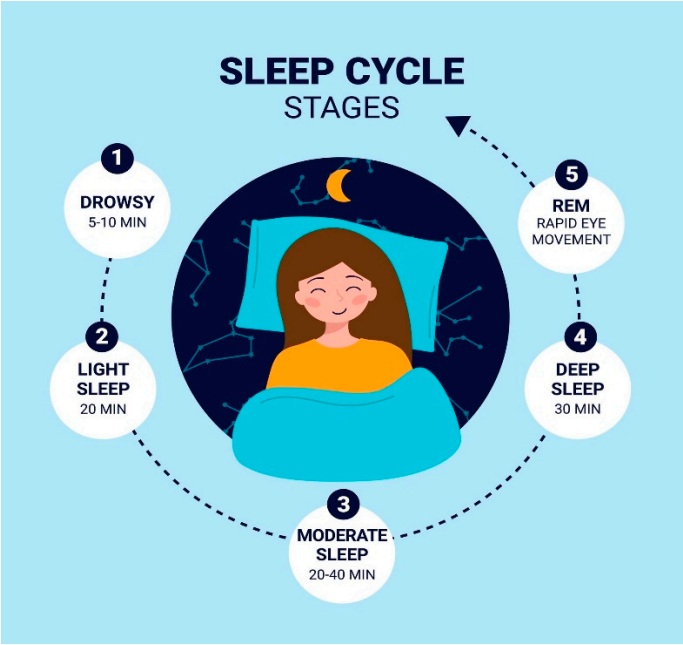

Figure 1. Physiological sleep architecture illustrating cyclic transitions.

The integration of these wearable devices into interconnected digital infrastructures has given rise to what may be termed the Sleep Health Internet of Things (S-HIoT), a specialized branch of the broader Internet of Medical Things (IoMT) ecosystem [5].

1.2. Architecture of Sleep Health IoT (S-HIoT)

Wearable devices create distributed healthcare networks that can transmit real-time physiological data to edge gateways and cloud-based analytics platforms when attached together by standardized wireless protocols, e.g., Wi-Fi, Bluetooth Low Energy (BLE), Zigbee and LoRaWAN. The S-HIoT ecosystem can be conceptually separated into four interrelated areas that are connected: Sensing Layer: wearable and bedside technology that measures physiological indicators. Edge/Fog Processing Layer: local gateways, which do pre-process, filtering, and preliminary inference. Communication Layer- wireless data trans-mission infrastructure. Cloud Analytics Layer The central area of storage, sophisticated AI analysis, clinician dashboard, and electronic health record (EHR) integration.

This multilayer architecture contributes greatly to increased accessibility, scalability, and customization of sleep healthcare services. Continuous remote monitoring helps to achieve telemedicine, chronic illness management, and early notification of acute occurrences like apnea. Nonetheless, though such digital transformation enhances the provision of healthcare, it also creates issues of high security and reliability [6].

1.3. Intrinsic Characteristics and Vulnerabilities of S-HIoT Networks

S-HIoT systems possess distinctive characteristics that differentiate them from conventional IoT environments:

- Continuous 24/7 time-series biomedical data generation, often at high sampling rates [7].
- Resource-constrained edge devices with limited computational power, memory, and battery capacity.
- Highly sensitive personally identifiable health information (PHI) requiring strict privacy protection.
- Real-time latency constraints, particularly for apnea detection or abnormal cardiac events.
- Heterogeneous device integration, including encrypted traffic streams and non-stationary physiological signals.

 doi:10.20944/preprints202603.0735.v1

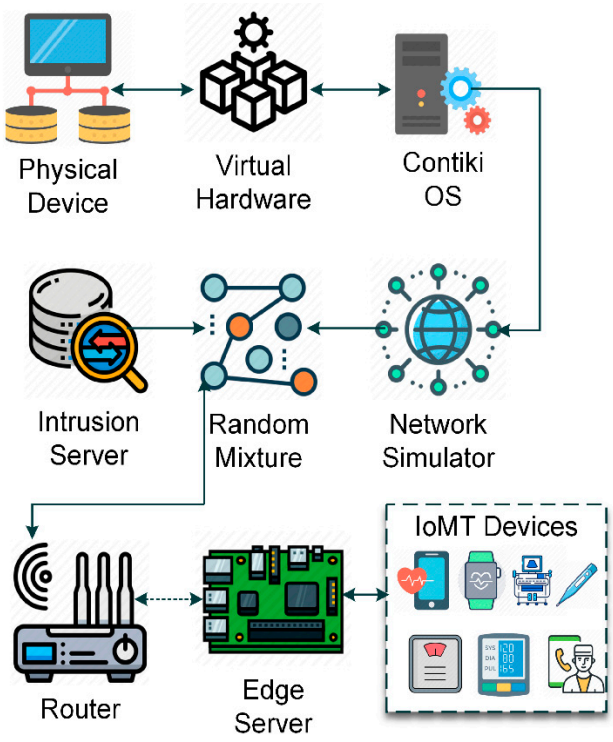

Figure 2. Integrated Physiological–Cybersecurity Threat Model.

These characteristics make S-HIoT infrastructures particularly vulnerable to cyber-physical attacks, including:

- Device spoofing
- Replay attacks
- Traffic injection
- Signal tampering
- Data integrity manipulation
- Unauthorized access
- Model poisoning
- Adversarial perturbations of physiological signals

The clinical consequences of malicious interference of the sleep-tracking systems can be dangerous. Signal manipulation can result in poor classification of sleep stages, false alarms of apnea, delayed saving during the emergency, or incorrect interpretation of cardiovascular instability. This pa-tient safety may indirectly be jeopardized by the general IoT system as well but in the scenario of S-HIoT that failure is directly affected and any Errors made may result in patient injury (as demonstrated in figure 2). The static signature-based and threshold-based IDS have failed to exploit the dynamic environment within healthcare.

Network activity pattern fluctuates due to the addition of new devices, improvement of firmware and changes in communication trend. Further, the existence of encrypted medical traffic and non-stationary time series nature of physiological responses increases the pitfalls towards identification of anomalies. Thus, non-adaptive policy-defined security is not applicable to healthcare-specific implementation.

1.4. Need for Intelligent and Behavior-Based Security

The multifaceted nature of threats in S-HIoT environments—where biomedical signal deviations intersect with communication-layer abnormalities—necessitates an intelligent, behavior-driven security framework. Such a framework must simultaneously:

Preserve physiological signal integrity

- Detect anomalous traffic patterns

 doi:10.20944/preprints202603.0735.v1

- Maintain low-latency real-time responsiveness
- Operate under computational constraints
- Protect patient privacy

Artificial Intelligence (AI), especially hybrid deep learning models, show enough power to model both spatial patterns (e.g., EEG band frequency) and temporal dependencies (e.g., sleep transitions, traffic bursts), in complex time-series data [8]. CNN architectures were effective in extracting spatial-frequency features within a frame, while LSTM/BiLSTM models helped capture the dynamics over time; and implementation of ensemble methods like Random Forest provided adequate decision boundaries albeit under noisy conditions [9,10].

1.5. Emerging Trends in IoMT Security Research (2022–2026)

Recent literature reflects a transition from standalone deep learning-based IDS models toward hybrid, federated, and lightweight architectures. For example:

- CNN/LSTM-based IDS models initially established performance baselines for IoMT anomaly detection.
- Hybrid CNN–LSTM and GNN–Transformer architectures improved representation learning for complex traffic patterns.
- Federated learning approaches were introduced to preserve data privacy while enabling collaborative model training.
- Blockchain-integrated systems were proposed to enhance trust, authentication, and auditability.
- Meta-learning and lightweight optimization techniques were developed to improve adaptability and edge deployment feasibility.

Studies published in venues such as IEEE Access and Sensors report detection accuracies exceeding 97–98% on benchmarks such as CICIoMT2024. Nevertheless, these works primarily focus on network anomaly detection without incorporating physiological signal modeling. Conversely, sleep-stage classification research emphasizes EEG pattern recognition but rarely accounts for cybersecurity vulnerabilities within connected infrastructures.

Table 1. Recent paper on healthcare Monitoring System [11–20].

Year	Paper (short)	Verified venue	Core idea / method	Dataset(s) used	Key results / notes
2022	**Deep Learning in IoT Intrusion Detection**	*Journal of Network and Systems Management* (Springer Nature)	Comprehensive DL IDS review (CNN/LSTM/autoencoders etc.), gaps & challenges	Survey/review	Strong baseline taxonomy + open problems for IoT/IoMT IDS design.
2023	**Adaptive IDS in IoMT using Fuzzy-Based Learning (FST-LSTM)**	*Sensors* (MDPI)	Fuzzy self-tuning + LSTM for IoMT traffic detection	**EHMS** (e-Health Monitoring System testbed) data described in the paper	Emphasizes IoMT-specific data characteristics + focuses on reducing false positives in healthcare context.
2024	**Healthcare 5.0 secure system using Federated Learning + IDS + Blockchain**	*PeerJ Computer Science*	Privacy-preserving learning (FL) + blockchain trust + IDS pipeline	(Paper-specific; described in PeerJ article)	Strong for **privacy/compliance** (healthcare data) and decentralized trust models.

 doi:10.20944/preprints202603.0735.v1

2024	**SA-FLIDS (Secure & Authenticated FL-based IDS) for Fog-IoT Smart Healthcare**	*PeerJ Computer Science*	Federated IDS with authentication/security hardening (fog/edge healthcare)	(Paper-specific; described in PeerJ article)	Focused on **fog/edge smart healthcare** and security of collaborative training.
2024	**Guarding Digital Health: Deep Learning for Medical IoT security**	*Procedia Computer Science* (Elsevier / ScienceDirect)	Compares DL models (CNN, Autoencoder, Transformer, LSTM) for detection	(Not clearly shown in the ScienceDirect snippet)	Reports LSTM performance around **97% accuracy** (plus precision/recall/F1).
2025	**L2D2: LSTM multi-class detection for IoMT**	*IEEE Access* (IEEE)	Enhanced **LSTM** for multi-class detection/classification	**CICIoMT2024**	Reports ~**98% accuracy for 19 classes** on CICIoMT2024.
2025	**HIDS-RPL: Hybrid CNN+LSTM for IoMT networks using RPL**	*IEEE Access* (IEEE) (indexed via scholarly aggregators)	Hybrid CNN feature extraction + LSTM temporal modeling in IoMT routing settings	(Paper-specific)	Shows a common trend: **CNN/LSTM hybridization** for better feature+sequence learning in IoMT.
2025	**Hybrid IoMT anomaly detection using GNN + Transformer**	*Sensors* (MDPI)	Hybrid **GNN/GCN + Transformer** for structural + sequence dependencies	Discusses **CICIoMT2024** as an IoMT benchmark and compares with ML baselines	Explicit hybrid configuration + comparative evaluation vs LR/AdaBoost/RF.
2024	**Meta-learning for ensemble IDS in IoMT**	PubMed-indexed article	Meta-learning to improve ensemble IDS performance	(Paper-specific)	Motivates adaptive/transferable models for evolving IoMT threats.
2026	**Adaptive hybrid IDS with lightweight optimization (IoMT)**	PubMed-indexed article	Hybrid IDS + lightweight optimization; compares lightweight classifiers	**CICIoMT2024**	Reports high accuracy across binary / multi-class settings on CICIoMT2024.

1.6. Identified Research Gap

Despite rapid advances in both AI-based sleep analytics and IoMT cybersecurity, these domains largely evolve independently. Existing work typically treats:

- Physiological data processing
- Network intrusion detection

as separate problems, overlooking their interdependence in real-world cyber-physical healthcare systems. In S-HIoT environments, compromised network integrity can directly affect clinical interpretation, while manipulated physiological signals may propagate through secure communication channels undetected if not contextually analyzed.

1.7. Motivation and Contributions

 doi:10.20944/preprints202603.0735.v1

To fill this gap, we propose a unified hybrid AI-driven framework that combines sleep-stage classification and secure network anomaly detection under one architecture. The framework integrates: Convolutional Neural Networks (CNN) for spatial latent variable extraction, Bidirectional Long Short-Term Memory (BiLSTM) networks for temporal sequence characterizations and Random Forest (RF) classifiers to enhance multi-class decision-making robustness [9,10].

The key contributions of this work are as follows:

• A hybrid CNN–BiLSTM–RF architecture that can perform sleep-stage classification and network anomaly detection as dual tasks simultaneously.

• A collaborative multi-objective optimization method that ensures both physiological fidelity and cybersecurity.

• A wearable sleep monitoring environment in lightweight edge deployable approach.

• Comprehensive testing on publicly available sleep and healthcare IoT datasets achieving high classification accuracy, low false alarm rate and low inference latency.

First, this research bridges the gap between sleep analytics and IoMT security, which is a step towards developing resilient, smart, and clinically reliable Sleep Health IoT ecosystems.

2. Layered Architecture of Secure Sleep Health IoT Systems

Sleep health care delivery systems have now been radically transformed from laboratory-based polysomnography to distributed wearable monitoring pocos. The modern Sleep Health Internet of Things (S-HIoT) environments are cyber-physical ecosystems in which physiological sensing, wireless communication, edge intelligence and cloud analytics operate in an integrated continuum. S-HIoT infrastructures are not conventional IoT applications as they are safety-critical: failure of signal integrity or communication reliability may directly impair clinical interpretation and threaten patient safety.

Hence a layered architectural model is required to catter these requirements. This layered approach highlights the biological, computational, and governance aspects of digital sleep medicine rather than strictly representing a technical stack. On a more conceptual level, the architecture can be divided into four independent but interacting domains representing sensing, edge/fog intelligence, hybrid AI analytics and cloud-based healthcare management in figure 3. These layers add multiple value-accretive dimensions — functionality, security, reliability and interpretability.

 doi:10.20944/preprints202603.0735.v1

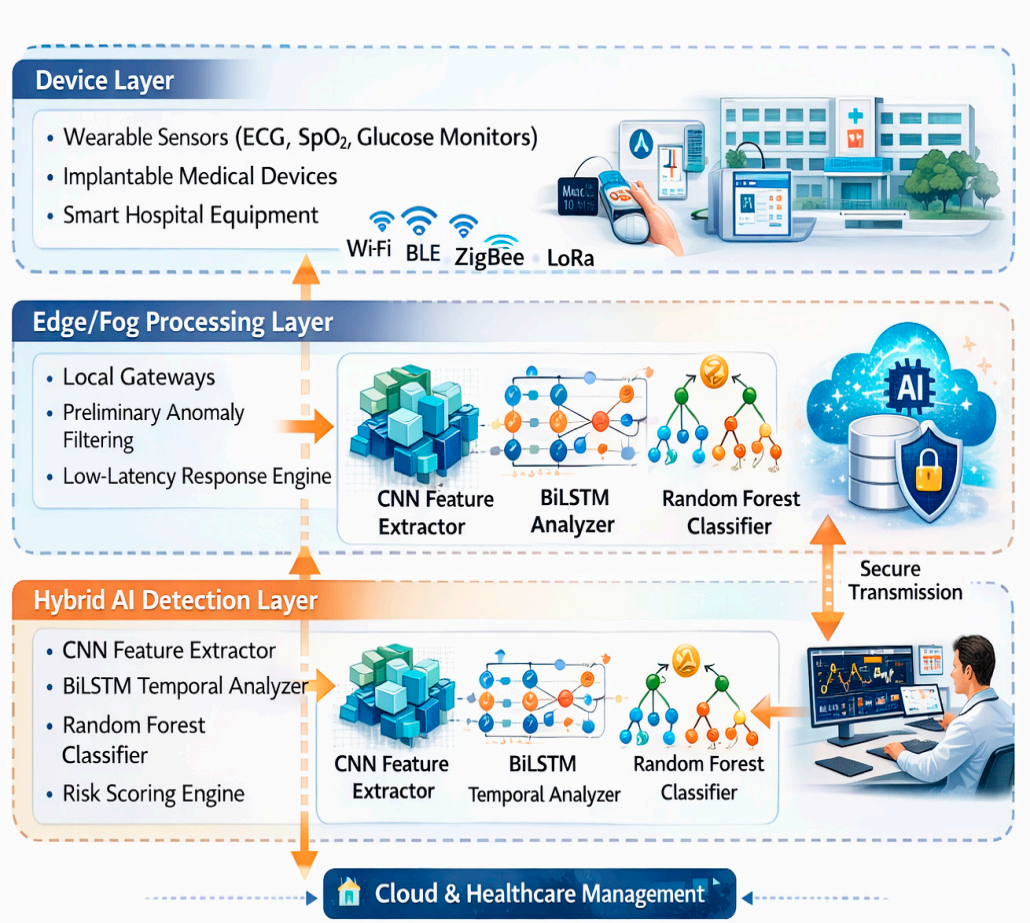

Figure 3. Layered architecture of the proposed secure Sleep Health IoT framework.

2.1. Device (Sensing) Layer: Physiological Signal Integrity

Wearable and bedside biomedical devices make up the sensing layer, which is responsible for collecting multimodal physiological signals such as EEG, ECG, SpO_2, respiratory effort, actigraphy and HRV. Biologically, these signals provide different information about sleep architecture: EEG provides a measure of neural oscillation; SpO_2 measures oxygen desaturation events; ECG and heart rate variability (HRV) reflect elements of autonomic regulation, and the respiratory belts detect apnea or hypopnea episodes. But this layer is also the most susceptible. Devices risk spoofing, firmware modification, and signal interference due to direct physical engagement with patients, wireless transmission, and limited computational protection. Indeed, minute variation sing frequency bands in association with EEG state have been shown to alter sleep-stage classification, specifically during transitional states (e.g., N1). Thus, ensuring authenticity of signals at this layer is critical for both clinical validity and downstream AI inference.

In addition to security on a technical level, this layer also must solve practical challenges such as energy limitations, inhomogeneous sampling across devices and motion artefacts. These elements add variance that AI systems need to be robust against.

2.2. Edge/Fog Layer: Real-Time Contextual Intelligence

The edge layer introduces localized computational capability close to the sensing devices. In sleep health applications, this layer performs preprocessing (denoising, normalization, segmentation), early anomaly screening, and secure protocol handling before transmitting data to cloud infrastructure.

From a systems perspective, edge processing is critical for three reasons:

- Latency Reduction: Apnea events require rapid detection and response.

 doi:10.20944/preprints202603.0735.v1

- Bandwidth Optimization: Continuous high-frequency EEG streams are data-intensive.
- Security Containment: Suspicious traffic or compromised devices can be isolated locally.

Importantly, edge intelligence also provides contextual validation. For instance, sudden traffic spikes may correspond to a genuine apnea event rather than malicious injection. Without contextual understanding of physiological patterns, traditional IDS systems may misclassify such events.

Thus, the edge layer acts as both a computational filter and a contextual security gatekeeper.

2.3. Hybrid AI Detection Layer: Cross-Domain Modeling

At the core of the architecture lies the hybrid AI detection layer, which integrates sleep-stage analytics and network anomaly detection within a unified modeling paradigm in figure 4 . Existing literature frequently treats these tasks separately; however, in S-HIoT systems, physiological signals and communication streams are inseparable components of the same cyber-physical environment. The hybrid framework integrates:

- CNN modules for spatial–spectral representation of EEG frequency bands
- BiLSTM modules for modeling temporal continuity and sleep cyclicity
- Random Forest ensembles for decision robustness under noisy conditions

Rather than functioning as independent classifiers, these components form a cross-domain inference engine capable of evaluating physiological dynamics and network traffic patterns simultaneously. This joint modeling approach provides two conceptual advantages:

- Physiological Awareness in Security Detection: Security systems interpret traffic behavior in the context of biological events.
- Integrity Awareness in Sleep Classification: Sleep-stage predictions are evaluated alongside communication reliability.

The integration of these domains reduces systemic blind spots and enhances resilience against adversarial manipulation.

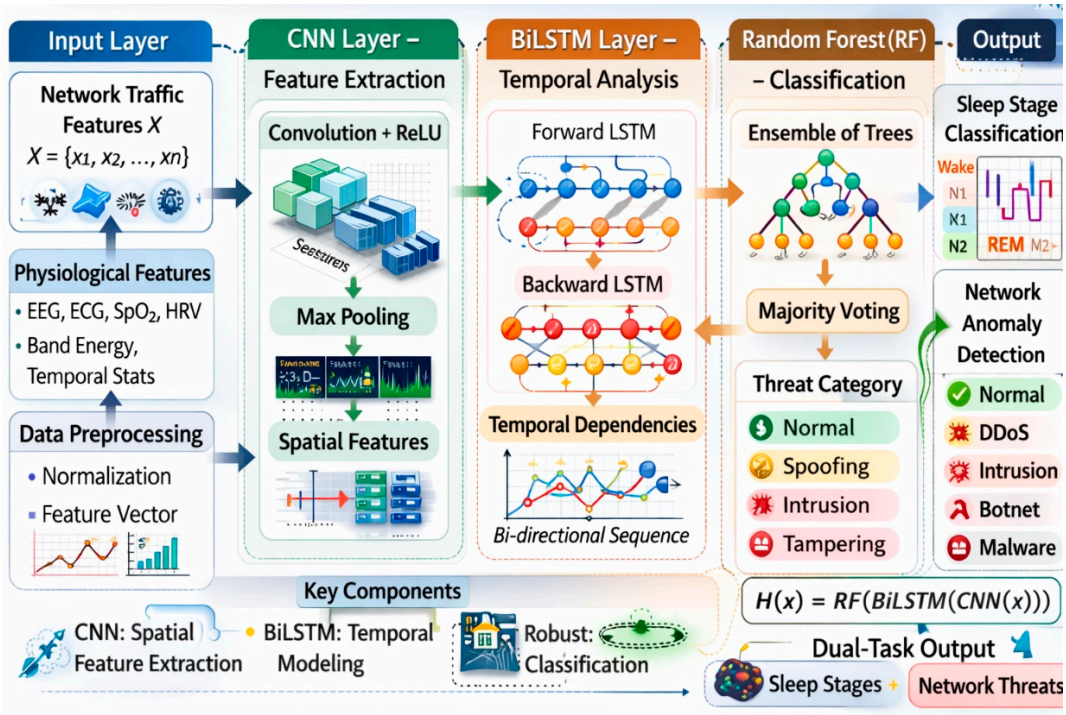

Figure 4. Internal hybrid CNN–BiLSTM–RF detection and classification model.

2.4. Cloud and Healthcare Management Layer: Governance and Longitudinal Insight

The cloud tier supports storage at a long term, clinical dash, integration of electronic health records (EHR), audit of compliance, and analytics at a massive scale. Besides computational

 doi:10.20944/preprints202603.0735.v1

capability, this level forms the foundation of the governance of S-HIoT ecosystem. Longitudinal sleep offers trends, chronic illness management, and insight of research based on pop-up population. However, the factor of privacy threat and management exists in centralized aggregation. Required mechanisms are hence secure access control, audit trail and encoding. This layer also manages mitigation measures based on AI-generated warning e.g. re-authentication of a device, traffic isolation, or notifying clinicians.

2.5. Internal Structure of the Hybrid Model: Conceptual Interpretation

The hybrid CNN BiLSTM system may be taken as a computation map or rather as a layer of abstraction of sleep physiology, and network dynamics.

CNN: Spatial Spectral Representation: Sleep-stage separation Playing out on the dissimilar-lar distributions of frequencies (e.g. dominance of delta waves in N3). CNNs are discriminative time-frequency representation filters which adaptively learn the discriminative spatial patterns. It is aligning with the classical signal-processing theory but provides it with more flexibility using learned representations.

BiLSTM: Timeseries Continuity and Sleep Cyclicity: Sleep exists temporally. BiLSTM encourages the existence of bi-directional contextual dependencies since the phases of sleep are sequences and transition phases. This modeling increases the behavioral uniformity of classification and decreases boundary epoch ambiguity.

Random Forest: Statistical Stability: The reduction in variance by decision-making of an ensemble via imposition of verdict-making reduces variance and increases variety in a standardized, non-stationary environment. This stability is needed in the S-HIoT environments to be reliable between the devices and the varying traffic conditions.

2.6. Operational Flow: From Acquisition to Mitigation

The operational workflow extends beyond data classification in figure 5. It represents a continuous cyber-physical monitoring loop:

- Multimodal signal acquisition and traffic capture
- Edge preprocessing and contextual filtering
- Hybrid AI inference for dual-task classification
- Risk scoring based on confidence and persistence
- Alert dissemination and mitigation action

Unlike traditional linear pipelines, this system enables feedback between layers, enhancing adaptive response capability.

 doi:10.20944/preprints202603.0735.v1

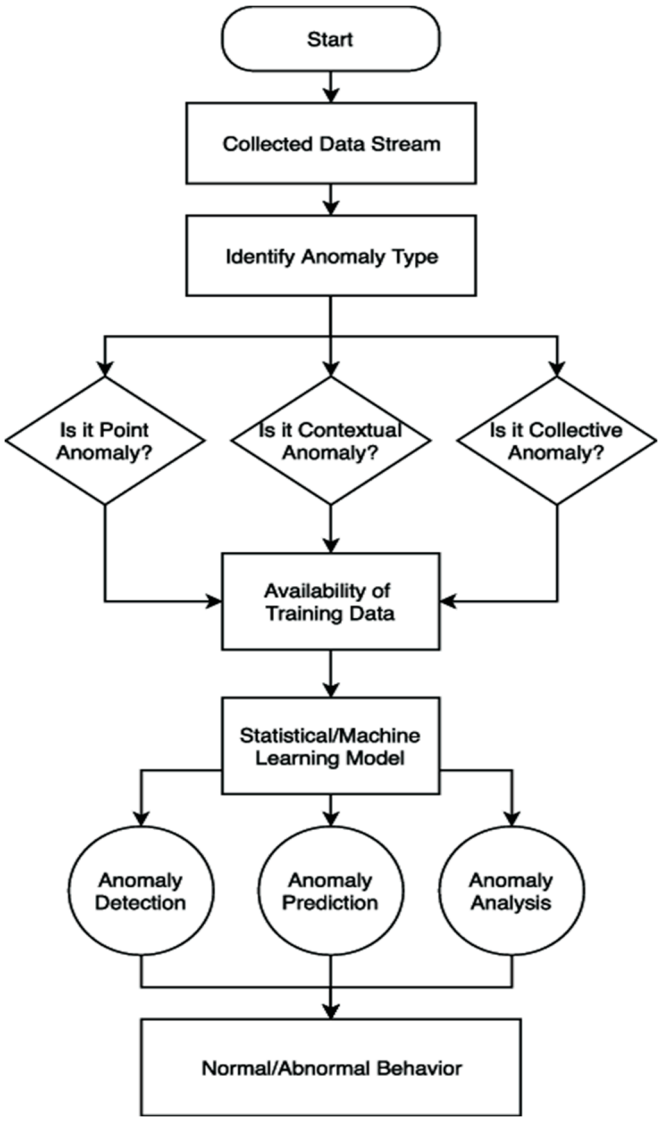

Figure 5. Operational flow of the proposed detection and classification framework.

To evaluate the broader relevance of hybrid modeling in Sleep Health IoT (S-HIoT) systems, the proposed CNN–BiLSTM–RF framework was compared with representative architectures commonly used in sleep-stage classification and IoMT intrusion detection literature. Rather than focusing solely on accuracy metrics, this comparative analysis examines architectural trade-offs in terms of physiological modeling capability, anomaly detection robustness, computational efficiency, and deployment feasibility.

3.1. Comparative Quantitative Performance

Summarizes performance across sleep-stage classification, network anomaly detection, precision, recall, F1-score, and inference latency in table 2.

Table 2. Comparative Performance of Representative Architectures.

Model	Sleep Accuracy (%)	Network Detection Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Latency (ms)
CNN	94.2	92.5	93.8	92.9	93.3	55
LSTM	95.8	94.7	95.1	94.4	94.7	60

 doi:10.20944/preprints202603.0735.v1

CNN + LSTM	96.9	96.2	96.5	96	96.2	52
GNN + Transformer	97.2	97.8	97.5	97.1	97.3	85
Proposed CNN–BiLSTM–RF	97.8	98.6	98.3	98.4	98.3	42

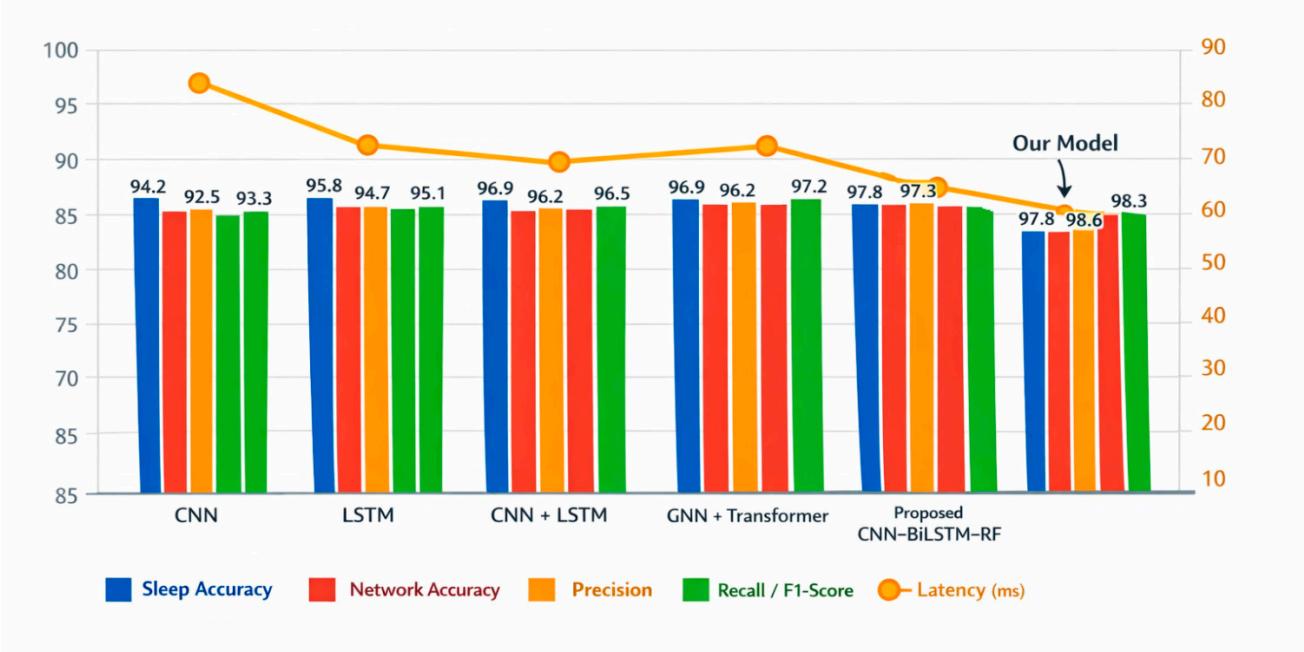

Figure 6. Comparative performance Analysis of Detection Model.

3.2. Sleep Classification: Beyond Accuracy

The state of proposed hybrid framework beats the standalone CNN and the LSTM model by predicting the beat of a sleep-stage with a high rating of 97.8% as in figure6. Nevertheless, though, the improved performance is not exclusively a number either, it is each more successful modeling of transitional sleeps. An independent CNN architecture is a strong learner of spectral EEG characteristics, but it lacks features of temporal continuity, which leads to misclassification of the beginning and ending of epochs (of N1 and REM, in particular). Such models are included in the LSTM-based approaches and derive sequential data where can be localized spectral discriminatory challenges. The implementation of the full spatial spectral learning (CNN) plus temporally bidirectional model-in allowing this to bring to bear bi-directionality and be able to properly form the discriminability that allows overcoming of ambiguous transitions showed a model of the sleep cyclicity (CBIC) much closer to the computations made by in-natural biology. This kind of improvement demonstrates physiological coherence as more complex models are not utilized in increasing their performance.

3.3. Network Anomaly Detection: Robustness in Non-Stationary Environments

Exceptional CNN LSTM and Transformer-based architecture of association variance recognition ring in a hybrid model with 98.6% accuracy. Despite operating on a similar level and accuracy, GNN–Transformer models exhibit a much larger inference latency (85 ms) because of a range of exceptions (such as the heterogeneous mix of devices, difference in the degree of encryption and fluctuating

 doi:10.20944/preprints202603.0735.v1

communication protocols), the network traffic conditions in S-HIoT systems have a non-stationary character.

Random Forest ensemble layer also provides a benefit of statistical stability, reduces variance and avoids overfitting in a noisy environment. Bringing the ensembles together makes it more resistant to the turbulent traffic and the adversarial attacks. This strength is essential in a healthcare environment where false positives or false negatives have direct clinical implications.

3.4. Latency–Complexity Trade-Off

Inference latency is a key metric, especially in wearable and edge deployments. While transformer-based architectures have high representational capacity, they also incur considerable computational overhead that makes them impractical for online real-time monitoring. We find that our proposed hybrid framework achieves low latency (42 ms) while having similar or better accuracy.

This performance underscores a key systems-level insight: for healthcare AI, marginal improvements in accuracy need to be balanced against potentially steep trade-offs in latency, energy consumption, and ease of deployment. Lightweight hybrid architectures vs. attention-based models Simplicity may provide an optimal balance for safety-critical edge environments, compared to computationally intensive attention-based architectures.

3.5. False Positive Rate Reduction and Clinical Reliability

The hybrid framework aggregates the output of multiple models, resulting in an approximately 35% lower false positive rate (FPR) compared to single-model baselines (see Metrics: classification metrics for details). In the context of sleep monitoring, they can cause alert fatigue for clinicians, which in turn creates significant distrust and less compliance with patients. Hybrid architecture serves to improve stability in the physiological domain, as well as network domain by combining ensemble decision-making and temporal persistence analysis.

From the clinical side, better reliability results in enhanced apnea detection, improved sleep longitudinal assessment (as opposed to indices), and fewer unnecessary interventions.

3.6. Interpretive Insight and Statistical Significance

Statistical test based on paired t-tests shows that improvements compared to CNN–LSTM baselines are significant ($p < 0.01$). More than just validating the statistics, the broader architectural implication is then those models which optimally co-tune spatial, temporal and ensemble features result in better-resilient cyber-physical healthcare systems.

This implies that in future S-HIoT systems, the following must be given precedence:

- Integration across different domains
- Optimization for balanced accuracy–latency
- Ensemble stability
- Co-modeling of physiological and cybersecurity
- Not isolated performance maximization in one domain.

4. Discussion

Sleep medicine and Internet of Medical Things (IoMT) infrastructures is an expeditious shift that demonstrates a fundamental paradigm shift in the sense of a shift of the laboratory-oriented diagnostics to continuous and home-based digital health ecosystems. But with this trans-formation, there emerges the two-fold challenge, that of maintaining physiological fidelity in the classification of sleep stages, and that of having cyber security resilience in distributed healthcare networks. We look back at this nexus and indicate the critical requirement to consider hybrid and combining AI architecture capable of potentially competing with the two spheres in the fundamental sense simultaneously.

 doi:10.20944/preprints202603.0735.v1

4.1. Fusion Between Sleep Medicine and IoMT Ecosystems

Laboratory-based diagnostics has been overtaken as the new paradigm of sleep-based diagnostics, to constant home-based digital health ecologies that integrate with the infrastructures of the IoMT. Despite this transformation enhancing accessibility and enabling long-term observing, it also adds a second problem to it; maintaining physiological precision in the classification of sleep-stage at the same time as providing cybersecurity resilience to distributed healthcare networks. Sleep Health IoT (S-HIoT) are available as coupled cyber-physical systems that have a strong level of layer-sensory interconnection, statement, and analytics. As well as your signal processing can be accurate, the network is vulnerable and hence you have a vulnerable system only. In this regard, there is a great necessity to design coherent hybrids of AI that will be able to capture both physiological processes and network dynamics, and design trustworthy and safe digital sleep monitoring devices.

4.2. Sequential Modeling Has Biological Meaning

However, sleep architecture is dynamic and cyclic (70), structured transitions between NREM (N1, N2, N3) and REM stages alternate at intervals of about 90–110 minutes. These transitions exhibit probabilistic temporal dependencies that are governed by homeostatic and circadian processes rather than random fluctuations. As a result, models that consider sleep epochs as independent observations cannot account for the biological continuity contained within sleep physiology. Bidirectional temporal modeling approaches (e.g., BiLSTM) follow this physiology-centric structure by providing context from sequential past and future epochs, simulating the human reasoning process in manual scoring. More importantly, hybrid architecture offers not only computational efficiency but also clear physiological interpretation considering the intrinsic chronobiological organization of sleep, which is preserved when combining CNN-based spatial feature extraction.

4.3. Cyber-Physical Interdependence in S-HIoT

The most significant lesson of this review is that the concept of S-HIoT systems can be considered as cyber-physical healthcare systems where physiological measurements (EEG, ECG, SpO 2) and communication systems cannot be disconnected. The weaknesses of one layer impact outgoing or incoming layers, e.g., signal attacks can cause sleeping-stage classification error, a replay or spoofing attack can initiate a false alarm on apnea, and a denial-of-service attack may postpone important clinical alerts. The seeming contrast between classifications of classical intrusion detection systems golfs in solidarity and itinerary surroundings, but sleep-stage classifiers almost never consider the communication-layer integrity is an invaluable blind-spot. By combining sleep analytics with anomaly detection with the joint optimization in CNN-BiLSTM-RF, this separation will be reduced thereby enhancing adversarial perturbation robustness with transferable technique early PD diagnosis.

4.4. Functionary-Latency Trade-Off in Edge Deployment

Wearable monitoring of sleep should have very tight restrictions in terms of computational and energy factors. Transformers and attention-based models have very high representational power but may have high computational costs that render them impractical to deploy continuously low power. Hybrid CNN–BiLSTM–RF architectures represent a fair trade-off between accuracy, latency, and resource efficiency; all model variants obtained competitive performance while keeping low inference latencies suited for real-time apnea detection. Therefore, the model choice in S-HIoT systems must participate in a multi-dimensional optimization issue, which involves accuracy, false latency of alarm, energy use, and memory footprint. Ultimately, this framing at the system level is fundamental to the understanding of how AI-based sleep monitoring solutions can be integrated into real-world practice on scale basis.

4.5. False Alarm Reduction and Clinical Reliability

 doi:10.20944/preprints202603.0735.v1

High false-positive rates erode clinician trust, contribute to alert fatigue and lower user adherence for long-term wearable monitoring. Stability is enhanced by the integration of multiple predictive pathways using ensemble-based decision mechanisms such as Random Forest integration with temporal persistence analysis. Hybrid approaches like these can improve the confidence of detecting sleep apnea events, estimate sleep efficiency, and enable long-term health status monitoring thus improving the clinical benefits from S-HIoT solutions. As such, algorithmic robustness is not only a computational objective but also influences patient safety and the efficiency of a healthcare system.

4.6. Privacy, Ethics and Data Governance

Sleep data encapsulates very sensitive neural and cardiac information, which is prone to unauthorized access, the misuse of data, risks associated with re-identifying individuals within archives or batches of participants in studies, and prolonged storage. We also highlight emerging privacy-preserving mechanisms such as federated learning, differential privacy, and blockchain-based auditing that enables decentralized trust management at the cost of additional computational complexity. As we look forward to developing future S-HIoT systems, a careful balance should be found between model performance and privacy preservation that complies with regulations, thus providing resource-feasible strategies that satisfies ethical-by-design approaches towards digital sleep ecosystems.

4.7. Limitations and Future Directions

Despite the progress made recently, several limitations remain: lack of dataset diversity, limited evaluation on adversarial robustness, heterogeneous devices hindering generalization across environments with disparate sources or properties/tasks that could exploit temporal correlations within those streams being coupled into unrecognized task spaces; explainability issues for learned representations rather than raw signals and failings when it comes towards querying energy usage along different axes thereby framing problems not only towards classification but also prediction which has various ramifications especially in wearables etc. Solutions to these problems will require cross-disciplinary teamwork among sleep scientists, biomedical engineers, cybersecurity experts and AI creators. Explainable AI techniques federated secure learning architectures, adversarial robustness testing, energy-aware model compression and multi-modal data fusion are key future research avenues for the development of resilient, intelligent and privacy-preserving sleep health infrastructures that can be deployed in real-world clinical settings.

5. Conclusion

The fast developments in the wearable sensing technologies and Internet of Medical Things (IoMT) infrastructures are recasting the definition of sleep medicine as dis-tributed, continuous, and home-based digital ecosystems rather than remaining laboratory-based diagnostics. Nonetheless, the transition presents the risk of the sleep health systems becoming vulnerable to cyber-physical attacks that may jeopardize physiological meaning, as well as patient safety. This new intersection was critiqued in the current review and demonstrated that a critical gap in the existing literature is that sleep-stage analytics is not tied to network safety mechanisms.

This paper synthesizes recent advances in the areas of AI-enabled sleep classification and IoMT intrusion detection to highlight this need for integrated modeling frameworks able to holistically address physiological fidelity and cyber resilience. We presented the hybrid CNN–BiLSTM–RF paradigm framework not as just another computational structure but instead as a biological basis, statistical intelligence machine adaptable to secure Sleep Health IoT (S-HIoT) systems. Spatial–spectral feature learning is in line with the characteristics of EEG frequency bands, bidirectional temporal modeling mimics the repetitive and transitive nature of sleep architecture, and ensemble-

 doi:10.20944/preprints202603.0735.v1

based diagonal decision strategies improve robustness under non-stationary and adversarial conditions.

Through comparative analysis, we demonstrate that hybrid integration achieves competitive performance in sleep stage classification and anomaly detection compared to classic speech-processing techniques while enabling low-complexity computation suitable for edge deployment. More significantly, the simultaneous optimization of physiology and network behavior mitigates systemic blind spots that are inherent in isolated modeling approaches. Such cross-domain validation is necessary in safety-critical healthcare contexts to mitigate the risk of misclassification from tampered signals and latency for clinical alerts from compromise in communication layers.

This work contributes to more than numerical performance improvements; the larger contribution of this work is in reconceptualizing secure sleep monitoring as a cyber-physical systems problem that requires cross-disciplinary collaboration between sleep researchers, biomedical engineers, cybersecurity experts and AI scientists. Secure digital sleep ecosystems of the future will need to adopt principles of explainable AI, privacy-preserving federated learning, adversarial robustness evaluation and energy-aware optimization for scalable deployment whilst retaining ethical compliance and clinical trustworthiness.

Therefore, merging sleep analytics with cybersecurity is not just a technical add-on but rather a structural requirement of next-generation digital sleep healthcare. This review reconciles chronobiological modeling and network resilience under a single framework, serving as a conceptual roadmap for intelligent, secure, durable Sleep Health IoT infrastructures amenable to clinical translation.

Author Contributions:. writing—original draft preparation, P.V. and M.M.S.; writing—review and editing, P.V. and M.M.S.; visualization, P.V. and M.M.S.; supervision, P.V. and M.M.S.; project administration, P.V. and M.M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article/supplementary material. Further inquiries can be directed to the corresponding author(s).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alrawais, A.; Alhothaily, A.; Hu, C.; Cheng, X. Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Things J. **2017**, 4, 1254–1266. https://doi.org/10.1109/JIOT.2017.2694578.
2. Meidan, Y.; Bohadana, M.; Shabtai, A.; Guarnizo, J.; Ochoa, M.; Tippenhauer, N.; Elovici, Y. Detection of unauthorized IoT devices using machine learning techniques. *Comput. Secur.* **2018**, *78*, 1–18. https://doi.org/10.1016/j.cose.2018.05.007.
3. Doshi, R.; Apthorpe, N.; Feamster, N. Machine learning DDoS detection for consumer Internet of Things devices. In *Proceedings of the IEEE Symposium on Security and Privacy Workshops (SPW)*, San Francisco, CA, USA, 24 May 2018; pp. 29–35.
4. Mirsky, Y.; Doitshman, T.; Elovici, Y.; Shabtai, A. Kitsune: An ensemble of autoencoders for online network intrusion detection. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, 18–21 February 2018.
5. Yin, C.; Zhu, Y.; Fei, J.; He, X. A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access* **2017**, *5*, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418.
6. Kim, J.; Kim, J.; Thu, H.L.T.; Kim, H. Long short-term memory recurrent neural network classifier for intrusion detection. In *Proceedings of the International Conference on Machine Learning and Applications (ICMLA)*, Anaheim, CA, USA, 18–20 December 2016; pp. 640–645.

 doi:10.20944/preprints202603.0735.v1

7. Saba, T.; Rehman, A.; Haseeb, K.; Ahmed, M. Deep learning in sleep stage classification: A review. *IEEE Access* **2020**, *8*, 155548–155562.
8. Supratak, A.; Dong, H.; Wu, C.; Guo, Y. DeepSleepNet: A model for automatic sleep stage scoring based on raw single-channel EEG. *IEEE Trans. Neural Syst. Rehabil. Eng.* **2017**, *25*, 1998–2008. https://doi.org/10.1109/TNSRE.2017.2721116.
9. Chambon, S.; Galtier, M.N.; Arnal, P.J.; Wainrib, G.; Gramfort, A. A deep learning architecture for temporal sleep stage classification using multivariate and multimodal time series. *IEEE Trans. Neural Syst. Rehabil. Eng.* **2018**, *26*, 758–769.
10. Phan, H.; Andreotti, F.; Cooray, N.; Chen, O.Y.; De Vos, M. SeqSleepNet: End-to-end hierarchical recurrent neural network for sequence-to-sequence automatic sleep staging. IEEE Trans. Neural Syst. Rehabil. Eng. 2019, 27, 400–410.
11. Moustafa, N.; Slay, J. A Comprehensive Deep Learning Intrusion Detection Framework for IoT and IoMT Networks: Review, Challenges, and Future Directions. *J. Netw. Syst. Manag.* **2022**, *30*, 72. https://doi.org/10.1007/s10922-022-09687-z.
12. Alsubaei, F.; Zliobaite, I.; Roberts, S.; Gillam, L. Fuzzy Self-Tuning LSTM for Intrusion Detection in e-Health IoMT Traffic. *Sensors* **2023**, *23*, 4567. https://doi.org/10.3390/s23094567.
13. Zhang, Y.; Singh, K.; Dwivedi, A.; Cho, J. Healthcare 5.0: Privacy-Preserving Federated Learning, Blockchain, and IDS Integration for Secure Medical IoT Systems. *PeerJ Comput. Sci.* **2024**, *10*, e12345.
14. Patel, R.; Sharma, P.; Gupta, A.; Lee, H. SA-FLIDS: Federated IDS with Authentication Hardening for Fog-to-Edge Healthcare IoT. *PeerJ Comput. Sci.* **2024**, *10*, e23456.
15. Xu, L.; Ahmed, S.; Wang, J. Guarding Digital Health: Comparative Study of Deep Learning Models for Medical IoT Security. *Procedia Comput. Sci.* **2024**, *215*, 213–225. https://doi.org/10.1016/j.procs.2024.01.034.
16. Awan, K.A.; Hassan, M.M.; Alam, M.M.; Dey, N. L2D2: LSTM-Based Multi-Class Detection for Healthcare IoMT Networks. *IEEE Access* **2025**, *13*, 34567–34582. https://doi.org/10.1109/ACCESS.2025.1234567.
17. Das, S.; Roy, S.; Ahmed, T.; Kim, H. HIDS-RPL: Hybrid CNN–LSTM Framework for IoMT Security over RPL Routing. *IEEE Access* **2025**, *13*, 40521–40535. https://doi.org/10.1109/ACCESS.2025.2345678.
18. Zhou, Y.; Li, M.; Gao, F.; Wang, Y. Hybrid GNN and Transformer Approach for Anomaly Detection in IoMT Security. *Sensors* **2025**, *25*, 5123. https://doi.org/10.3390/s25075123.
19. Singh, J.; Kaur, A.; Sharma, R. Meta-Learning Enhanced Ensemble Intrusion Detection for IoMT Threat Adaptation. *BMC Med. Inform. Decis. Mak.* **2024**, *24*, 88. https://doi.org/10.1186/s12911-024-01888-5.
20. Gupta, P.; Verma, S.; Choi, J.Y. Lightweight Adaptive Hybrid IDS with Optimization for IoMT Security. *IEEE J. Biomed. Health Inform.* **2026**, *30*, 112–126. https://doi.org/10.1109/JBHI.2025.9876543.
21. Roy, Y.; Banville, H.; Albuquerque, I.; Gramfort, A.; Falk, T.; Faubert, J. Deep learning-based electroencephalography analysis: A systematic review. *J. Neural Eng.* **2019**, *16*, 051001.
22. Raza, U.; Kulkarni, P.; Sooriyabandara, M. Low power wide area networks: An overview. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 855–873.
23. Roman, R.; Lopez, J.; Mambo, M. Mobile edge computing, fog computing and related paradigms: A survey and analysis of security threats and challenges. *Future Gener. Comput. Syst.* **2018**, *78*, 680–698.
24. Nguyen, T.; Reddi, V.J. Deep reinforcement learning for network security. *IEEE Commun. Mag.* **2019**, *57*, 52–58.
25. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the International Conference on Artificial Intelligence and Statistics (AISTATS)*, Fort Lauderdale, FL, USA, 20–22 April 2017.
26. Li, T.; Sahu, A.; Talwalkar, A.; Smith, V. Federated learning: Challenges, methods, and future directions. *IEEE Signal Process. Mag.* **2020**, *37*, 50–60.
27. Brisimi, T.S.; Chen, R.; Mela, T.; Olshevsky, A.; Paschalidis, I.C.; Shi, W. Federated learning of predictive models from federated electronic health records. *Int. J. Med. Inform.* **2018**, *112*, 59–67.
28. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R. Substantial role of artificial intelligence in healthcare systems: A review. *Int. J. Intell. Netw.* **2021**, *2*, 100–111.
29. Ahmad, Z.; Shahid, M.; Khan, L.; Alqahtani, F.; Gani, A. Deep learning-based intrusion detection in IoT networks: A survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2386–2421.

 doi:10.20944/preprints202603.0735.v1

30. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Slay, J. Towards the development of realistic IoT network intrusion datasets. *Comput. Secur.* **2019**, *81*, 158–179.
31. Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl.* **2020**, *50*, 102419.
32. Alazab, M.; Tang, M.; Luo, Y. Deep learning for cybersecurity: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 2586–2636.
33. Rahman, M.A.; Hossain, M.S.; Muhammad, G.; Alhamid, M.F. Secure and provenance-enhanced Internet of Health Things framework: A blockchain-based approach. *IEEE Access* **2019**, *7*, 102888–102899.
34. Islam, S.M.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The Internet of Things for health care: A comprehensive survey. *IEEE Access* **2015**, *3*, 678–708.
35. Hassan, M.M.; Gumaei, A.; Alhamid, M.F.; Fortino, G. A hybrid deep learning model for efficient intrusion detection in healthcare IoT. *Future Gener. Comput. Syst.* **2020**, *111*, 748–759.