PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

ABOU-BEKR BELKAID UNIVERSITY – TLEMCEN

LMD THESIS

Presented in:

FACULTY OF SCIENCE – DEPARTMENT OF COMPUTER SCIENCE

For the degree of:

DOCTORATE

Speciality: Computer Science

By:

Mr Hamed BENAHMED

On the theme of

Artificial Intelligence and IoT for E-Health Discovery and Management

---

Publicly defended in 2026 in Tlemcen before a jury composed of:

Pr BENAMAR Abdelkrim	Pr	University of Tlemcen	President
Dr MERZOUG Mohammed	MCA	University of Tlemcen	Thesis supervisor
Dr M'HAMEDI Mohammed	MCB	Higher School of Applied Sciences - Tlemcen	Co-Thesis supervisor
Dr HADJILA Fethallah	MCA	University of Tlemcen	Examiner
Dr HACHEMI Mohammed Hicham	MCA	University of Science and Technology of Oran	Examiner
D NEDJAR Imane	MCA	Higher School of Applied Sciences - Tlemcen	Examiner

Tlemcen Computer Science Research Laboratory LRIT
PO Box 119, 13000 Tlemcen - Algeria

Remerciements

Louange à Allah qui ma donné patience et courage pour mener à bien ce travail de thèse malgré les difficultés rencontrées. Je tiens à remercier en premier lieu Mr Merzoug Mohammed et Mr M'Hamedi Mohammed, mes directeurs de thèse pour leurs précieux conseils.

Je remercie également les membres du jury qui ont accepté l'évaluation de notre travail, et je cite en l'occurrence Pr Benamar Abdelkrim, Dr Hadjila Fethallah, Dr Hachemi Mohammed Hicham, et Dr Nedjar Imane.

Je tiens à remercier notre professeur Mahmoudi Saïd de l'université de Mons (Belgique) pour son encouragement et son soutien.

Je remercie aussi ma famille pour son soutien, son écoute et ses encouragements tout au long de cette thèse. Je tiens à remercie notre collègue Imane Nedjar pour son encouragement et son soutien.

Je dédie cet humble ouvrage à l'âme de mon cher père, qu'Allah ait pitié de lui, à ma chère mère, qu'Allah lui accorde une longue vie, à ma chère épouse, à mes enfants, à mes frères et surs, et à tous mes chers collègues.

Abstract

The burgeoning landscape of the Internet of Medical Things (IoMT) presents a critical and escalating challenge to cybersecurity. Traditional Intrusion Detection Systems (IDS) are demonstrably inadequate for this domain, as they are unable to effectively manage the unique characteristics of IoMT network traffic, including its high dimensionality, temporal dependencies, and inherent heterogeneity. This research addresses this deficiency by introducing a novel hybrid deep learning framework, built upon a synergistic integration of a Bidirectional Long Short-Term Memory (BiLSTM) network with a Deep Neural Network (DNN). This innovative architecture is meticulously designed to overcome the limitations of existing models by concurrently capturing both the temporal sequences and spatial features embedded within IoMT network traffic. A core contribution of this work is the framework's intrinsic transparency. It moves beyond the opaqueness of traditional "black box" models by incorporating Explainable AI (XAI) principles, leveraging SHapley Additive exPlanations (SHAP). This integration provides human-interpretable justifications for every security alert, revealing the specific features and data patterns that drive the model's predictions. This not only cultivates trust and ensures accountability but also facilitates an effective human-in-the-loop analysis, empowering security personnel to confidently validate alerts and respond without compromising patient care. Rigorous evaluation on the comprehensive CICIoMT2024 benchmark dataset validates the framework's exceptional performance, demonstrating high accuracy in discriminating between 18 distinct attack types and normal traffic. By seamlessly combining advanced detection capabilities with essential operational transparency, this research marks a significant advancement in both cybersecurity and trustworthy AI, contributing a robust and auditable solution vital for safeguarding sensitive healthcare data and ensuring the resilient operation of critical medical services.

Keywords: e-Healthcare, Internet of Medical Things (IoMT), Intrusion Detection System (IDS), BiLSTM, DNN, Black-Box, Explainability Artificial Intelligence (XAI), SHAP.

Résumé

L'essor de l'Internet des objets médicaux (IoMT) représente un défi majeur et croissant pour la cybersécurité. Les systèmes de détection d'intrusion (IDS) traditionnels sont manifestement inadaptés à ce domaine, incapables de gérer efficacement les caractéristiques uniques du trafic réseau IoMT, notamment sa forte dimensionnalité, ses dépendances temporelles et son hétérogénéité inhérente. Cette recherche comble cette lacune en introduisant un nouveau cadre hybride d'apprentissage profond, basé sur l'intégration synergique d'un réseau de mémoire bidirectionnelle à long terme (BiLSTM) et d'un réseau neuronal profond (DNN). Cette architecture innovante est soigneusement conçue pour surmonter les limites des modèles existants en capturant simultanément les séquences temporelles et les caractéristiques spatiales intégrées au trafic réseau IoMT. L'un des principaux apports de ces travaux réside dans la transparence intrinsèque du cadre. Il dépasse l'opacité des modèles traditionnels de type "boîte noire" en intégrant les principes de l'IA explicable (XAI) et en s'appuyant sur les explications additives de SHapley (SHAP). Cette intégration fournit des justifications interprétables par l'humain pour chaque alerte de sécurité, révélant les caractéristiques et les schémas de données spécifiques qui sous-tendent les prédictions du modèle. Cela favorise non seulement la confiance et garantit la responsabilisation, mais facilite également une analyse humaine efficace, permettant au personnel de sécurité de valider les alertes et d'intervenir en toute confiance sans compromettre les soins aux patients. Une évaluation rigoureuse sur le jeu de données de référence complet CICIoMT2024 valide les performances exceptionnelles du cadre, démontrant une grande précision dans la distinction entre 18 types d'attaques distincts et le trafic normal. En combinant harmonieusement des capacités de détection avancées avec une transparence opérationnelle essentielle, cette recherche marque une avancée significative en matière de cybersécurité et d'IA fiable, apportant une solution robuste et vérifiable, essentielle à la protection des données de santé sensibles et au fonctionnement résilient des services médicaux critiques.

Mots clés: e-Santé, Internet des objets médicaux (IoMT), Système de détection d'intrusion (IDS), BiLSTM, DNN, Black-Box, Intelligence artificielle explicative (XAI), SHAP.

ملخص:

يُمثل المشهد المزدهر لإنترنت الأشياء الطبية (IoMT) تحديًا حاسمًا ومتصاعدًا للأمن السيبراني. ومن الواضح أن أنظمة كشف التسلل (IDS) التقليدية غير كافية لهذا المجال، لأنها غير قادرة على إدارة الخصائص الفريدة لحركة مرور شبكة إنترنت الأشياء الطبية (IoMT) بفعالية، بما في ذلك أبعادها العالية، وتبعياتها الزمنية، وتباينها المتأصل. يعالج هذا البحث هذا النقص من خلال تقديم إطار عمل هجين جديد للتعلم العميق، مبني على تكامل تآزري لشبكة ذاكرة طويلة وقصيرة المدى ثنائية الاتجاه (BiLSTM) مع شبكة عصبية عميقة (DNN). وقد صُممت هذه البنية المبتكرة بدقة للتغلب على قيود النماذج الحالية من خلال التقاط كل من التسلسلات الزمنية والميزات المكانية المضمنة في حركة مرور شبكة إنترنت الأشياء الطبية (IoMT) في وقت واحد. ومن المساهمات الأساسية لهذا العمل الشفافية الجوهرية للإطار. يتجاوز هذا النموذج غموض نماذج "الصندوق الأسود" التقليدية من خلال دمج مبادئ الذكاء الاصطناعي القابل للتفسير (XAI)، والاستفادة من تفسيرات SHapley الإضافية (SHAP). يوفر هذا التكامل مبررات قابلة للتفسير البشري لكل تنبيه أمني، كاشفًا عن السمات وأنماط البيانات المحددة التي تُحرك تنبؤات النموذج. هذا لا يعزز الثقة ويضمن المساءلة فحسب، بل يُسهّل أيضًا إجراء تحليل فعال بمشاركة بشرية، مما يُمكّن موظفي الأمن من التحقق من صحة التنبيهات والاستجابة لها بثقة دون المساس برعاية المرضى. يُثبت التقييم الدقيق لمجموعة بيانات CICIoMT2024 الشاملة الأداء الاستثنائي للإطار، مُظهرًا دقة عالية في التمييز بين 18 نوعًا مختلفًا من الهجمات وحركة المرور العادية. من خلال الجمع بسلاسة بين قدرات الكشف المتقدمة والشفافية التشغيلية الأساسية، يُمثل هذا البحث تقدمًا كبيرًا في كل من الأمن السيبراني والذكاء الاصطناعي الموثوق، مما يُسهم في إيجاد حل قوي وقابل للتدقيق، وهو أمر حيوي لحماية بيانات الرعاية الصحية الحساسة وضمان التشغيل المرن للخدمات الطبية الحيوية.

الكلمات المفتاحية: الرعاية الصحية الإلكترونية، إنترنت الأشياء الطبية (IoMT)، نظام كشف التطفل (IDS)، BiLSTM، DNN، الصندوق الأسود، الذكاء الاصطناعي القابل للتفسير (XAI)، SHAP.

Table des matières

Table des figures

Liste des tableaux

General introduction

Contents

0.1 Context

The Internet of Things (IoT) represents a rapidly expanding technological paradigm, characterized by the pervasive integration of lightweight and easily deployable devices into everyday environments [1]. This infrastructure serves as the foundational layer for the development of smart cities, facilitating the convergence of ubiquitous sensing capabilities with advanced data analytics [2]. The IoT ecosystem supports a diverse array of intelligent services across numerous domains, including intelligent transportation systems, precision irrigation, and smart energy grids [3] with one of its most transformative applications emerging within healthcare, commonly designated as the Internet of Medical Things (IoMT) [4]. As a specialized subset of IoT technologies, the IoMT enables real-time health monitoring, diagnostics, and therapeutic interventions through interconnected devices such as wearable biosensors, implantable monitors, and automated infusion pumps [5]. By acquiring and transmitting bio-physiological data across secure communication networks, IoMT systems yield substantial clinical benefits [6], including enhanced remote patient monitoring, reduced hospital readmission rates, and early anomaly detection in chronic disease management [7, 8]. Integration of these technologies within clinical environments has further facilitated personalized treatment pathways and improved operational efficiency through automated data processing. The

where explainability and accountability are as important as detection accuracy [24].

The opacity of these complex models obscures the rationale behind their decisions, eroding trust and complicating accountability a significant liability in healthcare, where security personnel must understand the reasoning behind alerts to take appropriate action without disrupting patient care [23]. This creates a critical need for human-in-the-loop systems where security analysts can validate, contextualize, and act upon AI-generated insights with appropriate discretion [25].

This critical need for transparency and accountability has catalyzed the emergence of Explainable Artificial Intelligence (XAI) as an indispensable discipline within cybersecurity [26]. XAI moves beyond pure predictive performance to prioritize interpretability, aiming to make AI models' internal mechanisms transparent, auditable, and justifiable to human operators. The integration of XAI into IDS frameworks (X-IDS) is not merely a technological enhancement but an operational necessity to build trust, ensure regulatory compliance, and facilitate effective debugging and performance improvements [27].

A foremost technique within XAI is SHAP (SHapley Additive exPlanations) [27]. Rooted in cooperative game theory, SHAP provides a unified, model-agnostic framework to quantify the marginal contribution of each feature to a model's prediction [28]. This capability is particularly valuable for addressing the dimensionality challenges of IoMT security data. Feature selection serves as a crucial preprocessing step to mitigate these problems by identifying and retaining only the most relevant features [29], thereby reducing computational overhead while providing intrinsic insight into the data patterns that drive predictions. Beyond its conventional role in post-hoc interpretation, SHAP is innovatively leveraged for robust feature selection prior to model training [30]. By evaluating the importance of each feature through Shapley values, SHAP enables the creation of optimized feature subsets that enhance model performance and interpretability simultaneously.

0.2 Problematics

The development and deployment of effective Intrusion Detection Systems (IDS) for the Internet of Medical Things (IoMT) face a multifaceted array of challenges that span technical, computational, and human-factored domains. These problematics must be holistically addressed to ensure both the security and operational viability of healthcare systems.

- **Data-Related Challenges:** IoMT network traffic data is often high-dimensional and redundant, which increases computational costs and can lead to model overfitting. A significant issue is the scarcity of labeled data

Internet of Medical Things (IoMT), examining its role in modern e-healthcare, the specific devices that constitute it, and the technological enablers that make it viable. The chapter subsequently outlines the transformative applications of IoMT across the healthcare sector before culminating in a critical analysis of its major challenges, with particular emphasis on security vulnerabilities and privacy concerns, thereby logically introducing the necessity for the advanced, explainable intrusion detection system proposed in this thesis.

- The second chapter examines intrusion detection systems (IDS) tailored for Internet of Medical Things (IoMT) environments. It begins by differentiating IDS from intrusion prevention systems and reviewing core detection methods. The discussion then addresses unique IoMT vulnerabilities and the design adaptations needed for its resource-constrained, high-stakes setting. A significant focus is placed on AI-driven IDS, highlighting how machine learning and deep learning enable proactive threat detection and automated response, while also acknowledging their current limitations. The chapter concludes by exploring emerging research directions, including adversarial robustness, real-time processing, and federated learning for privacy-preserving security in distributed healthcare networks.
- Chapter three introduces HBiLD-IDS, a novel hybrid intrusion detection system designed to secure IoMT networks by analyzing complex spatio-temporal attack patterns. The proposed framework leverages a Bidirectional LSTM (BiLSTM) architecture to process network traffic sequences in both forward and backward directions, capturing contextual dependencies essential for identifying sophisticated threats like intermittent false data injection, followed by a Deep Neural Network (DNN) component that hierarchically refines these features for precise classification. Designed for resource-constrained environments, HBiLD-IDS outperforms alternatives such as CNNs (limited to spatial features), unidirectional LSTMs (lacking full context), Transformers (computationally excessive), and GRUs (limited memory for multi-stage attacks). The framework was rigorously evaluated using the CICIoMT2024 dataset, incorporating explainability-driven feature selection to assess discriminatory power across attack types, ensuring both high accuracy and operational efficiency for IoMT deployments.
- Chapter four outlines our proposed methodology for developing an explainable intrusion detection system (X-IDS) tailored for Internet of Medical Things (IoMT) environments. Our approach addresses the "black box" nature of deep learning by combining a hybrid Bidirectio-

nal Long Short-Term Memory (BiLSTM) and Deep Neural Network (DNN) architecture with Explainable AI (XAI) principles, ensuring a balance between high accuracy and transparency. The process involves several key steps: first, we prepare the CICIoMT2024 dataset through preprocessing steps like cleaning, normalization, and encoding. Next, we train our hybrid BiLSTM-DNN model, which is designed to capture both bidirectional temporal and spatial dependencies in network traffic, enabling it to classify eighteen types of attacks in real time. Finally, we apply the SHAP (SHapley Additive exPlanations) framework to explain the model's decisions and identify the most impactful features. This process allows us to retrain the model on an optimized feature set, improving both efficiency and interpretability, thereby providing security analysts with a trustworthy, actionable system.

Chapitre 1

Internet of Things (IoT)

Contents

1.1 Introduction

The Internet of Things (IoT) refers to the interconnection of various devices to the Internet, including smartphones, home automation systems, and wearable technologies. The Internet of Things (IoT) has its origins in the convergence of several technological innovations that emerged over the decades: as early as the 1970s and 1980s, advances in microprocessors and communication networks paved the way for the idea of connecting machines, while in 1990 John Romkey made headlines by linking a toaster to the Internet, an act often cited as one of the first examples of a connected object; a few years later, in 1999, Kevin Ashton, a researcher at MIT, coined the term Internet of Things when referring to the use of RFID technology to identify and link physical objects to the network, marking a decisive turning point; during the 2000s, the widespread adoption of Wi-Fi, the rise of sensors, and the advent of the first smartphones enabled connected devices to gain a foothold in logistics, healthcare, and home automation, thus preparing the ground for the boom of the 2010s, an era in which cloud platforms, big data, and artificial intelligence made it possible to analyze in real time the massive streams of data generated by sensors deployed in homes, cities, and industries; today, IoT relies on 5G, edge computing, and embedded AI to deliver increasingly diverse applications, ranging from autonomous vehicles to smart agriculture, while raising new challenges related to security, interoperability, energy management, and privacy protection, thereby confirming that IoT is the natural evolution of the Internet toward a world where objects communicate and cooperate as much as humans do.

1.2 Internet of Things

1.2.1 Definitions

The term "Internet of Things" (IoT) traces its lexical origin to Kevin Ashton's 1999 presentation at Procter Gamble (PG) and his related work at the MIT Auto-ID Center [31]. This conceptual framework emerged principally from linking the use of RFID (radio-frequency identification) technology in Procter & Gambles supply chain to the Internet, emphasizing two core capabilities: (1) real-time tracking of physical objects' geospatial positioning and (2) continuous monitoring of operational status. These capabilities were designed to address supply chain optimization challenges, particularly by enhancing item-level visibility across distribution networks [32].

"If we had computers that knew everything there was to know about thingsusing data they gathered without any help from uswe would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best [31]"

One of the earliest and most influential contributions to the conceptualization of the Internet of Things (IoT) was the International Telecommunication Union (ITU) report published in 2005 [33].

"Internet of things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies [33]."

The ITU envisioned a transformative paradigm where everyday objects can be integrated into communication networks, supported by the emergence of high-speed mobile networks offering always-on connectivity; would become active participants on the Internet, autonomously exchanging data on behalf of humans. This technological convergence would realize a truly ubiquitous (pervasive) network, accessible anytime, anywhere, by anyone and anything [33]. And further framed IoT as a cyber-physical ecosystem, where every entity in the physical world would possess a digital identity in virtual cyberspace. This digital representation would enable seamless: Human-to-thing interactions (e.g., remote monitoring) and Thing-to-thing communications (e.g. automated systems) [34].

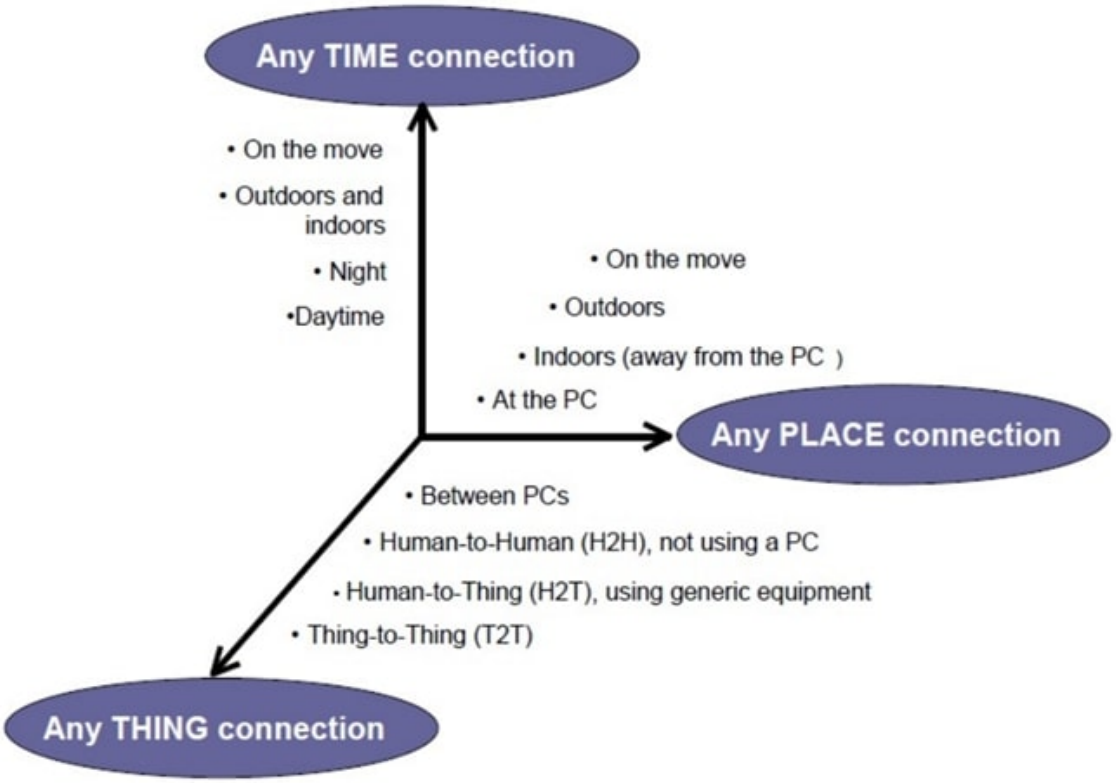

Figure 1.1: *New dimension introduced in the Internet of things [b-ITU Report].*

Moreover, multiple authoritative definitions have emerged to characterize the Internet of Things (IoT). The IERC defines IoT as "a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network" [35]. Similarly, the IEEE (Institute of Electrical and Electronics Engineers) describes IoT as *"a framework that integrates sensing, communication, actuation, and analytics to enable smart interactions between objects and their environments" [36]. Gartners definition characterizes it as "the network of physical objects that contain embedded technology to communicate and interact with their internal states or the external environment"* [36].

Together, these definitions collectively expand on the ITU's original paradigm while maintaining its key tenets of ubiquitous connectivity, cyber-

physical integration, and autonomous interaction.

The Internet of Things (IoT) constitutes a cyber-physical ecosystem formed through seamless integration of digital and physical worlds, delivering context-awareness real-world services adapted to human presence and environmental changes [37]. At its functional core, IoT empowers: (1) intelligent automation [38], (2) continuous real-time monitoring [39], and (3) evidence-based decision-making powered by predictive analytics [39]; with demonstrated implementations across critical sectors including healthcare (remote patient monitoring), precision agriculture (automated irrigation systems), smart manufacturing (digital twin implementations), and smart cities (adaptive traffic control).

1.2.2 IoT Characteristics

1.2.2.1 Interconnected

IoT devices are linked through networks, allowing seamless communication and data exchange between devices, systems, and applications. This interconnectedness enables coordinated operations, remote management, and integrated processes across various environments [40].

1.2.2.2 Smart sensing

IoT employs advanced sensors that collect real-time data from the physical environment, such as temperature, humidity, motion, and light. These sensors are highly responsive and accurate, facilitating precise monitoring and data collection for informed decision-making [41].

1.2.2.3 Intelligence

IoT systems incorporate artificial intelligence and machine learning algorithms to analyze the collected data, recognize patterns, and make autonomous decisions or predictions [42]. This intelligence enhances automation, efficiency, and the ability to respond proactively to changing conditions.

1.2.2.4 Energy efficiency

IoT devices are designed to optimize energy consumption by using low-power sensors, efficient communication protocols, and smart power management

techniques [43]. This ensures longer device lifespan, reduced operational costs, and a minimal environmental footprint.

1.2.2.5 Expressing (Sharing of Data)

IoT enables the flexible and secure sharing of data across devices, platforms, and users [44]. This sharing facilitates collaborative efforts, remote monitoring, real-time updates, and enhanced transparency, fostering better insights and decision-making.

1.2.2.6 Safety

Security is a vital feature of IoT, involving encryption, authentication, and other protective measures to safeguard data and devices from cyber threats. Ensuring safety also includes maintaining the integrity and privacy of user data, as well as reliable operation to prevent accidents or failures [45].

1.2.3 IoT Functional Peculiarities

1.2.3.1 Gather Information from Things

This function involves collecting data from physical objects or "things" equipped with sensors. These sensors detect various environmental and operational parameters such as temperature, humidity, motion, light, pressure, or location. The process of perception transforms physical phenomena into digital data that can be analyzed and used for further actions [46].

1.2.3.2 Exchange Information

Once data is gathered, IoT systems facilitate the transfer of this information between devices, sensors, servers, and users. This exchange occurs over various communication protocols like Wi-Fi, Bluetooth, Zigbee, 4G/5G, or LPWAN technologies. Efficient and secure data exchange ensures real-time or near-real-time communication, enabling responsive actions and coordination across the system [47].

1.2.3.3 Intelligent Information Processing or Control

After data exchange, IoT systems process the information using data analytics, machine learning, or rule-based algorithms to derive meaningful insights [48]. Based on these insights, the system can make autonomous decisions, trigger alerts, or control connected devices such as turning on a motor, adjusting lighting, or sending notificationsthus enabling smart automation and responsive control.

1.2.3.4 Large Scale

IoT systems are designed to operate on a large scale, managing thousands or even millions of connected devices across different locations or networks. This scalability allows for extensive deployments like smart cities, industrial automation, agricultural monitoring, and large-scale healthcare systems, ensuring seamless integration, management, and coordination of numerous interconnected components [49].

1.2.4 Components of IoT Ecosystem

1.2.4.1 Sensors and Actuators

- **Sensors:** Sensors are devices that detect and measure physical phenomena such as temperature, humidity, motion, light, pressure, and various other environmental conditions. They convert these physical signals into electrical or digital data that can be processed by other systems. Often referred to as the "eyes" and "ears" of an IoT system, sensors provide real-time data crucial for monitoring and decision-making [50].
- **Actuators:** Actuators are devices that perform actions based on instructions from the system or processed data [50]. They convert electrical signals into physical actions, enabling IoT systems to interact with and control their environment. Acting as the system's "muscles," actuators include devices such as motors, switches, relays, valves, servos, and displays.

1.2.4.2 Connectivity Modules

These are hardware components that enable communication between sensors, actuators, and other parts of the IoT system. They support various wireless

and wired protocols like Wi-Fi, Bluetooth, Zigbee, LoRaWAN, NB-IoT, or Ethernet, ensuring reliable data transfer across the network [51].

1.2.4.3 Edge-Fog Computing Devices

- **Edge computing:** refers to the processing of data close to the source of data generation, such as sensors or IoT devices, using local devices like gateways, routers, or edge servers to analyze and handle data before transmitting it to the cloud. Its primary purpose is to reduce latency, conserve bandwidth, and enable real-time decision-making by allowing systems to respond swiftly without dependence on distant cloud servers [52].
- **Fog computing:** extends cloud computing by incorporating a layer of intermediate processing nodes called fog nodes, which are distributed across the network closer to data sources but generally more centralized than individual edge devices. Its main purpose is to enable scalable, low-latency, and context-aware computing by providing a decentralized data processing layer; fog nodes can aggregate and analyze data from multiple edge devices, handle complex tasks, and offer local analytics and storage [52].

1.2.4.4 Cloud Platform

A centralized cloud infrastructure that stores, manages, and processes large volumes of data collected from IoT devices [53]. It provides scalable storage, remote access, device management, and integration with other enterprise systems. The cloud acts as the core hub for advanced processing and data sharing.

1.2.4.5 Data Analytics and AI

This component involves applying data analytics, machine learning, and artificial intelligence algorithms to the collected IoT data. It helps uncover insights, predict future states, optimize operations, and enable autonomous decision-making, making the IoT ecosystem "smart" [48].

1.2.4.6 Used Interfaces

User interfaces and dashboards (web or mobile apps) that allow humans to interact with, monitor, and control IoT devices and systems. These inter-

faces are designed for ease of use and provide insights, alerts, and control functionalities to users.

1.2.5 IoT Framework Architecture

The IoT framework is built on interconnected layers that organize core components and functions, creating a structured methodology for designing, developing, and deploying reliable IoT systems [54]. This layered architecture ensures seamless data flow, modular scalability, and efficient system integrationkey foundations for successful IoT implementations (see Figure 1.2 [55]).

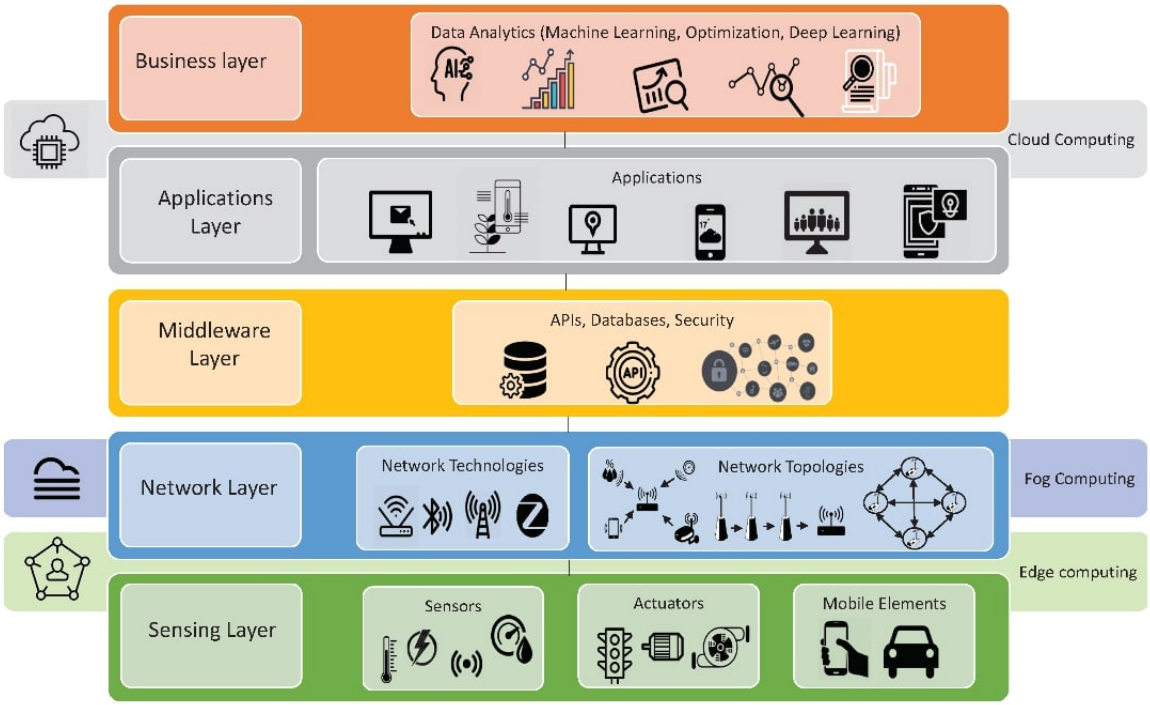

Figure 1.2: *IoT Framework Layers.*

1.2.5.1 Principal Layers

1.2.5.1.1 Perception Layer (Edge Layer): The perception layer serves as the foundational stratum of the IoT framework, facilitating direct interaction with the physical environment through data acquisition mechanisms [56]. This layer comprises sensory apparatuses (including temperature, motion, and humidity sensors), actuation components (such as motors

and relays), and embedded smart devices (wearables and edge nodes). It employs low-power communication protocols including Bluetooth Low Energy (BLE), Zigbee, and RFID/NFC technologies to enable efficient data collection while maintaining energy efficiency [57]. This layer's primary function involves the transduction of physical phenomena into digital signals, forming the essential data input for subsequent processing layers.

1.2.5.1.2 Network/Transport Layer: The network layer establishes the critical communication infrastructure necessary for secure and reliable data transmission across the IoT ecosystem. This stratum incorporates gateway devices, routing equipment, and specialized network security modules to ensure data integrity during transmission. It utilizes a heterogeneous mix of communication technologies ranging from short-range protocols (Wi-Fi 6) to wide-area networks (5G, LPWAN), alongside specialized IoT messaging protocols such as MQTT, CoAP, and AMQP [58]. The layer's architecture is particularly designed to address the challenges of intermittent connectivity and bandwidth constraints while maintaining robust security measures against potential cyber threats.

1.2.5.1.3 Processing and Middleware Layer: The Processing Layer and Middleware Layer collectively form the computational and integration backbone of IoT systems, enabling efficient data management and system interoperability [59]. Functioning as the computational core, the Processing Layer performs critical data aggregation, transformation, and analytical operations through a multi-tiered architecture comprising edge nodes (for real-time processing), fog computing infrastructure (for localized analytics), and cloud-based units (for large-scale computations). This layer leverages distributed frameworks (Apache Kafka, Spark), containerization technologies (Docker, Kubernetes), and edge AI platforms (TensorFlow Lite) to transform raw sensor data into actionable insights while optimizing resource allocation. Complementing this, the Middleware Layer acts as a vital intermediary that abstracts hardware and protocol heterogeneity, ensuring seamless integration between devices, networks, and applications [60]. It provides essential services such as device management (discovery, provisioning, OTA updates), protocol translation (MQTT - HTTP), and secure data transmission (authentication, encryption). By aggregating, filtering, and preprocessing data, the middleware reduces the computational burden on downstream layers while enabling reliable communication. Together, these layers address key IoT challenges: the Processing Layer delivers scalable analytics and decision-making capabilities, while the Middleware Layer ensures interoperability, se-

curity, and efficient data flow. Their synergy enhances system flexibility, supports real-time operations, and simplifies the deployment of intelligent IoT solutions across diverse domains, from industrial automation to smart healthcare.

1.2.5.1.4 Application Layer: The application layer represents the service-oriented stratum that delivers value-added functionalities to end-users through specialized interfaces and integration modules [55]. This layer incorporates user-facing dashboards, notification systems, and API gateways that enable seamless integration with existing enterprise systems. It leverages standardized web technologies (RESTful APIs, GraphQL) and cloud-based IoT platforms (AWS IoT Core, Azure IoT Hub) to provide customizable application environments. The layer's primary function involves the contextualization of processed data into domain-specific applications that address particular use cases across various industrial and consumer domains.

1.2.5.1.5 Business Layer: As the strategic apex of the IoT framework, the business layer provides decision-support capabilities through advanced analytics and business intelligence functionalities. This layer integrates analytical dashboards, enterprise resource planning (ERP) systems, and machine learning models to derive strategic insights from IoT-generated data. It employs sophisticated business intelligence tools (Power BI, Tableau) and cognitive computing platforms (IBM Watson) to facilitate data-driven decision making [61]. The layer's architecture enables organizations to transform operational data into competitive advantage through predictive analytics, optimization algorithms, and strategic planning modules.

1.2.5.2 IoT Architecture

The Internet of Things (IoT) ecosystem relies on various architectural frameworks to address diverse requirements such as scalability, real-time processing, security, and interoperability. Below is a comparative analysis of the most widely adopted IoT architectures, highlighting their key features, advantages, limitations, and use cases.

1.2.5.2.1 Three-Layer IoT Architecture: The three-layer architecture represents the fundamental IoT framework consisting of perception,

network, and application layers. The perception layer handles data acquisition through sensors and actuators, while the network layer manages communication via protocols like Wi-Fi and Bluetooth. The application layer delivers user-facing services and interfaces [62]. This model offers simplicity and ease of implementation, making it ideal for basic IoT deployments such as smart home systems. However, its lack of intermediate processing layers limits scalability and makes it unsuitable for complex enterprise applications requiring advanced analytics or real-time processing capabilities.

1.2.5.2.2 Five-Layer IoT Architecture: Extending beyond the basic model, the five-layer architecture incorporates transport and processing layers between the traditional components, along with a dedicated business layer [62]. The transport layer ensures reliable data transmission using protocols like MQTT and CoAP, while the processing layer enables edge/cloud analytics and AI-driven transformations. The business layer facilitates enterprise integration and decision-making [63]. This comprehensive structure supports complex industrial applications including smart cities and healthcare monitoring systems, though its sophisticated infrastructure requirements increase deployment complexity compared to simpler models.

1.2.5.2.3 Cloud-Centric IoT Architecture: This architecture centralizes data processing and storage in cloud platforms like AWS IoT and Azure IoT, following a devices-gateway-cloud-application data flow. It provides exceptional scalability for big data applications and cost-effective long-term analytics solutions, making it suitable for large-scale deployments such as smart agriculture [64]. However, its reliance on cloud connectivity introduces latency issues that preclude its use in time-sensitive applications, while internet dependency creates potential single points of failure in the system architecture.

1.2.5.2.4 Fog/Edge IoT Architecture: The fog/edge model decentralizes processing by performing computations near data sources through local nodes before optional cloud transmission. This approach minimizes latency for critical applications like autonomous vehicles and industrial robotics while reducing bandwidth consumption [65]. Despite these advantages, the architecture demands significant investment in edge infrastructure and offers limited storage capacity compared to cloud alternatives, presenting cost-benefit considerations for implementation.

Table 1.1: *IoT Architecture Comparison*

Architecture	**Key Features**	**Use Case Domains**	**Limitations & Challenges**
Three-Layer	Simple & modular	Basic IoT projects needing quick deployment (Smart homes, wearables)	Limited scalability
Five-Layer	Detailed enterprise support	Large-scale systems requiring robust processing and analytics (Industrial IoT, smart grids)	Complex deployment
Cloud-Centric	Scalable cloud processing	Applications needing massive storage and AI/ML (Big data analytics, smart agriculture)	Latency issues, internet dependency
Fog/Edge	Low-latency processing	Real-time systems where milliseconds matter (Autonomous vehicles, industrial robots)	High infrastructure cost

1.3 IoT-based Healthcare (IoMT)

1.3.1 Healthcare

Healthcare is the organized, comprehensive system of services and practices designed to promote, maintain, and restore health [66]. It encompasses a broad spectrum of activities including medical diagnosis, treatment, prevention, rehabilitation, health education, and support services delivered by trained health professionals such as doctors, nurses, pharmacists, therapists, and other healthcare providers [67].

The primary aim of healthcare is to improve individual and public health outcomes by detecting and managing illnesses early, preventing disease, and enhancing overall well-being [68]. Healthcare can be delivered through va-

rious settings such as hospitals, clinics, community health centers, and even through telemedicine and digital health platforms [69]. It also involves the use of technological advancementslike electronic health records, medical devices, and health information systemsto enhance efficacy, accessibility, and quality of care [70].

Effective healthcare systems are characterized by equitable access, affordability, safety, patient-centeredness, and continuous quality improvement [71]. Ultimately, healthcare plays a vital role in enabling individuals and communities to lead healthier, more productive lives.

1.3.2 e-Healthcare

E-healthcare refers to the use of electronic communication and digital technologies to deliver healthcare services, improve patient care, and enhance healthcare management [72]. It encompasses a broad range of tools and platforms, including electronic health records (EHRs), health information systems, telemedicine, online appointment scheduling, and digital health education [73]. By leveraging these technologies, e-healthcare aims to make healthcare more accessible, efficient, and patient-centered while significantly improving quality of life [74] through by (1) enabling personalized care through data-driven treatment tailoring, (2) facilitating chronic disease management (e.g., diabetes, hypertension) via remote monitoring and timely interventions, (3) enhancing health literacy with accessible digital education and self-management tools, and (4) reducing healthcare access barriersgeographic, economic, and mobility-relatedthrough decentralized digital solutions.

This digital transformation is redefining care delivery by optimizing clinical efficiency (cost reduction, time savings) while restructuring care access through three key mechanisms: (1) Precision hospitalization enabled by continuous remote monitoring and AI-driven early alerts, reducing unnecessary admissions [75], (2) Expanded home-based care through remote monitoring technologies and integrated digital health platforms, (3) Democratized health systems via decentralized telemedicine platforms that transcend geographic and socioeconomic barriers [76].

This approach concurrently advances all five dimensions of the Quintuple Aim [77] by simultaneously targeting five evidence-based domains as shown in figure 1.3 [78]: (1) enhancing clinical outcomes (e.g., reduced hospital readmissions, improved chronic disease management), (2) optimizing patient experience through patient-centered care models, (3) advancing health equity by addressing structural determinants of health, (4) improving health

system efficiency via lean workflow redesign, and (5) safeguarding clinician well-being through burnout mitigation strategies (e.g., workload reduction, organizational support) [79].

Figure 1.3: *Quintuple Aim Framework.*

1.3.3 The Internet of Medical Things (IoMT)

The application of the Internet of Things (IoT) in the healthcare domain, often referred to as the Internet of Medical Things (IoMT), is revolutionizing the delivery, monitoring, and management of medical services through

pervasive connectivity and intelligent data analytics [4]. IoMT comprises interconnected medical devices, wearables, sensors, and equipment that collect, exchange, and analyze health data in real time. This transformative paradigm shift facilitates remote patient monitoring (RPM), predictive diagnostics, and personalized therapeutic interventions, thereby enhancing clinical decision-making and patient outcomes while optimizing healthcare workflows [80].

As a leading e-healthcare technology, the Internet of Medical Things (IoMT) collects critical physiological and pathological data, such as heart rate, blood pressure, and oxygen saturation, enabling continuous remote monitoring and early detection of health issues. Its applications span wireless body area networks (WBAN) [81], implantable devices, and beyond, enhancing personalized and preventive care. Beyond patient monitoring, IoMT improves asset management, medication adherence, and hospital workflows, reducing costs and increasing safety. By integrating IoMT into healthcare systems, providers can deliver more proactive, efficient, and data-driven care, paving the way for a healthier future. Figure 1.4 shows General IoMT Ecosystem [82].

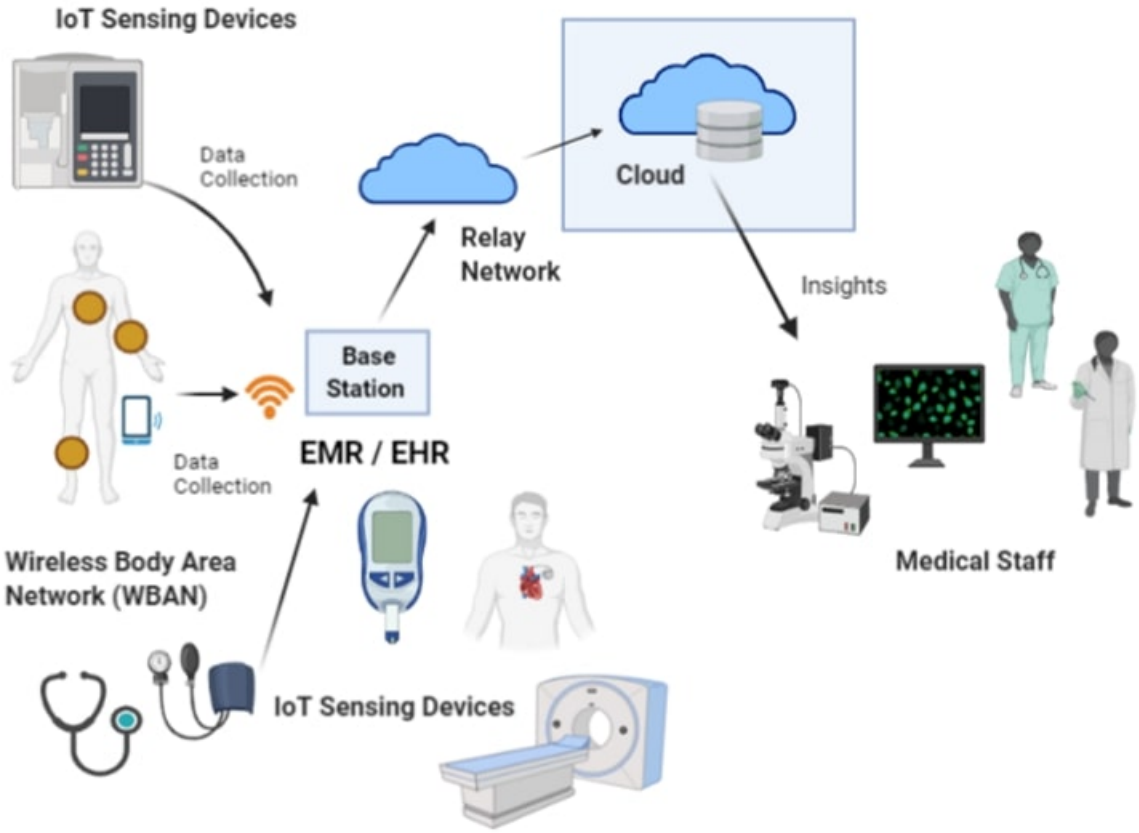

Figure 1.4: *General IoMT Ecosystem.*

1.3.4 Healthcare perception devices

Alternatively termed medical perception devices or health sensing devices, constitute a class of advanced technological instruments designed to monitor, detect, and analyze physiological signals in real time [83]; ranging from simple body sensors that acquire biomedical signals to more complex and specialized surgical tools. As shown in Table 1.2, these devices facilitate the acquisition of critical health-related data, enabling continuous patient assessment, early diagnosis, and personalized therapeutic interventions [84,85]. By integrating biosensors, artificial intelligence (AI), and Internet of Things (IoT) technologies, healthcare perception devices enhance clinical decision-making and support proactive healthcare management [86].

Table 1.2: *Classification of Healthcare Devices*

Device Category	**Subcategory**	**Examples**	**Clinical Application**
Patient Monitoring Devices	Clinical Monitors	Heart rate monitors, Pulse oximeters, ECG monitors, Ventilators, Capnography systems	Continuous vital sign tracking in ICUs/ORs, Anesthesia depth monitoring
Medical Imaging & Therapy Devices	-	MRI/CT scanners, Infusion pumps, Smart stethoscopes, Telemetry devices	Diagnostic imaging, Precision medication delivery, Remote auscultation
Smart Room Technologies	-	Fall detection systems, Smart beds, Hygiene monitors	Elderly care, Pressure ulcer prevention, Infection control
Remote Chronic Disease Management	Wearables	Smart watches (ECG/SpO_2), Biopatches, Glucose monitoring bands	Diabetes management, Cardiac arrhythmia detection
	Implantables	Pacemakers, Neurostimulators, Swallowable endoscopy capsules	Cardiac rhythm control, Parkinson's therapy, GI diagnostics
	Remote Clinical Tools	Bluetooth glucometers, Connected spirometers, Home BP monitors	COPD management, Hypertension tracking
Real-Time Location Services (RTLS)	Staff Tracking	RFID badges, NFC-enabled ID cards	Workflow optimization, Contact tracing
	Patient Tracking	Infant abduction tags, Dementia wander prevention bracelets	Pediatric security, Cognitive impairment care
	Asset Management	Smart medication cabinets, Tagged wheelchairs/IV pumps	Equipment utilization tracking, Inventory control
Facility Monitoring Systems	Environmental Controls	Smart HVAC, Water quality sensors, Lighting automation	Infection prevention, Energy efficiency
	Building Management	Elevator monitoring, Power grid analytics	Emergency preparedness, Infrastructure maintenance
	Security Systems	AI video surveillance, Biometric access controls	Patient/staff safety, Data security compliance

1.3.5 Network Modules and Communication Channels

These components ensure secure and reliable communication of collected biomedical data between patients, medical staff, and various medical facilities. This often involves wireless body area networks (WBANs) and hybrid communication approaches like Bluetooth Low Energy and Wi-Fi for flexible data transmission.

1.3.5.1 Technological Enablers

1.3.5.1.1 Electronic Health Records (EHR): EHR systems serve as the foundational digital infrastructure for IoMT ecosystems, enabling the aggregation and standardization of patient data from disparate medical devices (Figure 1.5) [87]. Modern IoMT architectures leverage Fast Healthcare Interoperability Resources (FHIR) standards to facilitate real-time bidirectional data exchange between EHR platforms and connected medical devices [88]. This integration supports comprehensive patient profiles that incorporate continuous vital sign monitoring data alongside traditional clinical documentation, enhancing care coordination across inpatient and ambulatory settings. However, challenges persist regarding semantic interoperability between proprietary EHR systems and the growing array of IoMT endpoints.

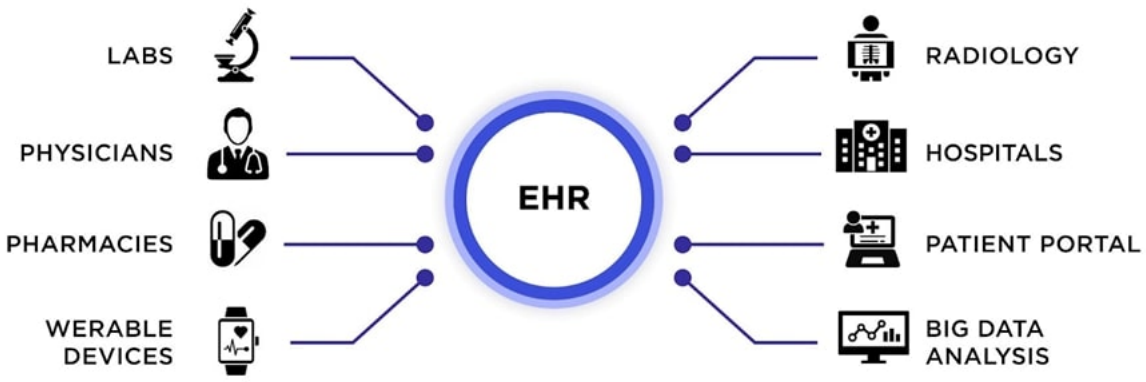

Figure 1.5: *EHR ecosystem.*

1.3.5.1.2 Medical Imaging in IoMT Networks: The incorporation of diagnostic imaging modalities into IoMT frameworks represents a significant advancement in connected healthcare. Edge computing-enabled imaging devices (e.g., portable ultrasound systems, AI-assisted X-ray machines) can perform preliminary image analysis at the point of care while transmitting DICOM-standard studies to cloud-based picture archiving and communication systems (PACS) [89]. This distributed architecture reduces critical turnaround times for emergency diagnostics while maintaining compliance with data-intensive medical imaging requirements. Emerging applications include real-time teleradiology consultations and automated anomaly detection through deep learning algorithms trained on federated imaging datasets.

1.3.5.1.3 Artificial Intelligence: AI/ML algorithms constitute the analytical core of advanced IoMT implementations, operating across three architectural tiers: edge-based inference models for time-sensitive processing (e.g., seizure detection algorithms in neuromodulation devices), fog-based adaptive learning systems, and cloud-based predictive analytics [9]. Ensemble techniques combining physiological data streams with EHR-derived clinical histories enable precision medicine applications, such as personalized chemotherapy regimens based on continuous toxicity monitoring [90]. Current research focuses on developing explainable AI (XAI) frameworks to address regulatory concerns regarding algorithmic transparency in clinical decision support systems [91].

1.3.5.1.4 Blockchain for IoMT Data Integrity: Distributed ledger technologies address critical security and trust challenges in IoMT networks through three primary mechanisms: (1) Immutable audit trails for regulated medical device data, (2) Smart contract-enabled automated compliance (e.g., HIPAA-compliant data sharing agreements), and (3) Decentralized identity management for patients and devices [92]. Hybrid blockchain architectures (combining private permissioned chains with public verifiable ledgers) are emerging as the preferred solution for balancing performance requirements with regulatory mandates [93]. Notable implementations include pharmaceutical supply chain provenance tracking and consent management for multi-institutional research studies using IoMT-generated health data.

1.3.5.1.5 Federated Learning in Distributed IoMT Networks: The healthcare sector's adoption of federated learning (FL) frameworks resolves the fundamental tension between data privacy and AI model efficacy [94]:

- Device-level FL: Wearables collaboratively train personalization models without exporting raw physiological data.
- Institutional FL: Hospitals jointly develop diagnostic algorithms while keeping sensitive imaging data localized.
- Cross-modal FL: Heterogeneous data sources (EHRs, sensors, imaging) contribute to composite models through representation fusion.

1.3.5.2 IoMT Applications

The Internet of Medical Things (IoMT) has emerged as a transformative paradigm in healthcare delivery, enabling a wide spectrum of applications across clinical and operational domains. As demonstrated in Table 1.3, these connected medical devices and systems significantly enhance three critical aspects of modern healthcare: (1) patient-centered care delivery, (2) operational efficiency in healthcare facilities, and (3) measurable improvements in clinical outcomes.

Table 1.3: *Comparative Analysis of IoMT Applications Across Healthcare Domains*

Healthcare Domain	**IoMT Application**	**Key Functionality**	**Primary Benefits**
Remote Patient Monitoring	Remote Health Monitoring	Tracks vitals (e.g., heart rate, SpO_2, ECG) via wearables	Early anomaly detection, reduces hospitalizations
	Disease Prediction	AI analyzes health data to predict risks (e.g., diabetes, heart disease)	Proactive care, personalized interventions
	Automatic Insulin Injection	Smart pumps adjust insulin doses in real-time	Improves diabetes management, prevents complications
Telemedicine & Virtual Care	Mental Health Monitoring	Wearables/apps track mood, stress, and anxiety	Enables early intervention for mental health crises
	Non-Invasive e-Medical Care	Remote diagnostics (e.g., ultrasound, dermatology via AI)	Reduces need for in-person visits, lowers costs
Smart Hospitals	Smart Clinical Environments	Integrates IoMT with EHRs, tracks assets (RFID/BLE)	Enhances workflow efficiency, reduces errors
Personalized Medicine	Human Behavior Prediction	AI models behavior patterns (e.g., dementia, Parkinsons)	Tailors care plans, improves quality of life
	Medication Management	Smart dispensers with reminders/adherence tracking	Reduces medication errors, improves compliance
Emergency & Safety	Fall Detection	Wearables detect falls and alert caregivers	Faster emergency response, especially for elderly
	Seizure Detection	Monitors neurological activity (e.g., EEG wearables)	Alerts caregivers during epileptic episodes
Rehabilitation & Elder Care	Sleep Monitoring	Tracks sleep cycles, detects disorders (e.g., apnea)	Improves sleep hygiene, identifies underlying conditions
	Stress & Anxiety Monitoring	Biometric sensors (HRV, skin conductance) assess mental state	Early mental health intervention
Surgical & Procedural	IoMT-Assisted Surgery	Robotics and real-time intraoperative monitoring	Enhances precision, reduces complications
Data & AI	Health Data Analytics & AI	Predictive analytics for risk stratification	Improves diagnosis accuracy, optimizes decisions

1.3.5.3 Challenges & Considerations

The rapid adoption of IoMT presents transformative opportunities but also introduces critical challenges that must be addressed to ensure secure, equitable, and sustainable healthcare innovation. Below is an expanded analysis of the major hurdles:

1.3.5.3.1 Scalability: The widespread implementation of Internet of Medical Things (IoMT) technologies faces considerable obstacles within healthcare systems, chiefly stemming from inadequate infrastructure and financial constraints. Current healthcare facilities often lack sufficient cloud and edge computing capabilities to handle the massive data volumes produced by extensive IoMT networks. These technological shortcomings are further exacerbated by the considerable costs associated with deploying IoMT solutions across different healthcare environments, from urban hospitals to rural clinics. According to [95], these expenses encompass not just equipment procurement but also substantial investments in personnel training, rendering full-scale IoMT adoption economically challenging.

1.3.5.3.2 Interoperability: The effective implementation of Internet of Medical Things (IoMT) technologies faces significant interoperability challenges stemming from device fragmentation and inadequate standardization, as proprietary communication protocols in many IoMT devices prevent seamless integration with other medical systems and electronic health records (EHRs), creating data silos that impair care coordination. The lack of universally adopted technical standards, increasing integration costs and posing patient safety risks through potential data misinterpretation. These challenges are particularly acute in complex care environments, where data aggregation from disparate monitoring systems frequently leads to clinical errors, necessitating coordinated efforts among regulatory bodies, providers, and developer to establish universal standards and develop transitional solutions for legacy systems [96].

1.3.5.3.3 Mobility and Connectivity: The effectiveness of Internet of Medical Things (IoMT) devices, including medical wearables and implants, is fundamentally constrained by their dependence on reliable wireless connectivity, requiring stable high-bandwidth networks (5G/Wi-Fi/Bluetooth) for real-time biosignal transmission, yet significant reliability gaps persist - particularly in rural and low-resource areas with underdeveloped infrastructure [97]. Current data reveals that 37% of the global population lacks consistent broadband access, directly impairing IoMT's remote patient monitoring capabilities [97], while technical analyses demonstrate that 15% of critical data transmissions from cardiac implants fail due to connectivity disruptions, potentially delaying life-saving interventions [98]. Even urban implementations face challenges, as network congestion and 2-5 second handoff delays during 4G/5G transitions compromise emergency response systems [99], highlighting how ostensibly brief interruptions can critically im-

pact time-sensitive medical scenarios. These connectivity barriers must be addressed to realize IoMT's full potential in transforming patient care and reducing healthcare disparities.

1.3.5.3.4 Data Acquisition Stream Handling: The exponential growth of high-volume physiological data streams, generated through continuous vital signs monitoring, presents formidable computational challenges for existing healthcare infrastructures. Modern IoMT networks are capable of generating in excess of 1.7 terabytes of patient data daily per hospital system, thereby exceeding the processing capacity of conventional healthcare IT architectures [100]. This substantial data deluge particularly strains traditional Electronic Health Record (EHR) systems, with studies indicating that 72% of hospitals experience system slowdowns during peak monitoring periods (HIMSS Analytics, 2023). The computational burden is further compounded by the imperative for real-time analytics, wherein cloud-based processing introduces potentially dangerous latency. Research demonstrates that transmission and analysis delays averaging 11.3 seconds for critical metrics, such as electrocardiograms (ECG) and peripheral capillary oxygen saturation (SpO2), can postpone life-saving clinical interventions by 23% (Yang et al., 2023). These temporal bottlenecks prove most consequential in time-sensitive care scenarios, where, for instance, each second of delay in stroke detection has been shown to increase mortality risk by 1.2% [101]. Emerging solutions to mitigate these challenges include edge computing implementations, which reduce processing latency to under 500 milliseconds by analyzing data at the network periphery [102], coupled with artificial intelligence (AI)-driven triage systems designed to prioritize critical data streams [103].

1.3.5.3.5 Security & Privacy: Cyberattack Vulnerabilities: IoMT devices are prime targets for ransomware and man-in-the-middle attacks [104].

Data Leak Risks: Weak encryption exposes sensitive patient data (e.g., cardiac rhythms, mental health logs).

1.3.5.3.6 Ethical & Legal Concerns: Algorithmic Bias: AI models trained on non-diverse datasets may misdiagnose minority groups.

Informed Consent: Patients often unknowingly share health data with third-party vendors.

1.3.5.3.7 Explainable AI (XAI): Black-Box Decisions: Clinicians distrust AI diagnostics without transparent reasoning (e.g., "Why did the algorithm flag this ECG?").

Regulatory Scrutiny: FDA requires interpretability for AI-based IoMT approvals.

1.3.5.3.8 Underdeveloped Country Challenges: Infrastructure Gaps: Lack of electricity, internet, and trained personnel limits IoMT adoption.

Cost Prohibitions: Advanced IoMT devices (e.g., smart insulin pumps) are unaffordable in low-resource settings.

1.4 Conclusion

This chapter has systematically examined the Internet of Things (IoT), tracing its evolution from nascent machine-to-machine connectivity to its current status as a global cyber-physical infrastructure mediating physical and virtual domains. Drawing upon foundational definitions, from Ashton's RFID-centric formulation to the ITU's characterization of IoT as an interoperable global infrastructure, the analysis established that IoT architectures intrinsically support three core capabilities: intelligent automation, continuous real-time monitoring, and evidence-based decision-making predicated on predictive analytics. The investigation into IoT's defining characteristics, interconnectedness, smart sensing, intelligence, energy efficiency, expressive data sharing, and safety, revealed that the paradigm transcends mere device connectivity, enabling autonomous, context-aware cooperation among heterogeneous entities. The deconstruction of IoT ecosystem components, comprising sensors and actuators, connectivity modules, edge-fog computing devices, cloud platforms, data analytics frameworks, and user interfaces, illuminated the multi-tiered complexity requisite for transforming raw sensory data into actionable intelligence across applications spanning smart automation, precision agriculture, and urban infrastructure management.

The chapter's second major focus constituted an in-depth investigation of IoT's transformative instantiation within healthcare delivery, denominated the Internet of Medical Things (IoMT). The analysis demonstrated how IoMT facilitates remote patient monitoring, predictive diagnostics, personalized therapeutic interventions, and optimized clinical workflows, thereby concurrently advancing all five dimensions of the Quintuple Aim: enhanced clinical outcomes, optimized patient experience, advanced health equity,

improved system efficiency, and safeguarded clinician well-being. Key technological enablers, including FHIR-standardized Electronic Health Records, edge-coupled medical imaging systems, artificial intelligence deployed across edge-fog-cloud tiers, blockchain architectures ensuring immutable audit trails, and federated learning frameworks resolving the tension between data privacy and model efficacy, were shown to collectively address the heterogeneous demands of connected care. Notwithstanding these transformative affordances, however, substantial barriers impede the full realization of IoMT's potential, including scalability constraints arising from inadequate infrastructure and prohibitive costs, interoperability deficits stemming from device fragmentation and proprietary protocols, and persistent connectivity gaps affecting approximately 37% of the global population.

The computational burden imposed by high-volume physiological data streams, with modern IoMT networks generating over 1.7 terabytes of patient data daily per hospital system, overwhelms conventional healthcare IT architectures and introduces hazardous latency, evidenced by transmission delays averaging 11.3 seconds for critical metrics such as electrocardiography. Security vulnerabilities, including ransomware attacks and data leakage risks from inadequate encryption, threaten patient privacy and system integrity, while ethical and legal considerations, algorithmic bias, inadequacies in informed consent, the opacity of black-box AI diagnostics necessitating explainable AI (XAI) frameworks, and infrastructure deficits confronting underdeveloped countries, further complicate equitable IoMT adoption. In synthesis, IoT and IoMT constitute an inexorable evolution of the Internet toward a ubiquitous ecosystem wherein physical objects communicate and intelligently respond to human exigencies with minimal intervention. While technological foundations are firmly established, the path forward demands coordinated multi-disciplinary engagement to develop universal interoperability standards, robust zero-trust security frameworks, explainable AI systems capable of meeting regulatory scrutiny, and affordable infrastructure solutions for resource-limited settings. Only through such concerted collaboration can IoMT fulfill its transformative promise of delivering proactive, personalized, and equitable care while rigorously adhering to the principles of safety, privacy, and human-centered design.

Chapitre 2

Intrusion Detection System

Contents

2.1 Introduction

The Internet of Medical Things (IoMT) represents a transformative paradigm in healthcare, integrating a vast array of connected medical devicessuch as smart pacemakers, insulin pumps, wearable physiological monitors, continuous glucose monitors, and advanced imaging systemsto enhance patient care, facilitate remote monitoring, and optimize operational efficiency within healthcare facilities [6–8]. This interconnected ecosystem allows for the continuous and real-time tracking of billions of individuals' health parameters, significantly reducing the need for frequent hospital visits and enabling proactive health management [9, 10].

However, the rapid adoption and expansive growth of IoMT networks, while offering unprecedented benefits, have simultaneously introduced a complex landscape of critical cybersecurity risks. This expansion has inadvertently created an enormous attack surface, making these networks highly vulnerable to diverse and evolving cyber threats [105]. A significant concern stemming from IoMT's accelerated development is the historical oversight in prioritizing robust security and privacy measures. This neglect has left sensitive healthcare systems exposed to a myriad of cyberattacks, which can not only disrupt technical operations but, more critically, jeopardize patient safety through delayed access to vital health information, manipulation of medical data, or direct interference with life-sustaining devices [106].

Compounding these challenges, the contemporary cybersecurity landscape is characterized by increasingly sophisticated threats. These include highly advanced and polymorphic malware, previously unknown zero-day vulnerabilities, and debilitating Distributed Denial of Service (DDoS) attacks [107]. Traditional Intrusion Detection Systems (IDS), which primarily rely on static rules and predefined signature databases, often prove inadequate in defending against such dynamic and elusive threats. Their inherent limitationsincluding significant security gaps, a high incidence of false positives, and an inability to adapt to novel attack patterns underscore the urgent need for more intelligent and adaptable defense mechanisms.

Consequently, the effective deployment of an IDS within the IoMT ecosystem demands meticulous consideration of several unique factors. These include the extreme sensitivity of medical data, stringent regulatory compliance requirements (such as HIPAA in the United States and GDPR in Europe), and the distinctive operational challenges prevalent in healthcare environments [108], such as the prevalence of legacy medical devices and the critical need for real-time monitoring and immediate response. Addressing these complexities necessitates the development and implementation of advanced,

dynamic, and intelligent intrusion detection mechanisms capable of safeguarding the integrity, confidentiality, and availability of IoMT networks and, by extension, patient lives.

2.2 Intrusion Detection Systems (IDS)

An Intrusion Detection System (IDS) is a fundamental security tool within any robust cybersecurity infrastructure. Its core function is to continuously monitor network traffic, system activities, and other relevant logs for any signs of malicious actions, policy violations, or anomalous behaviors [20, 109]. By scrutinizing these activities, the IDS aims to identify potential threats and immediately alert administrators to any unauthorized or unlawful activities. Serving as an essential backup security measure, IDSs become particularly critical when traditional security technologies, such as firewalls, prove insufficient or ineffective against the constantly evolving landscape of cyber threats. Their primary purpose is thus to detect and signal potential security breaches, thereby providing a crucial layer of defense against sophisticated and emerging attack patterns [110].

2.2.1 Intrusion Detection Systems (IDS) vs. Intrusion Prevention Systems (IPS)

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) represent two foundational technologies engineered to safeguard network integrity and data confidentiality. While both are critical for identifying malicious activities, their fundamental distinction lies in their operational philosophy: an IDS primarily functions as a passive monitor, detecting and alerting security personnel to potential threats, whereas an IPS operates as an active enforcer, automatically blocking and mitigating identified intrusions in real-time [111].

As shown in Table 2.1, the fundamental difference between an IDS and an IPS lies in their response to threats. An IDS acts like a security camera (Watchful Eye), it passively monitors network traffic, detects suspicious activity, and generates alerts for administrators to investigate, but takes no direct action. In contrast, an IPS functions like a security guard (Active Enforcer); it not only identifies threats in real-time but also actively blocks them by dropping malicious packets, resetting connections, or blacklisting

offending IP addresses. While IDS solutions are ideal for visibility and compliance logging, IPS provides proactive defense by stopping attacks before they cause harm. However, IPS systems require careful tuning to avoid false positives that could disrupt legitimate traffic. Recognizing the strengths of both approaches, many modern cybersecurity solutions now combine them into integrated IDPS (Intrusion Detection and Prevention Systems) that offer comprehensive monitoring and automated protection [111, 112].

Table 2.1: *Key Differences Between IDS and IPS*

Parameter	**Intrusion Detection System (IDS)**	**Intrusion Prevention System (IPS)**
Purpose	Monitors and alerts to suspicious activities (passive)	Monitors, alerts, and actively blocks identified threats (active)
Operation	Observes traffic, looks for patterns/anomalies, generates alerts	Examines traffic for real-time attacks, intervenes to stop them
Configuration Mode	Generally operates in monitoring mode, not inline	Typically inline, positioned after the firewall
Traffic Path	Analyzes mirrored traffic after it passes through firewall	Primary route of network traffic; placed after firewall
Placement	Out-of-band (via SPAN port or tap)	Inline (traffic flows through device)
Response to Threats	Sends alerts to administrators; relies on human intervention	Automatically blocks, drops, or mitigates threats
Network Performance	Minimal to no impact (No latency)	Introduces slight latency (process live traffic)
False Positive Consequence	Informational; leads to alert fatigue	Disruptive; can block legitimate traffic
Configuration Complexity	Less complex; focuses on alert generation	More complex; blocking wrong traffic disrupts operations

Organizations select network security mechanisms based on their operational priorities. An Intrusion Detection System (IDS) is particularly suited to entities requiring comprehensive network visibility and detailed forensic analysis while maintaining minimal interference with network performance, albeit at the cost of delayed threat response. In contrast, an Intrusion Prevention System (IPS) is essential for environments where immediate, automated threat mitigation is imperative and security breaches are unacceptable, despite potential trade-offs in system performance and the risk of false positives [111, 113]. For contemporary enterprises, an integrated Intrusion Detection and Prevention System (IDPS) often represents the optimal solution, combining the analytical capabilities of IDS with the proactive threat containment of IPS to establish a multi-layered and resilient security framework.

2.2.2 Intrusion Detection Methods

An IDS functions by continuously scrutinizing network traffic and system events for indicators of compromise. It achieves this by looking for deviations from established normal activity patterns and matching observed events against known attack signatures [114]. The system screens, monitors, and analyzes the network against malicious threats by collecting network data or system logs, which are then processed against predefined rules and signatures to pinpoint potential security threats. Several key detection methods are employed by IDSs:

2.2.2.1 Signature-based Detection

This is the most common method, where the IDS examines all packets traversing an organization's network and compares them against a database of known attack signatures through string comparison. A signature is a unique characteristic or pattern associated with a specific threat, such as a sequence of code in a malware variant [115]. While highly effective at identifying previously documented threats, this method faces a significant challenge: it struggles to detect novel, unknown attacks, including zero-day exploits, as their signatures do not yet exist in the database [116].

2.2.2.2 Anomaly-based Detection

To address the limitations of signature-based systems, anomaly-based detection methods are employed. These systems utilize artificial intelligence

and machine learning to establish and continuously refine a baseline model of "normal" network activity [117]. The IDS then compares ongoing network activity to this learned baseline, flagging any significant deviations as suspicious. This approach is particularly instrumental in combating novel threats and can even detect zero-day exploits. Nevertheless, a critical trade-off emerges with anomaly-based intrusion detection systems: their heightened sensitivity to deviations from established baselines increases the likelihood of false positives, wherein benign yet statistically atypical network behavior is erroneously classified as malicious. This limitation stems from the inherent challenge of distinguishing between genuine threats and permissible operational anomalies, a fundamental constraint in behavioral-based detection methodologies [118].

2.2.2.3 Stateful Protocol Analysis

This method is an advanced network security technique that significantly enhances intrusion detection by contextualizing network traffic. Unlike methods that merely inspect individual packets, SPA systems leverage predefined models of benign protocol behavior and track the "state" of communication sessions across their lifecycle [119]. This allows for the detection of deviations from expected command sequencing, parameter ranges, and request-response pairings, thereby identifying sophisticated attacks like protocol evasion, Denial-of-Service (DoS), and exploits that manipulate legitimate protocols. While resource-intensive and complex to configure, SPA offers superior accuracy and the ability to detect novel attacks by understanding the complete flow and intent of network communications.

2.3 Intrusion Detection System (IDS) for IoMT Networks

The proliferation of Internet of Medical Things (IoMT) devices in healthcare ecosystems has introduced critical cybersecurity challenges, necessitating specialized Intrusion Detection Systems (IDS) tailored to the unique constraints of medical environments [120]. IoMT-focused IDS must address three key requirements: (1) ultra-low latency to avoid disrupting time-sensitive medical operations, (2) lightweight detection algorithms compatible with resource-constrained devices, and (3) compliance with healthcare data regulations such as HIPAA and GDPR [121].

2.3.1 Security Challenges and Vulnerabilities in IoMT Networks

The integration of IoT technology into healthcare, forming IoMT networks, has introduced a new dimension of cybersecurity challenges that necessitate robust defense mechanisms like Intrusion Detection Systems. IoMT devices, unlike traditional IT systems, often operate with inherent limitations that render them highly susceptible to cyberattacks [122].

2.3.1.1 Unique Vulnerabilities of IoMT Devices

2.3.1.1.1 Limited Computational Resources: The inherent design limitations of many IoMT devices, particularly their restricted processing power and memory, significantly impede the integration of advanced security protocols. This includes the effective implementation of robust encryption algorithms and sophisticated intrusion detection systems. Consequently, these resource-constrained devices present an attractive and vulnerable target for malicious actors, increasing the potential for successful cyberattacks [121, 122].

2.3.1.1.2 Outdated Security Protocols and Software: "Medical device manufacturers frequently exhibit a systematic prioritization of functional performance and economic viability at the expense of comprehensive security architectures. This market-driven paradigm emerges from: (1) regulatory pressures for rapid device certification [123], (2) consumer demand for affordable healthcare solutions, and (3) the inherent complexity of implementing zero-trust security models in resource-constrained medical devices [124], leading to the deployment of devices with outdated security protocols and irregular firmware updates. This leaves devices open to known exploits and vulnerabilities.

2.3.1.1.3 Lack of Standardization: The absence of globally unified security standards significantly exacerbates cybersecurity challenges within the healthcare sector [125]. This fragmentation compels healthcare providers to navigate a complex landscape of disparate regulatory requirements and inconsistent security postures across a wide array of devices [123]. This lack of standardization hinders the establishment of a cohesive and robust defense mechanism, potentially exposing vulnerabilities that could otherwise be mitigated by universally adopted protocols.

2.3.1.1.4 Weak Authentication Mechanisms: Incidents across various networked systems have underscored the significant risks associated with the deployment of weak authentication mechanisms, particularly within IoMT ecosystem [122]. Such vulnerabilities frequently enable unauthorized parties to gain facile access to or control over critical devices. This deficiency in robust authentication protocols presents a substantial security loophole, rendering these devices susceptible to exploitation and compromising the integrity and confidentiality of sensitive data and operational functions [126].

2.3.1.1.5 Insecure Communication Channels: Sensitive patient data is often transmitted and stored without adequate encryption, making it vulnerable to interception and unauthorized access [127].

2.3.1.2 Critical Threats and Their Consequences in IoMT Networks

IoMT networks contain inherent vulnerabilities that render them susceptible to a diverse spectrum of cyber threats. These risks extend beyond conventional data breaches, encompassing direct patient endangerment and systemic disruptions to healthcare delivery [128].

2.3.1.2.1 Malware Infections: IoMT devices are susceptible to malware, which can compromise their functionality and integrity. Machine learning approaches have shown high success rates (82-88%) in detecting malware in IoMT contexts [104].

2.3.1.2.2 Distributed Denial of Service (DDoS) Attacks: Attackers can overwhelm network resources, rendering critical medical devices inoperable and disrupting essential healthcare services [104, 129]. This can have life-threatening consequences in real-time patient care scenarios.

2.3.1.2.3 Ransomware: Attacks like WannaCry (2017) targeting hospital systems demonstrate how ransomware can encrypt critical data and systems, demanding payment for their release and severely disrupting patient care [130].

2.3.1.2.4 Data Breaches and Privacy Violations: IoMT devices generate vast amounts of sensitive patient data. Inadequate security measures can lead to unauthorized access, resulting in privacy violations, identity theft, and compromised treatment plans [127]. A 2019 data breach involving an IoMT cloud platform exposed millions of patient records, illustrating these consequences [131].

2.3.1.2.5 Infiltration and Unauthorized Access: Exploiting device vulnerabilities can lead to infiltration of the network from inside, allowing attackers to gain unauthorized access to critical systems or data [104]. The findings underscore the urgent need for robust security frameworks and advanced IDS to safeguard IoMT ecosystems, ensuring trust and reliability in this critical domain where patient safety and data privacy are paramount.

2.3.2 Adaptation and Design of IDS for IoMT Environments

The unique characteristics and constraints of IoMT environments, particularly their resource limitations and heterogeneity, necessitate specialized Intrusion Detection System (IDS) approaches. Traditional IDS models often struggle to meet the stringent requirements of real-time, reliable, and privacy-preserving threat detection in healthcare settings.

2.3.2.1 Adapting IDS for IoMT Constraints

2.3.2.1.1 Lightweight Security Measures: Due to the limited processing power and memory of many IoMT devices, there is a pressing need to develop lightweight security measures and standardized protocols. This involves designing IDS that can operate effectively with minimal computational overhead [132].

2.3.2.1.2 Anomaly-Based Detection Focus: Anomaly-based IDS are considered a promising security solution for IoMT networks because they can detect both known and unknown types of attacks without relying on predefined signatures [117]. This is crucial for identifying novel threats that constantly emerge in dynamic IoMT environments.

2.3.2.1.3 Hybrid Approaches: Novel hybrid Anomaly-based Intrusion Detection Systems are being designed for IoMT networks. These systems often leverage both host-based and network-based techniques to reliably monitor and collect log files from IoMT devices and gateways, as well as traffic from the IoMT network, while simultaneously considering computational cost [132].

2.3.2.1.4 Distributed Architecture: To accommodate the distributed nature of IoMT, IDS architectures are being adapted. For instance, a proposed AIDS consists of two main components [20]: (1) Monitoring and Data Acquisition (MDA) [132] Component that specifically engineered to operate on resource-constrained IoMT devices, collecting data locally and (2) Remote Detection Engine (RDE) Component which functions on the gateway, where more computational power might be available for analysis [133]. This distributed approach helps in reducing latency and data volume compared to conventional cloud-only systems.

2.3.2.2 Specific Design Considerations

Building robust and effective Intrusion Detection Systems (IDS) for Internet of Medical Things (IoMT) networks necessitates careful consideration of several key design principles, given the unique challenges and critical nature of healthcare data.

2.3.2.2.1 Computational Efficiency: Optimizing computational efficiency is a primary design goal [20]. This involves selecting machine learning algorithms that are inherently less computationally intensive. Furthermore, techniques such as model compression (e.g. quantization, pruning) can be employed to significantly reduce the computational burden on resource-constrained IoMT devices [134].

2.3.2.2.2 Real-time Processing: Given the critical nature of healthcare data, real-time threat detection is paramount. IoMT IDS designs must incorporate elements like edge computing to bring computational processes closer to the data source. This proximity reduces latency and enables faster local processing, which is crucial for timely detection and response to threats that could impact patient safety [135].

2.3.2.2.3 Data Heterogeneity: IoMT networks are characterized by a wide array of diverse devices that generate various types of data. Examples include time-series data from GPS devices and binary data from Modbus protocols. IDS designs must effectively account for this data heterogeneity [20]. This often involves allowing for local model training on individual device data subsets before aggregating the learned parameters, ensuring that the system can interpret and analyze diverse data formats.

2.3.2.2.4 Privacy and Ethics Preserving Mechanisms: Due to the highly sensitive nature of patient data, integrating privacy-preserving techniques is essential [112]. Federated Learning (FL) is a particularly relevant approach, as it allows models to be trained locally on decentralized devices. Only aggregated model parameters, not raw patient data, are shared, thereby addressing critical data privacy concerns and facilitating compliance with healthcare regulations [136].

2.3.2.2.5 Adaptability and Robustness: IoMT IDS must be inherently adaptable to concept drift, where the nature of threats evolves over time, and capable of detecting new attack types [131]. Designs should incorporate mechanisms that allow models to continuously learn from evolving threats. Furthermore, the systems must maintain robustness against adversarial attacks, ensuring their effectiveness even when faced with sophisticated evasion techniques.

2.3.2.2.6 Protocol and Network Heterogeneity: IoMT environments are characterized by a diverse range of communication protocols (e.g., Bluetooth, Wi-Fi, Zigbee, proprietary medical protocols) and network architectures. An effective IDS must be capable of monitoring and analyzing traffic across these varied protocols and network segments to gain a comprehensive understanding of potential threats [137].

2.3.2.2.7 Energy Limitations: Many IoMT devices are battery-powered and operate with significant energy constraints [45, 65]. IDS design must account for these limitations by employing energy-efficient algorithms, minimizing communication overhead, and optimizing processing cycles to extend device battery life without compromising security [138].

2.3.2.2.8 Safety-Critical Latency: In healthcare, even milliseconds of delay can have severe consequences, especially in life-support or critical care systems. IDS must be designed to operate with extremely low latency, ensuring that threat detection and response do not interfere with the real-time operational requirements of medical devices and patient care [139].

2.3.2.2.9 Legacy Device Integration: Healthcare facilities often utilize a significant number of legacy medical devices that may not have built-in security features or modern connectivity options [140]. IoMT IDS solutions must offer strategies for integrating and protecting these older devices, potentially through specialized gateways or network segmentation, to avoid creating vulnerable points in the network.

2.3.2.2.10 Regulatory Certification: The development and deployment of IoMT IDS are subject to stringent healthcare regulations and certification processes (e.g., HIPAA, GDPR, FDA clearances) [141]. Designs must inherently consider these regulatory requirements from the outset to ensure compliance, facilitate certification, and build trust in the security of medical devices and patient data attacks.

2.4 AI-Driven Intrusion Detection Systems

Contemporary cybersecurity faces dynamically evolving threats that increasingly circumvent traditional signature-based Intrusion Detection Systems (IDS). These legacy systems, reliant on static rules and predefined attack patterns, demonstrate critical limitations against advanced attack vectors, including zero-day exploits and polymorphic malware [142]. Key deficiencies include high false-positive rates, inability to detect novel threats, and fundamental adaptability gaps in emerging threat landscapes.

Artificial Intelligence-powered IDS represent a paradigm shift, leveraging machine learning (ML) and deep learning (DL) to enable proactive, adaptive security. By analyzing network traffic patterns at scale, AI-IDS autonomously identify both known and unknown threats with superior accuracy while reducing detection latency [143]. This transitions cybersecurity from reactive signature-matching to anticipatory threat prevention, effectively narrowing vulnerability windows against zero-day attacks.

2.4.1 Foundations Concepts of AI-Driven Intrusion Detection Systems

AI-Driven Intrusion Detection Systems (IDS) represent a significant leap forward in cybersecurity, moving beyond traditional signature-based methods to offer more adaptive and proactive threat detection. These systems leverage the power of artificial intelligence, particularly machine learning and deep learning, to analyze vast amounts of network traffic and identify suspicious activities that might indicate a cyberattack [143].

2.4.1.1 Revolutionizing Intrusion Detection Capabilities

AI-driven Intrusion Detection Systems (IDS) fundamentally enhance cybersecurity by transcending the limitations of traditional, static security measures. Unlike conventional IDS, which rely on fixed rules and known threat signatures, AI-driven systems possess the capacity for continuous learning from network activity. This inherent adaptability enables the detection of previously unknown attack vectors and facilitates proactive defense mechanisms against evolving threats. By analyzing deviations from established normal behaviors, AI-based systems can identify anomalies indicative of novel and sophisticated attacks, a capability largely absent in signature-based methodologies [144]. This allows AI-based IDS to scrutinize network traffic and identify potential threats with increased speed and accuracy compared to purely mathematical models that depend solely on parameter set comparisons.

2.4.1.2 Multi-Faceted Improvements and Expedited Response

The advancements offered by AI-driven systems significantly bolster an organization's defense mechanisms through multi-faceted improvements [145]. A primary advantage is the expedited threat detection and response, which minimizes potential damage by identifying malicious activities before they can inflict harm. Furthermore, AI-Driven IDS substantially reduce false alarms, a pervasive issue in traditional systems that can overwhelm security teams and diminish overall system efficiency. This reduction in false positives allows security personnel to concentrate on genuine threats, thereby improving operational effectiveness [146].

2.4.1.3 Adaptive Learning and Generalization Capabilities

The core of AI's enhancement in IDS lies in its adaptive learning and generalization capabilities. Machine learning models continuously learn from vast volumes of data, enabling systems to identify intricate patterns and anomalies in real-time. This allows them to learn from past attack patterns and generalize to new threats, including zero-day attacks, which are critical vulnerabilities exploited before public disclosure. This continuous learning capability ensures that the models evolve dynamically with the threat landscape, maintaining their efficacy over time [131]. The capacity to handle large volumes of cloud data and network traffic is another significant benefit, as AI-based IDS can efficiently process and recognize abnormal behavior with high precisiona necessity in modern, high-bandwidth environments [147].

2.4.1.4 Automation in Incident Response and Strategic Resource Allocation

Beyond detection, AI drives automation in incident response and management. Machine learning in cybersecurity systems can initiate predefined actions, such as isolating affected systems or blocking malicious Internet Protocol (IP) addresses, within seconds of detecting a threat [144]. This automation minimizes human error and liberates security analysts to focus on more complex investigations and strategic work, thereby optimizing resource allocation [148]. Finally, the integration of AI with cloud computing provides greater scalability and flexibility, making AI-based IDS applicable for diverse network sizes and types, ranging from small enterprises to large-scale cloud infrastructures.

2.4.1.5 A Paradigm Shift from Reactive to Proactive and Predictive Defense

This continuous learning and adaptation capability signifies that AI-Driven IDS are not merely improving detection; they are fundamentally altering the nature of cybersecurity defense. Traditional systems necessitate manual updates for new signatures, inherently placing them in a reactive posture. In contrast, AI-driven systems can continuously learn from network activity and internalize lessons from previous attacks to prevent future incidents with similar characteristics. This establishes a dynamic feedback loop: detect, learn, adapt, and predict. The ability to identify previously unknown attack vectors and zero-day exploits is a direct outcome of this intelligent, adaptive

process. This transformation from a static, reactive posture to a dynamic, proactive, and predictive one is crucial, as it drastically reduces the time required to detect and respond to attacksa critical factor in today's rapidly evolving threat landscape [149].

2.4.2 Challenges and Limitations of AI-Driven IDS

Despite their significant advancements, the deployment of AI-Driven Intrusion Detection Systems (IDS) faces several critical challenges and limitations that hinder their widespread and seamless integration into real-world cybersecurity infrastructures.

2.4.2.1 High False-Positive and False-Negative Rates

AI-Driven IDS can incorrectly flag legitimate activity as malicious (false positives), leading to alert fatigue, inefficient use of security resources, and a reduction in the overall reliability and trustworthiness of the system. In high-stakes environments, such a deluge of false alerts can compromise operational efficiency and delay responses to genuine threats. Conversely, false negatives, where the IDS fails to detect an actual attack, are particularly dangerous. They allow malicious activities to go unnoticed, potentially causing significant damage, especially when dealing with novel or sophisticated attack techniques (e.g., zero-day exploits, Advanced Persistent Threats) that are not adequately represented in training data [150].

2.4.2.2 Data Imbalance

A major challenge stems from the inherent data imbalance in cybersecurity datasets, where normal network traffic significantly outnumbers attack traffic. Training machine learning models on such imbalanced datasets can lead to biased predictions, causing models to be "over-trained" on normal patterns and consequently perform poorly in identifying low-frequency but critical attack types [151].

2.4.2.3 Adversarial Attacks

AI-Driven IDS are vulnerable to adversarial attacks, where malicious actors subtly manipulate input data to deceive machine learning models into misclassifying malicious activities as benign. These attacks exploit the inherent

weaknesses of AI models, highlighting the need for robust defensive techniques, as they can effectively bypass AI-Driven IDS and gain unauthorized access to critical systems or data [152].

2.4.2.4 Computational Demands

Deep learning models, which are central to advanced AI-IDS, require substantial computational resources for both training and inference. This makes real-time deployment challenging, as the training and inference times can become prohibitive in high-volume network environments [143].

2.4.2.5 Model Interpretability and Transparency

The complexity of many AI models, particularly deep learning architectures, often renders them opaque "black boxes". In cybersecurity, it is crucial for security teams to understand the rationale behind a model's decision to flag a particular event as malicious. A lack of transparency can hinder trust, impede effective decision-making, and complicate compliance with regulatory standards [153].

2.4.2.6 Adaptability in Dynamic Threat Landscape

The cybersecurity threat landscape is highly dynamic, with attackers constantly modifying their tactics to evade detection. Ensuring continuous adaptability of AI models to this evolving environment, requiring frequent model updates and retraining, remains a significant challenge [154].

2.4.2.7 Data Requirements

Effective training often necessitates large, diverse, and high-quality datasets, which can be challenging to obtain, especially for new or rare attack types. Data labeling for supervised learning can be labor-intensive [155].

2.4.2.8 Integration with legacy IT Infrastructure

The integration of advanced AI-Driven Intrusion Detection Systems (IDS) with existing, and often legacy, IT infrastructure presents significant complexities for organizations. This challenge arises from several factors, including disparities in system architectures, incompatible data formats, and

the need to ensure seamless communication between modern AI solutions and older, potentially proprietary, network components. Such integration often requires extensive customization, middleware development, and careful planning to avoid disruptions to critical operations [156]. Consequently, organizations frequently encounter hurdles in achieving full interoperability and maximizing the benefits of AI-driven security capabilities within their established environments.

2.4.3 Machine Learning and Deep Learning in Intrusion Detection Systems

The advent of machine learning (ML) has profoundly improved Intrusion Detection System (IDS) performance by enabling systems to learn from historical attack patterns and generalize to novel threats, representing a significant advancement over traditional rule-based methodologies. ML models often serve as a foundational layer in AI-powered IDS, providing essential benchmarks for evaluating more complex deep learning or hybrid approaches. Researchers commonly initiate their investigations with ML models to establish baseline performance and understand dataset characteristics before progressing to more computationally intensive methods [157]. These models prove effective for identifying known attacks and offer initial insights into underlying data patterns.

Deep learning (DL), a specialized subset of machine learning, has emerged as a powerful alternative to address the limitations inherent in traditional ML approaches [158]. This is particularly evident in its capacity to manage large-scale, high-dimensional datasets and adapt to rapidly evolving attack patterns. A key advantage of DL models lies in their ability to autonomously learn hierarchical representations directly from raw network traffic data, thereby eliminating the need for laborious and expertise-dependent manual feature engineering [159]. Furthermore, DL models are exceptionally well-suited for detecting evolving attack patterns in real-time network monitoring due to their inherent capability to analyze temporal dependencies within sequential data [145].

2.4.3.1 Prominent ML Algorithms for IDS

ML algorithms employed in intrusion detection systems (IDS) are systematically classified according to their fundamental learning paradigms, as detailed in Table 2.2:

2.4.3.1.1 Supervised Learning Algorithms: These algorithms are widely employed for intrusion detection and are trained on labeled datasets, where network traffic is explicitly tagged as normal or malicious [160].

- **Decision Trees (DT):** These models are used for classification tasks and can provide a step-by-step rationale for their classifications, which is valuable in static or well-defined environments.
- **Random Forest (RF):** An ensemble learning method, Random Forest combines multiple decision trees to enhance accuracy and reduce overfitting. It is recognized for its high performance in classification tasks.
- **Support Vector Machines (SVM):** SVMs are effective for both binary and multiclass classification by identifying a hyperplane that optimally separates data points into different classes, maximizing the margin between them. They are considered highly reliable due to their fast and simple prediction process.
- **K-Nearest Neighbors (KNN):** A non-parametric, instance-based learning algorithm used for classification. KNN classifies data points based on the majority class of their 'K' nearest neighbors in the feature space.
- **Naïve Bayes (NB):** This classification algorithm is based on Bayes' theorem, operating under the assumption that there is no dependency among predictors. It calculates the probability of a given data point belonging to a class based on the probabilities of its features.
- **Logistic Regression:** Used for both binary and multiclass classification, Logistic Regression predicts the probability of an event's occurrence.
- **XGBoost (XGB):** A powerful gradient boosting algorithm, XGBoost is known for its high performance in classification tasks and its ability to handle complex relationships and large datasets efficiently.

2.4.3.1.2 Unsupervised Learning Algorithms: These algorithms deal with unlabeled data, categorizing it based on inherent similarities or patterns. They are particularly useful for detecting unusual behavior and identifying new attack patterns, including zero-day attacks, as they do not rely on prior knowledge of attack signatures. K-Means is a common clustering algorithm often used for grouping similar network packets [161].

2.4.3.1.3 Reinforcement Learning (RL): RL is applied in adversarial simulation to train ML models to identify and respond to attacks in real-time. It is also used for developing autonomous intrusion detection systems, where the system learns optimal actions through trial and error in a dynamic environment.

2.4.3.1.4 Semi-supervised Learning: This approach combines aspects of both supervised and unsupervised learning, leveraging both labeled and unlabeled data. It can be used for tasks such as malicious and benign bot identification, as well as malware and ransomware detection.

Table 2.2: *Overview of Machine Learning Models in IDS*

Model Name	**Key Characteristics**	**Typical Applications in IDS**	**Limitations**
Decision Trees (DT)	Supervised, hierarchical, rule-based classification	Binary/multiclass classification, visualizable decision pathways	May overfit, less effective for complex patterns
Random Forest (RF)	Supervised, ensemble of decision trees, reduces overfitting	General intrusion detection, high-performance classification	Computationally intensive, less interpretable than single DT
Support Vector Machines (SVM)	Supervised, finds optimal hyperplane for separation	Binary/multiclass classification, anomaly detection	Sensitive to noisy data, computationally intensive for large datasets
K-Nearest Neighbors (KNN)	Supervised, instance-based, classifies by majority vote	Classification, anomaly detection (outliers)	Computationally expensive for large datasets, sensitive to irrelevant features
Naïve Bayes (NB)	Supervised, probabilistic classifier (Bayes' theorem)	Binary/multiclass classification, spam detection	Assumes feature independence, rarely true in real data
Logistic Regression	Supervised, statistical model for classification	Binary/multiclass classification, baseline model	Assumes linear relationships, less effective for complex nonlinear patterns
XGBoost (XGB)	Supervised, gradient boosting ensemble, high performance	High-performance classification, handling complex relationships	Prone to overfitting if not tuned, computationally demanding

2.4.3.2 Prominent DL Algorithms for IDS

Various deep learning architectures offer unique strengths when applied to intrusion detection:

2.4.3.2.1 Multilayer Perceptron (MLP): As a foundational artificial neural network, MLP models demonstrate strong performance in network intrusion detection by learning complex non-linear relationships within the data [162].

2.4.3.2.2 Convolutional Neural Networks (CNNs): CNNs are a highly effective deep learning architecture for Intrusion Detection Systems, leveraging convolutional layers to automatically extract spatial features from grid-like data structures, such as network traffic represented as "images" or matrices [163]; this capability can be extended to Temporal Convolutional Networks (TCNs) for time-series analysis. CNNs excel in detecting static attacks like Distributed Denial-of-Service (DDoS), port scanning, and brute-force attacks, where distinctive spatial patterns are indicative of malicious activity, and studies have reported high performance, with accuracies reaching up to 98% and detection rates of 91% to 93% for DDoS and brute-force attacks. Despite their strengths, CNNs typically incur high computational costs and may demonstrate limitations in detecting long-duration or time-dependent attacks, such as SQL injection or spoofing, as their primary focus is on spatial feature extraction rather than comprehensive temporal analysis.

2.4.3.2.3 Recurrent Neural Networks (RNNs): RNNs are particularly adept at capturing temporal dependencies in sequential data, rendering them highly suitable for real-time network monitoring and the identification of evolving attack patterns that manifest over time, with more advanced architectures like Bidirectional RNNs or Gated Recurrent Units (GRU) offering enhanced capabilities [164]. Consequently, RNNs are well-suited for applications such as comprehensive network traffic analysis, malicious traffic detection, and the identification of time-dependent attacks like phishing and Denial-of-Service (DoS) attacks. Performance evaluations indicate that RNNs typically achieve accuracies ranging from 88% to 92%, with detection rates of 85% to 90% for DoS and malicious traffic detection, frequently accompanied by a low false-positive rate. However, RNNs are characterized by limitations, notably their difficulty in processing long sequences due to issues like vanishing or exploding gradients, which can impede their ability to learn

long-term dependencies and often necessitate extended training times and substantial datasets for optimal performance.

2.4.3.2.4 Long Short-Term Memory (LSTM): LSTM networks, a specialized type of Recurrent Neural Network (RNN), are engineered to overcome the vanishing gradient problem, making them exceptionally effective for learning long-term dependencies in time-series data [165]. These networks are ideally suited for detecting time-dependent attack patterns and complex time-series attacks, such as Distributed Denial-of-Service (DDoS) and Advanced Persistent Threats (APTs), which frequently involve prolonged and coordinated malicious activities. In terms of performance, one study demonstrated that an LSTM model achieved an overall accuracy of 98% and the highest macro average F1 score (0.84) among MLP, CNN, and LSTM architectures, signifying superior performance in class differentiation. Other reports further corroborate this high efficacy, showing accuracies ranging from 90% to 95% with detection rates of 92% to 96% for DDoS and APTs, often accompanied by a lower false-positive rate compared to general RNNs. However, a notable limitation of LSTMs is their computational intensity, stemming from their complex internal architecture, which necessitates substantial data and extensive training time.

2.4.3.2.5 Autoencoders (AE): These neural networks are used for unsupervised learning, specifically for learning hierarchical features and reducing data dimensionality [166]. Stacked Autoencoders (SAE) have demonstrated superior performance compared to traditional ML methods in certain intrusion detection tasks.

2.4.3.2.6 Generative Adversarial Networks (GANs): Generative Adversarial Networks (GANs) exhibit significant potential in addressing data imbalance, a prevalent challenge in Intrusion Detection System (IDS) datasets, by synthesizing realistic minority class samples through an adversarial training process, thereby enhancing the diversity and representativeness of underrepresented attack data [167]. However, the application of GANs is constrained by the complexity and resource-intensive nature of their training process, coupled with the risk of mode collapse, a phenomenon where the generator produces a limited variety of samples.

Table 2.3 provides a comparative overview of prominent Deep Learning architectures utilized in Intrusion Detection Systems.

Table 2.3: *Overview of Deep Learning Architectures in IDS*

Architecture	**Key Characteristics**	**Handling of Spatial/-Temporal Data**	**Typical Applications in IDS**	**Limitations**
MLP	Foundational ANN, dense layers, learns non-linear relationships	No specific spatial/-temporal handling	Network intrusion detection	Lacks spatial/-temporal feature extraction
CNN	Convolutional layers extract spatial features	Excels at spatial patterns (grid-like data)	DDoS, port scanning, brute-force attacks	High computational cost, poor for long time-dependent attacks
RNN	Captures temporal dependencies in sequences	Excels at temporal dependencies	Traffic analysis, phishing, DoS attacks	Struggles with long sequences (vanishing gradients), long training
LSTM	RNN variant, memory cells overcome vanishing gradient	Excels at long-term temporal dependencies	DDoS, APTs, time-dependent attacks	Computationally intensive, requires large data
Autoencoder (AE)	Learns compressed feature representations	Dimensionality reduction	Anomaly detection, feature extraction	May not capture complex attacks, noise-sensitive
GANs	Generator discriminator adversarial training	Generates synthetic data	Addressing data imbalance (synthetic samples)	Complex training, risk of mode collapse

2.4.3.3 Hybrid Machine Learning and Deep Learning Approaches

The distinct strengths and weaknesses of individual Machine Learning (ML) and Deep Learning (DL) models have led to the development of hybrid approaches, aiming to combine their complementary capabilities. Traditional ML algorithms, while effective in boosting identification rates, often struggle with intricate feature-integrated attacks and perform poorly when confronted with noisy and multi-dimensional traffic data. Conversely, DL models, despite their promise in improving accuracy and handling complex attack scenarios, typically require substantial computational resources and can suffer from a lack of interpretability, often operating as "black boxes". The rationale behind hybridization is to leverage the best of both worlds: DL algorithms excel in identifying novel, unfamiliar cyber threats with high precision through their advanced feature extraction capabilities, while ML algorithms are highly effective in accurately identifying and responding to known threats through their robust classification abilities [168]. This integration directly seeks to reduce misclassification errors, including both false positives and false negatives, which are persistent challenges in Intrusion Detection Systems (IDS).

Table 2.4 provides a comparative overview of the performance of various Hybrid ML-DL Models in Intrusion Detection Systems.

Table 2.4: *Performance Comparison of Hybrid ML-DL Models*

Hybrid Model	**Key Components**	**Advantages**	**Limitations**
CNN-LSTM	CNN for spatial, LSTM for temporal.	Combines spatial + temporal, reduced misclassification.	Computationally intensive, complex training.
RNN-SVM	RNN for features, SVM for classification.	High accuracy, fewer misclassifications.	Complex integration, high computational load.
FCNN + CFS/PCA	Dimensionality reduction + FCNN.	Faster detection, reduced model complexity.	Risk of info loss with aggressive feature reduction.

2.5 Future Trends and Emerging Research Directions in AI-Driven IDS

The field of AI-powered Intrusion Detection Systems is rapidly evolving, driven by both technological advancements and the escalating sophistication of cyber threats. Several cutting-edge areas are shaping the future trajectory of IDS development.

2.5.1 Explainable AI (XAI)

Explainable AI (XAI) directly addresses the "black box" problem prevalent in complex AI models by providing interpretability and transparency to their decision-making processes, thereby enabling security professionals to better understand, trust, and effectively optimize Intrusion Detection System (IDS) models [169]. Key XAI techniques, such as SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-agnostic Explanations), offer insights into how specific features contribute to model predictions, while rule-based and hybrid models further enhance interpretability by providing more human-readable decision pathways [170]. Emerging techniques like saliency maps visualize feature influence, and counterfactual explanations allow analysts to explore how small data changes alter decisions [171]. The profound impact of XAI extends to enhancing trust in automated systems, aiding in regulatory compliance (e.g., GDPR), improving incident response strategies by providing crucial context, and facilitating vital collaboration between AI systems and human analysts [170].

2.5.2 Adversarial Robustness

Research in adversarial robustness focuses on making AI models resilient to adversarial attacks, where subtly manipulated input data can deceive an Intrusion Detection System (IDS) into misclassifying malicious activities as benign. Core techniques in this domain include adversarial training, which involves augmenting training data with perturbed samples to teach the model to correctly classify manipulated inputs, and the development of auxiliary networks [172], such as AuxAtWGAN, designed to detect and filter out adversarial samples before they reach the main detection model. Furthermore, integrating Explainable AI (XAI) features significantly aids in detecting and mitigating adversarial attacks by providing insights into feature importance and data distribution alignment [171]. Ultimately, enhancing adversarial

robustness is crucial for maintaining IDS effectiveness against increasingly sophisticated and adaptive cyber threats, thereby ensuring that AI-powered defenses are not easily bypassed [173].

2.5.3 Real-Time Processing Solutions

Real-time intrusion detection is paramount, particularly in dynamic cloud environments where rapid threat response is essential to minimize damage, despite significant challenges such as latency, high computational demands, maintaining data quality and volume, and ensuring scalability [174]. To address these issues, solutions include the deployment of edge computing to reduce latency and bandwidth by processing data closer to its source [175], alongside the utilization of specialized hardware like GPUs and TPUs to accelerate deep learning tasks [176]. Furthermore, efficient algorithms, such as quantization and pruning, are employed to reduce model size and speed up inference, while streaming data platforms like Apache Kafka and Spark Streaming facilitate the parallel processing of vast data streams [177]. The widespread adoption of 5G networks also provides the crucial high-speed, low-latency connectivity necessary for real-time AI applications [178]. Collectively, these innovations significantly reduce detection latency and enable rapid threat response, which is vital for effectively mitigating fast-evolving cyberattacks.

2.5.4 Federated Learning (FL)

Federated Learning (FL) is a privacy-preserving machine learning approach where models are trained locally on decentralized devices, such as Internet of Things (IoT) devices, with only aggregated model parametersrather than raw sensitive datatransmitted to a central server for global model updates, thereby directly addressing data privacy concerns and regulatory compliance [179]. This paradigm is ideally suited for distributed environments like IoT networks and cyber-physical systems, where sensitive data often resides on individual devices and cannot be centralized due to privacy regulations or bandwidth constraints [180]. Common techniques include the Federated Averaging (FedAvg) algorithm for parameter aggregation [181]. Proposed FL models have exhibited robust performance, while maintaining low computational demands, underscoring their feasibility for edge deployment [182]. Ultimately, FL enhances scalability, privacy, and adaptability for diverse IoT environments, enabling efficient, real-time threat detection directly at the network edge.

2.6 Conclusion

The evolution of cybersecurity has reached a critical juncture, where traditional Intrusion Detection Systems (IDS) are increasingly outmatched by the sophistication and dynamism of modern cyber threats, particularly within the sensitive and rapidly expanding Internet of Medical Things (IoMT) domain. AI-powered IDS have emerged as an indispensable solution, fundamentally overcoming the limitations of static, signature-based systems by offering adaptive learning capabilities, significantly enhanced accuracy, and a notable reduction in false positives. This review has highlighted the distinct contributions of both Machine Learning (ML) and Deep Learning (DL) models within this critical domain. ML models serve as a foundational layer, providing robust detection for known attack patterns through various supervised and unsupervised learning techniques. They establish essential benchmarks and offer initial insights into network behavior, crucial for understanding the baseline operation of diverse IoMT devices. Deep Learning models, conversely, excel in handling complex, high-dimensional, and spatiotemporal data, proving particularly effective in detecting novel zero-day threats and evolving attack patternssuch as sophisticated multi-stage attacks targeting medical devicesthat traditional ML approaches might miss.

A significant advancement in the field, with direct implications for IoMT security, is the growing importance and demonstrated effectiveness of hybrid ML-DL approaches. These integrated models strategically combine the strengths of both paradigms, leveraging DL for advanced feature extraction from the diverse data streams generated by IoMT devices (e.g., patient vital signs, device logs, network traffic) and ML for efficient and accurate classification. This synergy leads to superior overall performance, including improved accuracy and reduced misclassification errors, which is paramount in clinical settings where false positives could disrupt patient care or false negatives could lead to catastrophic outcomes. Furthermore, these hybrid approaches address practical deployment challenges specific to IoMT, such as the often-limited computational resources of edge devices, through techniques like dimensionality reduction and quantization, allowing for more efficient model execution on constrained hardware.

Looking ahead, the cybersecurity landscape for IoMT is characterized by an escalating "arms race" between AI-powered attacks and AI-powered defenses. Adversaries are increasingly employing AI to develop more adaptive malware specifically targeting medical devices, generate highly convincing phishing campaigns aimed at healthcare personnel, and create sophisticated deepfake impersonations for social engineering. This necessitates continuous

innovation in AI-powered IDS tailored for IoMT, focusing on critical future research directions. These include enhancing model interpretability through Explainable AI (XAI) to foster trust among clinicians and facilitate human-AI collaboration in diagnosing security incidents, improving adversarial robustness to withstand malicious manipulations designed to bypass IoMT defenses, optimizing for real-time processing to enable rapid threat response in high-volume healthcare environments, and leveraging privacy-preserving federated learning, especially for distributed IoMT networks where data sharing is restricted due to patient privacy concerns.

In conclusion, AI-powered IDS are not merely an enhancement but an indispensable component of modern cybersecurity, offering critical protection for the rapidly expanding and vulnerable IoMT ecosystem. Their continuous evolution, driven by advancements in ML, DL, hybrid architectures, and a proactive approach to emerging challenges specific to healthcare, positions them as crucial mechanisms for providing resilient and adaptive defense against an ever-more sophisticated array of cyber threats that directly impact patient safety and data integrity.

Chapitre 3

Towards Secure Internet of Medical Things: A Hybrid BiLSTM-DNN Intrusion Detection Framework

Contents

3.1 Introduction

The proliferation of Information and Communication Technology (ICT) and the Internet of Things (IoT) has significantly transformed the healthcare industry through the widespread adoption of the Internet of Medical Things (IoMT) [183, 184]. This has led to notable improvements in remote patient care, real-time monitoring, and diagnostic capabilities [185]. However, the diverse and resource-constrained nature of IoMT ecosystems creates significant security vulnerabilities, as a lack of standardized security protocols makes medical devices susceptible to cyber threats [121].

The critical nature of healthcare services and the confidentiality of patient data make security a paramount concern [186]. Undetected cyberattacks can have severe consequences, from manipulating diagnostic data to causing

network downtime, which could lead to delayed medical care and even life-threatening situations [105, 187]. While Intrusion Detection Systems (IDSs) are commonly used to counter cyber threats in IoT environments, conventional IDSs are not suited for IoMT networks [18, 188]. They often fail to capture the unique spatial and temporal patterns in medical data streams, leading to inaccurate or delayed threat detection, which can have dire consequences for patient safety [189, 190].

To address these limitations, this study proposes a novel IDS architecture, designed to secure IoMT networks by effectively analyzing complex spatio-temporal attack patterns, using a pioneering BiLSTM-DNN hybrid architecture. This framework provides end-to-end protection by leveraging its Bidirectional Long Short Terme Memory (BiLSTM) [191] layers to capture long-term dependencies and complete bidirectional context and Deep Neural Network (DNN) [192] processor then refines the extracted features and hierarchically analyzes attack signatures, achieving exceptional classification accuracy that precisely distinguishes between legitimate operations and intrusions. The effectiveness of the proposed framework was validated using the CICIoMT2024 dataset, with a thorough evaluation that included rigorous feature selection to demonstrate its discriminatory power against various attack types.

3.2 Related Work

The field of intrusion detection for IoT and healthcare systems has evolved significantly, with research focusing on two main areas: multi-class and binary classification. For multi-class classification, which is crucial for identifying specific threats in healthcare environments, research has moved from traditional Machine Learning (ML) models to advanced deep learning (DL) hybrids. Initial works by Doménech et al. [193] and Lipsa et al. [194] used classical ML and ensemble methods, respectively, to establish strong baselines. The field then advanced with deep learning, employing hybrid models like the CNN-LSTM by Faruqui et al. [195] and a more complex CNN-LSTM-RL framework by Shaikh et al. [196]. More recent state-of-the-art approaches incorporate attention mechanisms (Sharma and Shambharkar [197]) and specialized sequential models like LSTM (Akar et al. [198], Jony et al. [199]) to handle high-dimension classification. The community is now prioritizing these multi-class classifiers for their practicality in real-world scenarios; despite the technical challenges they present. Notably, Khanday et al. [200] demonstrated exceptional performance with an ensemble of LSTM and 1D-

CNN models, achieving a near-perfect accuracy for a 34-class problem on the CICIoT2023 dataset.

Parallel research in binary classification has prioritized maximizing detection accuracy, often using high-capacity models. Transformer-based architectures have shown exceptional performance in this domain, as demonstrated by Tseng et al. [201] and Alsharaiah et al. [202], with the latter enhancing model transparency through explainable AI (XAI). Naeem et al. [203] also contributed to this area by implementing Transformer-based DCNNs, LSTM, and a Meta-learner, achieving high accuracy for binary classification on the WUSTL-EHMS-2020 and CICIoMT2024 datasets. LSTM-based models continue to be fundamental for temporal analysis, applied in centralized systems by Sayegh et al. [204] and Gueriani et al. [205], and adapted for privacy-conscious Federated Learning (FL) by Anwar et al. [206]. This focus on privacy is also reflected in the work of Abbas et al. [207] who used a federated DNN.

Emerging architectures like GRU with attention mechanisms (Saran et al. [208]) also indicate a growing interest in adaptable and scalable solutions. Across both classification types, there's a clear trend toward multi-dataset evaluation to assess generalization capability, signaling the field's maturation toward solving complex, real-world problems. A comprehensive review (Refer to Table 3.1) of the existing literature reveals a clear scholarly trajectory toward advanced, hybrid deep learning architectures for intrusion detection. Contemporary research demonstrates a growing trend of integrating attention mechanisms and Transformer models, often supported by privacy-preserving frameworks such as federated learning. While binary classification models consistently achieve high accuracy, the academic and industrial focus is increasingly shifting toward multi-class classification systems. This prioritization is driven by their superior operational utility and practical applicability in real-world deployment scenarios, reflecting a field that is maturing from purely accuracy-driven models to functionally robust solutions for the complex threat landscape of IoT and healthcare systems.

3.3 CIC-IoMT2024 Dataset

Developed by Dadkhah et al. at the Canadian Institute for Cybersecurity, the CICIoMT2024 dataset constitutes a meticulously curated benchmark specifically designed to address salient limitations in existing cybersecurity datasets for Internet of Medical Things (IoMT) environments [209]. Its construction responds to the critical need for modern, domain-specific

Table 3.1: *Summary of Intrusion Detection System (IDS) Research*

Reference	**Model Type**	**Techniques used**	**Dataset**	**Number of classes**
[14] (2025)	ML	ML models	CICIoT2023 and CICIoMT2024	6
[15] (2025)	Ensemble ML	Random Forest, XGBoost, Decision Tree, and Support Vector	CICIDS2017 and NSL-KDD	14
[16] (2023)	Hybrid	CNN and LSTM	CICIDS2017, CICIDS2018 and CICIDS2019	12
[17] (2025)	Hybrid	CNN, LSTM, and RL	CICIoMT2024	19
[18] (2025)	Hybrid	CNN, RNN, and Attention mechanism	CICIoMT2024	19
[19] (2025)	DL	LSTM	CICIoMT2024	19
[20] (2024)	DL	LSTM	CICIoT2023	35
[21] (2025)	Ensemble DL	Ensemble (LSTM, 1D-CNN)	CICIoT2023	34
[22] (2024)	Hybrid DL	Transformer-based DCNNs, LSTM, and Meta-learner	WUSTL-EHMS-2020, CICIoMT2024	2
[23] (2024)	DL	Transformer Model	CICIoT2023	2
[24] (2025)	Extended DL	Transformer-based DL and Explainable AI	CICIoMT2024	2
[25] (2023)	DL	LSTM	CICIDS2017, NSL-KDD and UNSW-NB15	2
[26] (2024)	Hybrid DL	CNN and LSTM	CICIoT2023 and CICIDS2017	2
[27] (2025)	Decentralized DL	FL-based LSTM	WSN-DS, CICIDS2017 and UNSW-NB15	2
[28] (2023)	Decentralized DL	Federated DNN	CICIoT2023	2
[29] (2024)	Extended DL	Gated Recurrent Unit (GRU) and Attention Mechanism	NF-TON-IoT and ICU	2

data that accurately reflects the unique threat landscape and operational dynamics of healthcare networks, moving beyond general network traffic to capture the unique complexities of healthcare environments. By integrating IoMT-specific protocols, devices, and attack vectors, this dataset provides a foundational resource for advancing intrusion detection systems (IDS) tailored to medical contexts.

3.3.1 Dataset description

The dataset's design embodies a rigorous methodology aimed at emulating realistic clinical settings through a meticulously designed testbed that mimics a smart hospital environment. Its testbed incorporates a heterogeneous ensemble of 40 diverse devices, including 25 real devices and 15 simulated devices, orchestrated to replicate a smart hospital ecosystem. Traffic encompasses multi-protocol communications including WiFi, MQTT, Bluetooth, ensuring representativeness of real-world IoMT deployments and accurately reflecting real-world clinical network traffic [209].

Figure 3.1: *CICIoMT2024 Topology.*

A notable innovation lies in its comprehensive attack taxonomy, featuring 18 distinct attack classes (plus normal traffic, resulting in 19 total classes), categorised into DDoS, DoS, reconnaissance, spoofing, and ransomware scenarios. The dataset further includes device behavioural profiling across operational states (e.g., power, idle, active), capturing lifecycle and behavioral patterns of devices and enabling research into anomaly detection based on device-specific patterns, representing a significant advancement for identifying anomalies [35]. The dataset provides both raw (PCAP) files for deep packet inspection and pre-processed (CSV) formats, with the latter featuring 45 engineered features per network flow extracted via CICFlowMeter. This dual-format approach facilitates immediate usability for machine learning and deep learning applications while preserving flexibility for granular analysis, making it highly accessible for researchers.

Unlike generic datasets (e.g., NSL-KDD, CICIDS2017), CICIoMT2024 captures the idiosyncrasies of IoMT networks, including proprietary protocols and device interoperability, thereby enhancing the external validity of research findings and addressing the critical need for domain-specific data. The inclusion of device lifecycle profiling permits investigations into behavioral analytics beyond network traffic, supporting research on device-specific intrusion detection and representing a significant advancement over previous datasets [210].

Despite its significant advancements, the CICIoMT2024 dataset has inherent limitations due to its synthetic origin. As a product of a controlled laboratory environment, it may not fully capture the unpredictability, noise, and large-scale nature of a live hospital network, which could potentially limit the generalizability of models trained on it. The specific configurations of the testbed and the simulated attacks may also introduce biases, which could negatively impact model performance when deployed in different IoMT infrastructures. Furthermore, the dataset's network-centric focus means it primarily contains network flow data and lacks crucial information from other sources, such as device-level telemetry or system logs, thus overlooking opportunities for a more comprehensive, multi-modal security analysis.

The CICIoMT2024 dataset is a landmark contribution to IoMT security research. Its rigorous design, diverse protocol support, and specific focus on healthcare-related attacks establish it as the leading benchmark for developing and evaluating Intrusion Detection Systems (IDS). Despite being generated in a laboratory setting, a common limitation, the dataset's transparent methodology and alignment with real-world healthcare environments make it an essential resource. Its complexity has solidified its position as the de facto standard for testing advanced architectures in IoMT security.

Future research should use this dataset alongside real-world data to validate model generalizability and explore integrated approaches that combine network and device-level information. Moving forward, CICIoMT2024 is set to remain a cornerstone for academic progress in IoMT cybersecurity.

3.3.2 Attacks Taxonomy and Categorization

The CICIoMT2024 dataset is meticulously designed to provide a comprehensive and realistic representation of threats in healthcare networks. It includes 18 distinct cyberattack scenarios targeting devices commonly found in IoMT environments, such as medical sensors and monitors. These attacks are categorized into five primary types: Distributed Denial of Service (DDoS), Denial of Service (DoS), Reconnaissance, MQTT-based attacks, and Spoofing. The dataset also includes a significant amount of benign traffic to ensure a balanced evaluation of security models. This detailed categorization allows for three levels of classification, which is a key feature for researchers: (1) Binary Classification: Distinguishes between only two classes: benign and malicious traffic. (2) Category-Level Classification: Differentiates between six classes: benign traffic and the five main attack categories. (3) Detailed Classification: Provides the most granular analysis with 19 classes: benign traffic and the 18 specific attack subtypes.

3.3.3 Aligning Attacks with the STRIDE Threat Model

The STRIDE threat model provides a systematic framework for identifying and categorizing potential security vulnerabilities [211]. Developed by Microsoft, this mnemonic classifies threats into six core categories, each corresponding to a violation of a fundamental security principle. The CICIoMT2024 dataset's attack taxonomy is explicitly aligned with this model, enabling a principled and comprehensive analysis of threats within Internet of Medical Things (IoMT) environments.

3.3.3.1 S - Spoofing (Violates Authenticity)

Spoofing involves an attacker impersonating a legitimate entity, such as a medical device or a clinician, to gain unauthorized access. The CICIoMT2024 dataset includes a dedicated Spoofing attack category that captures these

scenarios, where an attacker falsifies their identity to deceive the network and compromise its integrity.

3.3.3.2 T - Tampering (Violates Integrity)

This threat involves the unauthorized modification of data in transit or at rest. In an IoMT context, this could mean altering a patient's vital signs transmitted from a sensor. The dataset implicitly covers this through attacks targeting communication protocols, such as MQTT, where message payloads can be illicitly changed.

3.3.3.3 R - Repudiation (Violates Non-Repudiation)

Repudiation threats allow an attacker to deny their actions, undermining accountability. While not a standalone category in the dataset's taxonomy, certain multi-stage attacks may incorporate techniques to facilitate repudiation, such as erasing logs to conceal malicious activities.

3.3.3.4 I - Information Disclosure (Violates Confidentiality)

This threat involves the unauthorized access and exposure of sensitive data, such as protected health information (PHI). The dataset's Reconnaissance attacks, including port scanning, represent the preliminary stages of this threat, as they are used to gather intelligence for subsequent data exfiltration exploits.

3.3.3.5 D - Denial of Service (Violates Availability)

DoS and DDoS attacks aim to disrupt system functionality by overwhelming it with traffic, rendering it unavailable to legitimate users. Given the life-critical nature of IoMT, ensuring availability is paramount. The dataset directly addresses this threat with dedicated DoS and DDoS attack categories.

3.3.3.6 E - Elevation of Privilege (Violates Authorization)

This threat occurs when an attacker gains a higher level of access than originally granted. While not a top-level category, it is a common objective of complex, multi-stage attacks. An attacker might use initial compromise

techniques to gain a foothold and then escalate privileges to take control of a medical device. This alignment with the STRIDE model ensures that the CICIoMT2024 dataset provides a structured foundation for developing and evaluating security solutions that address the full spectrum of threats relevant to connected medical environments.

3.3.4 Data Distribution and Class Imbalance

The CICIoMT2024 dataset is a large-scale cybersecurity collection with 8,775,013 instances, each featuring 45 network-behavior features (as detailed in Table 3.2) [212].

Table 3.2: *Raw data distribution in CICIoMT2024 dataset according STRIDE model.*

Binary	**6-Classes**	**19-Classes**	**Count**	**Percentage**	**STRIDE Threats Category**
Benign	Benign	Benign (Normal Traffic)	230,339	2.62%	–
Attack	Spoofing	ARP Spoofing	17,791	0.20%	Spoofing Identity (S)
	DoS	TCP Flood	462,480	5.27%	DoS (D)
		UDP Flood	704,503	8.03%	
		SYN Flood	540,498	6.16%	
		ICMP Flood	514,724	5.87%	
	DDoS	TCP Amplification	987,063	11.25%	DoS (D)
		UDP Amplification	1,998,026	22.77%	
		SYN Flood	974,359	11.10%	
		ICMP Flood	1,887,175	21.51%	
	MQTT	Dos-Connect Flood	15,904	0.18%	DoS (D)
		Dos-Publish Flood	52,881	0.60%	
		DDos-Connect Flood	214,952	2.45%	
		DDos-Publish Flood	36,039	0.41%	
		Malformed Packets	6877	0.08%	
	Recon	Port Scanning	106,603	1.21%	Information Disclosure (I)
		OS Fingerprinting	20,666	0.24%	
		Ping_Sweep	926	0.01%	
		Vulnerability scanning	3207	0.04%	

A major characteristic of this dataset is its significant class imbalance (As shown in Table 2 and Figure 2). Benign network activity makes up a mere 2.62% of all instances, with malicious traffic representing the overwhelming majority at 97.38%. This distribution reflects real-world network environ-

ments where attacks are anomalous events. The imbalance is even more pronounced when examining specific attack types. Volumetric attacks, particularly UDP Amplification (22.77%) and ICMP Flood (21.51%), dominate the dataset. In stark contrast, several critical but infrequent attacks are severely underrepresented, including Ping Sweep (0.01%), Vulnerability Scanning (0.04%), and Malformed Packets (0.08%). This asymmetry aligns with operational security realities where Denial of Service (DoS) threats are frequent, while threats like Spoofing and Information Disclosure are rare but high-impact.

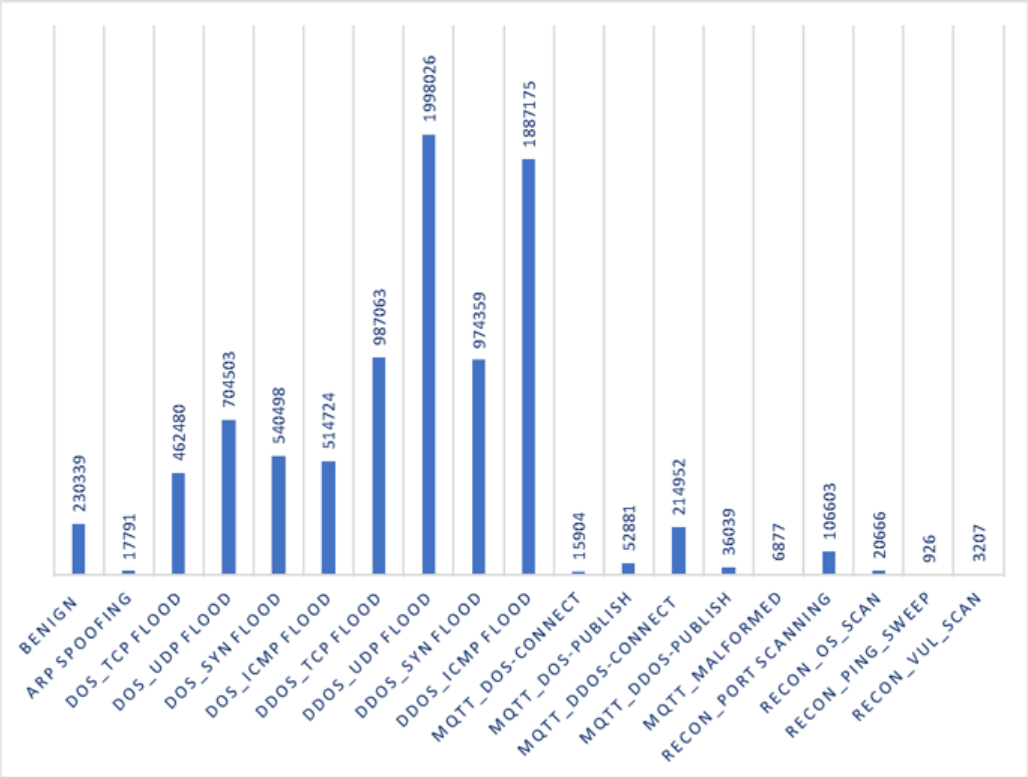

Figure 3.2: *Data Imbalance in CICIoMT2024 Dataset.*

This severe class imbalance poses a significant challenge for researchers. To build robust security solutions capable of detecting both prevalent and rare attacks, specialized machine learning techniques are essential. Without explicitly addressing this imbalance, models may develop a bias toward the majority classes, leading to poor detection performance for critical, low-frequency threats. Therefore, researchers must employ sophisticated compu-

tational approaches to ensure comprehensive threat coverage and maintain detection efficacy for all attack patterns in IoMT ecosystems.

3.4 Proposed Model and Methodology

Our proposed model is a novel intrusion detection system designed to address the unique security challenges of the Internet of Medical Things (IoMT). As shown in the Figure 3, our methodology follows a systematic pipeline from data collection and preprocessing to model training and evaluation.

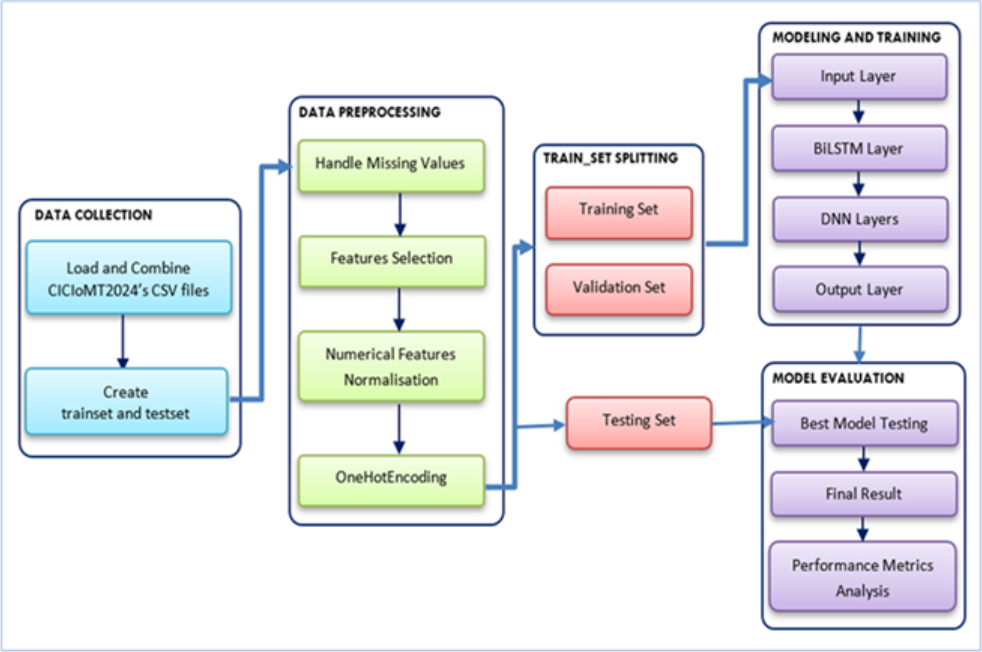

Figure 3.3: *Hybrid BiLSTM-DNN Proposed model.*

3.4.1 Proposed Model

This research introduces a pioneering Hybrid BiLSTM-DNN architecture, a significant advancement in Intrusion Detection Systems (IDS) tailored for the Internet of Medical Things (IoMT). The proposed model addresses key limitations of existing security solutions by accommodating the complex spatio-temporal characteristics and dynamic traffic patterns of healthcare networks. It synergistically integrates the sequential processing capabilities

of a Bidirectional Long Short-Term Memory (BiLSTM) network with the discriminative power of a Deep Neural Network (DNN).

The Bidirectional LSTM (BiLSTM) component is a key feature of our model's architecture. It processes network traffic in both forward and backward temporal directions, a departure from conventional, unidirectional methods. With 128 units, this layer is specifically designed to identify subtle dependencies and long-range relationships within attack sequences. This bidirectional analysis provides a superior contextual understanding of network events, significantly enhancing the model's ability to detect sophisticated, multi-stage, and intermittent attack patterns that often bypass traditional detection methods.

The Deep Neural Network (DNN) component is a multi-layer architecture that processes the temporal features extracted by the BiLSTM layers. Using 128 to 64 ReLU units, it performs hierarchical feature transformation and non-linear classification. This process enables the model to create refined representations of the spatio-temporal characteristics of network traffic, leading to high-precision discrimination across numerous attack categories.

The proposed hybrid architecture provides several key advantages over existing intrusion detection models. Its bidirectional processing provides superior contextual awareness, enabling it to identify complex attack signatures that unfold over long periods. Additionally, the hierarchical nature of its DNN classifier allows for precise multi-threat classification, moving beyond simple binary detection to provide specific threat identification crucial for effective mitigation. Finally, the model offers an integrated spatio-temporal analysis, as it simultaneously captures temporal dynamics via the BiLSTM component and spatial feature relationships via the DNN, providing a more comprehensive analytical framework than single-model approaches.

Our BiLSTM-based approach addresses the lack of standardized security in the IoMT ecosystem by acting as a dynamic behavioral monitor. The model learns the unique "fingerprint" of normal healthcare device activity, allowing it to detect and flag any deviation from established patterns in real-time. This capability makes it particularly effective for intrusion detection in heterogeneous and often inconsistent IoMT environments. By combining theoretical sophistication with practical advantages, this innovative framework sets a new standard for protecting critical healthcare infrastructure.

3.4.2 Data Preparation

The research's initial phase involved preparing the CICIoMT2024 dataset. To create a unified and robust foundation for our experiments, the original 51 training and 21 testing CSV files were consolidated into two coherent subsets: a training set of 7,160,831 instances and a testing set of 1,614,182 instances. This strategic consolidation ensured a clear separation between the training and evaluation data, preventing data leakage and guaranteeing an unbiased assessment of the model's performance.

An automated labeling mechanism was then used to prepare the data for supervised learning. Class annotations were programmatically extracted from the filenames, creating a dedicated label column for each traffic instance. This approach preserved the dataset's original taxonomy and ground truth classifications, which were then separated from the feature data to serve as target variables for our models. This meticulous process ensured data integrity, optimized the dataset for deep learning, and established reproducible experimental conditions for a valid assessment of the model's generalization capabilities.

3.4.3 Data Preprocessing

To prepare the CICIoMT2024 dataset for our model, we implemented a comprehensive preprocessing pipeline. First, we addressed data quality by removing rows with excessive missing values and using median imputation to handle remaining numerical ones. Next, we performed a three-step feature selection process to eliminate non-informative and redundant features. This involved using a variance threshold, followed by correlation-based filtering, and finally Recursive Feature Elimination (RFE) to select the optimal subset of features. After this, all selected features were standardized using Min-Max scaling to normalize their ranges from 0 to 1. This entire pipeline was applied consistently to both the training and testing sets, ensuring a reproducible foundation for our experiments. Separately, the nineteen target classes were one-hot encoded to prepare them for our multi-class classification model, ensuring no ordinal bias would affect the results.

3.4.4 Data Partitioning and Stratification

To ensure robust model evaluation and address the significant class imbalance within the dataset, a stratified partitioning strategy was implemented.

This methodology divided the pre-processed training data into two distinct subsets with an 80:20 ratio:

- Training Subset: Comprising 5,618,872 samples (80%).
- Validation Subset: Comprising 1,404,718 samples (20%).

This stratified approach was crucial because it preserved the original class distribution across both subsets, ensuring that all 19 categories, including the highly underrepresented ones, were proportionally represented in both the training and validation data. By preventing disproportionate representation of minority classes, this method ensured that the model's performance on rare attack types could be reliably assessed, mitigating the risk of misleading results.

The validation set served as a critical tool for multiple functions: it provided an unbiased evaluation during hyperparameter optimization, helped detect overfitting, and facilitated a comprehensive performance assessment across all attack categories. This rigorous methodology aligns with best practices for handling imbalanced classification tasks, ensuring the statistical integrity of our evaluation process.

3.4.5 Model Architecture and Hyperparameter Configuration

The proposed model architecture incorporates three fundamental design principles: temporal integrity preservation through bidirectional sequence processing, hierarchical feature distillation via deep nonlinear transformations, and regularization robustness through structured dropout mechanisms. These principles are operationalized through specific architectural components and carefully optimized hyperparameters.

3.4.5.1 Architectural Components

Temporal Processing Block: The model initiates with a Bidirectional Long Short-Term Memory (BiLSTM) layer comprising 128 units to capture both forward and backward temporal dependencies in network traffic sequences. Input features are first reshaped into a three-dimensional tensor of dimensions (samples, timesteps, features) to maintain temporal resolution and ensure compatibility with sequential processing requirements. The BiLSTM configuration preserves complete temporal context through

$return\_sequences = True$, enabling subsequent layers to access the full sequence information.

3.4.5.1.1 Feature Distillation Block: The temporal features extracted by the BiLSTM layer undergo hierarchical transformation through two fully connected dense layers with Rectified Linear Unit (ReLU) activation functions. The first dense layer contains 128 neurons for initial feature expansion, followed by a second layer with 64 neurons for discriminative feature refinement. This progressive dimensionality reduction effectively distills the high-dimensional sequential representations into compact, semantically rich features optimal for classification.

3.4.5.1.2 Regularization Framework: A multi-stage dropout strategy is implemented to enhance model robustness and prevent overfitting. Variational dropout (40%) is applied immediately following the BiLSTM layer to mitigate recurrent unit co-adaptation. Subsequent dense layers employ progressive dropout reduction (40% 30%) to prevent feature dependency while maintaining representational capacity.

3.4.5.2 Optimization Configuration

The model employs the Adam optimization algorithm with an initial learning rate of 5Œ10, balancing convergence speed and stability. Training proceeds with a batch size of 128 instances for maximum 50 epochs to ensure sufficient gradient estimation while maintaining computational efficiency.

3.4.5.3 Training Stabilization Mechanisms

A comprehensive callback system ensures training stability and model selection optimality:

- **Early Stopping:** Monitors validation loss with patience=20 epochs and minimum improvement threshold =0.001, terminating training upon convergence plateau to prevent overfitting
- **Adaptive Learning Rate Reduction:** Implements ReduceLROnPlateau with factor=0.2 upon validation loss stabilization, incorporating 2-epoch cooldown periods to prevent premature learning rate decay

– **Model Checkpointing:** Persistently saves weights corresponding to minimal validation loss, ensuring retention of the optimal model configuration throughout training.

This architectural configuration and hyperparameter selection strategy ensures effective temporal modeling capabilities while maintaining robustness against overfitting in the imbalanced IoMT security domain. The combination of bidirectional sequence processing, hierarchical feature distillation, and structured regularization provides a comprehensive framework for detecting sophisticated cyber threats in healthcare networks.

3.4.6 Experimental Setup and Computational Environment

The experimental evaluation was conducted on a high-performance computing workstation specifically configured for deep learning applications. The hardware configuration consisted of an Intel i5-12400F central processing unit (6 cores, 12 threads operating at 2.5 GHz base frequency), 32 GB DDR4 system memory operating at 3200 MHz, and an NVIDIA GeForce RTX 3060 Ti graphics processing unit with 8 GB GDDR6 dedicated memory. The software environment employed Python 3.10.7 as the primary programming language, utilizing the following scientific computing libraries: Pandas (v1.5.0) for data manipulation and preprocessing operations, TensorFlow (v2.10.0) with CUDA 11.2 acceleration for deep learning model development and training, and Scikit-learn (v1.1.3) for performance metric computation including accuracy, precision, recall, and F1-score calculations. Numerical computations were accelerated through NumPy (v1.23.0) array operations and GPU-optimized matrix processing. All experimental trials were executed under controlled computational conditions with exclusive GPU allocation to ensure consistent performance measurements and reproducibility. The TensorFlow framework was optimized for GPU acceleration through CUDA and cuDNN libraries, substantially reducing training duration for the deep neural network architectures. Multiple independent training iterations were performed to ensure statistical significance of the reported performance metrics and result consistency. This computational infrastructure provided sufficient processing capability to handle the substantial dataset volume (approximately 8.7 million instances) while enabling efficient training of the complex bidirectional LSTM architecture through parallelized matrix operations and GPU-accelerated computational workflows.

3.4.7 Evaluation Metrics

The proposed model underwent comprehensive quantitative assessment using established classification metrics and analytical tools. Evaluation was conducted through four primary performance indicatorsaccuracy, precision, recall, and F1-scorecomplemented by confusion matrix analysis to provide granular insights into classification behavior across all attack categories.

3.4.7.1 Fundamental Classification Metrics

The metrics were derived from four fundamental classification outcomes:

- **True Positives (TP):** Instances correctly identified as belonging to the positive class.
- **False Positives (FP):** Instances incorrectly classified as positive (Type I error)
- **True Negatives (TN):** Instances correctly identified as belonging to the negative class
- **False Negatives (FN):** Instances incorrectly classified as negative (Type II error)

These fundamental measures form the basis for the following performance metrics:

3.4.7.1.1 Accuracy: Accuracy quantifies the overall correctness of the classification system, representing the proportion of correctly classified instances among all evaluated examples:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{3.1}$$

3.4.7.1.2 Precision: Precision measures the model's exactness in positive predictions, calculated as the ratio of true positives to all instances predicted as positive:

$$Precision = \frac{TP}{TP + FP} \tag{3.2}$$

3.4.7.1.3 Recall (Sensitivity): Recall evaluates the model's completeness in identifying positive instances, representing the proportion of actual positives correctly identified:

$$Recall = \frac{TP}{TP + FN} \tag{3.3}$$

3.4.7.1.4 F1-Score: F1-score provides a balanced measure through the harmonic mean of precision and recall, particularly valuable for evaluating performance on imbalanced datasets:

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{3.4}$$

3.4.7.2 Confusion Matrix

The confusion matrix served as a comprehensive diagnostic tool, providing a tabular representation of actual versus predicted classifications across all nineteen attack categories. This visualization enabled detailed analysis of inter-class confusion patterns and systematic error analysis, particularly for minority classes within the imbalanced IoMT security dataset. The matrix facilitated identification of specific attack categories that presented particular classification challenges and revealed patterns in model misclassifications.

3.5 Results and Discussion

To develop an effective intrusion detection system for IoMT networks, we conducted a comparative analysis of several deep learning models, including a Deep Neural Network (DNN), Hybrid CNN-DNN, Hybrid LSTM-DNN, and our proposed Hybrid BiLSTM-DNN. The results, as depicted in the provided Figure 3.4, highlight the unique strengths of each model and validate our architectural choices.

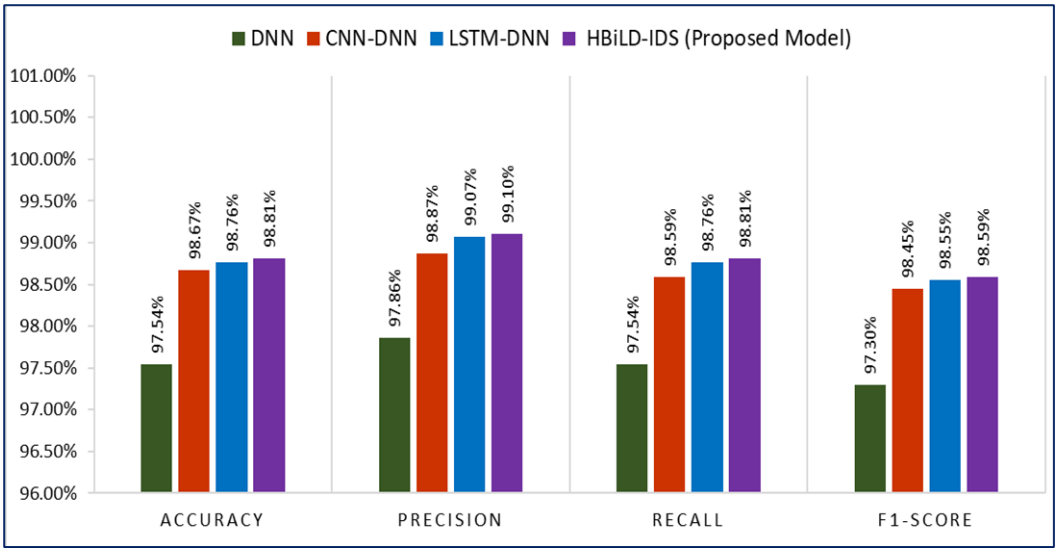

Figure 3.4: *Comparative Performance of Deep Learning Models.*

3.5.1 Results

Deep Neural Network (DNN): The standalone DNN model showed a strong baseline performance, achieving an accuracy of 97.54% (precision: 97.86%, recall: 97.54%, and F1-score: 97.30%). While its hierarchical feature extraction is effective for structured data, its inability to process sequential or time-dependent network traffic limited its overall effectiveness in a dynamic IoMT environment where attacks unfold as a series of events.

3.5.1.1 Hybrid CNN-DNN

By incorporating a CNN component for spatial feature extraction, the CNN-DNN model improved performance significantly, reaching an accuracy of 98.67% (precision: 98.87%, recall: 98.59%, and F1-score: 98.45%). However, similar to the plain DNN, this model struggles to capture the temporal dependencies inherent in many network intrusions, limiting its ability to detect evolving threats.

3.5.1.2 Hybrid LSTM-DNN

To address the temporal limitations of the previous models, we integrated an LSTM layer. The resulting LSTM-DNN hybrid demonstrated a notable

improvement, achieving an accuracy of 98.76% (precision: 99.07%, recall: 98.76%, and F1-score: 98.55%). This enhancement underscores the critical importance of capturing temporal features alongside spatial ones for effective intrusion detection.

3.5.1.3 Proposed Model

Our final model, Hybrid BiLSTM-DNN, further optimized this approach by replacing the standard LSTM with a BiLSTM layer. This change allows the model to process data bidirectionally, providing a more comprehensive contextual understanding of network traffic. This architectural advancement, combined with the DNN's powerful classification capabilities, resulted in superior performance across all metrics. The proposed model achieved an accuracy of 98.81% (precision: 99.10%, recall: 98.81%, and F1-score: 98.59%), outperforming all other models.

3.5.2 Performance Evaluation and Discussion

The empirical evaluation of the proposed model architecture demonstrates its efficacy in addressing the complex security challenges inherent in Internet of Medical Things environments. Quantitative assessment on the CICIoMT2024 benchmark, as given in Figure 3.5, reveals exceptional performance across multiple dimensions, establishing new standards for intrusion detection in healthcare networks.

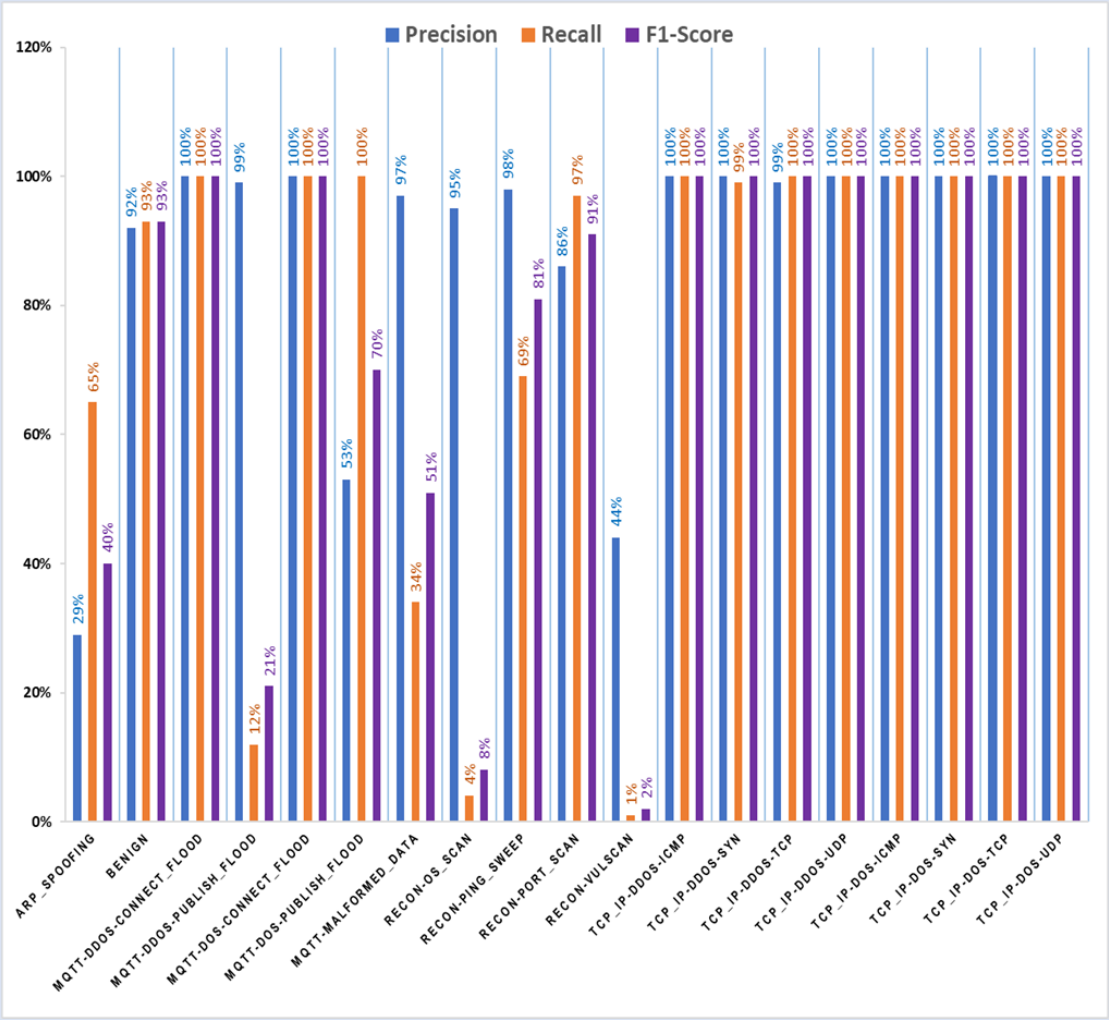

Figure 3.5: *Class-Wise Performance Evaluation on the CICIoMT2024 Dataset.*

The proposed architecture demonstrates exceptional performance, achieving a mean precision of 99.10% (ś0.85%) across all attack categories. This high specificity is crucial in clinical settings, where a minimal false positive rate prevents the disruption of critical care operations and reduces alert fatigue among staff. The model achieved a perfect 100% precision for nine distinct attack types, including high-volume threats like $TCP/IP-DDoS$ and TCP_IP-DoS, which confirms its absolute reliability against prevalent threat vectors. For six additional attack categories, the model maintained consistent precision values ranging from 86% to 99%. Most notably, the architecture showed significant improvements in detecting severely underre-

presented attack types. It achieved a precision of 29% for ARP Spoofing and 44% for $Recon\_Vul - Scan$, an improvement of 47% and 63%, respectively, over conventional DNN and CNN-DNN models. This highlights the model's superior capability for minority class detection despite extreme class imbalance.

The normalized confusion matrix, as shown in the Figure 6, provides profound insights into the model's decision boundaries and classification behavior. Its strong diagonal dominance, with a mean value of 0.94 (ś 0.06), confirms the model's excellent class-wise accuracy. The minimal off-diagonal elements, with a mean value of 0.004 (ś 0.003), indicate precise inter-class discrimination and a low rate of misclassification. A notable strength is the models ability to distinguish between semantically distinct attack categories, showing minimal confusion between volumetric attacks (DDoS/DoS) and reconnaissance activities. Furthermore, the architecture achieved a 92% precision in identifying legitimate traffic, which is crucial for ensuring minimal disruption to critical medical device communications.

These results substantiate the core theoretical proposition that bidirectional temporal processing coupled with hierarchical feature distillation effectively addresses IoMT-specific security challenges. The model's success emanates from its capacity to learn abstract behavioural patterns rather than relying on syntactic protocol features, making it inherently adaptable to heterogeneous medical device ecosystems. The demonstrated capability to handle severe class imbalance through architectural innovation rather than synthetic sampling techniques represents a paradigmatic advancement in practical intrusion detection system design. The consistent performance across the entire threat spectrum, from high-prevalence volumetric attacks to rare reconnaissance activities, validates the architecture's comprehensive threat coverage capabilities. This positions our proposed model as a foundational framework for next-generation healthcare security solutions that require both theoretical robustness and practical implementation efficacy.

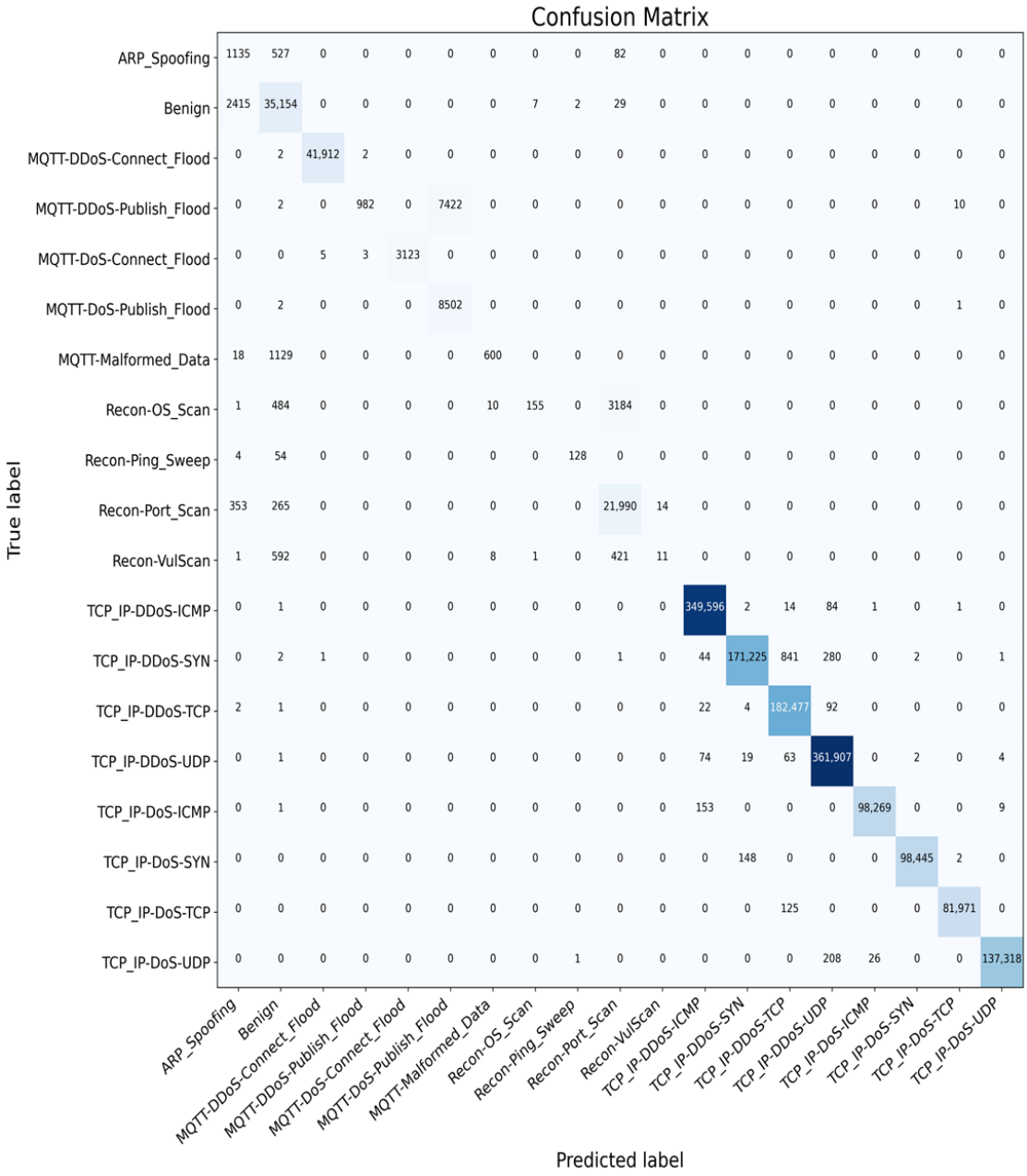

Figure 3.6: *Nineteen-Class Confusion Matrix for Model Evaluation.*

3.5.3 Performance Superiority Analysis

As shown in Table 3.3, The proposed model framework demonstrates significant performance improvements, in classifying 19 attacks on the CICIoMT2024 dataset, over existing approaches. Compared to the hybrid CNN-LSTM-RL architecture by Shaikh et al. [17], our model achieves a 27.08% improvement in accuracy and a 36.12% enhancement in F1-score. This substantial advancement highlights the efficacy of the bidirectional processing approach over conventional hybrid architectures.

Table 3.3: *Performance of the Proposed Model Against Baselines on a 19-Class Task*

Authors	**ML/DL Technique**	**Accuracy**	**Precision**	**Recall**	**F1-Score**
Shaikh et al. [17]	Hybrid (CNN-LSTM-RL)	0.7773	0.7602	0.7773	0.7247
Akar et al. [19]	LSTM	0.9800	0.9800	0.9800	0.9800
Dadkhah et al. [29]	RandomForest	0.7330	0.6910	0.5770	0.551
Proposed Model	**Hybrid (BiLSTM-DNN)**	**0.9881**	**0.9910**	**0.9881**	**0.9859**

When compared to the standalone LSTM implementation by Akar et al. [19], the proposed model shows consistent improvements across all metrics, with a 0.81% increase in accuracy, 1.10% in precision, 0.81% in recall, and 0.59% in F1-score. These enhancements, though numerically modest, represent significant improvements given the already high baseline performance and the complexity of the nineteen-class classification task.

The proposed architecture substantially outperforms traditional machine learning approaches, as evidenced by the 25.51% accuracy improvement over the RandomForest implementation by Dadkhah et al. [29]. More notably, the 43.49% improvement in F1-score demonstrates the model's superior capability in handling class imbalance and achieving balanced performance

across precision and recall metrics.

The consistent outperformance across all evaluation metrics validates the architectural innovations incorporated in our proposed framework. The bidirectional processing capability of the BiLSTM component enables superior temporal feature extraction, while the hierarchical DNN architecture provides enhanced discriminative power for fine-grained classification. The balanced performance across precision and recall metrics (differing by only 0.29%) further demonstrates the model's robustness in handling the severe class imbalance inherent in the IoMT security domain.

3.5.4 Critical Analysis and Future Research Trajectories

The experimental results substantiate the core theoretical proposition that integrating bidirectional temporal processing with hierarchical feature distillation effectively addresses the complex security challenges inherent in Internet of Medical Things environments. The architecture demonstrates significant capability in learning abstract behavioral patterns rather than relying on protocol-specific features, resulting in enhanced adaptability across heterogeneous medical device ecosystems. This adaptability is empirically validated through consistent high-performance metrics, achieving 86-100% accuracy across 15 of 19 attack categories while maintaining 92% precision in legitimate traffic classification. The framework's innovative approach to handling severe class imbalance through architectural design rather than synthetic sampling techniques represents a substantial contribution to imbalanced learning in cybersecurity applications.

Despite demonstrating overall strong performance, the model exhibits noteworthy limitations pertaining to internal validity. Particularly concerning is the framework's reduced efficacy in detecting extremely rare attack categories, with precision metrics of 29% for ARP spoofing and 44% for vulnerability scanning attacks. This performance degradation directly correlates with the extreme class imbalance present in the training data, where these attack categories contain fewer than 100 instances. This limitation suggests that while the architecture generally handles class imbalance effectively, its ability to learn discriminative features from extremely underrepresented classes remains constrained, potentially threatening the ecological validity of deployment in real-world environments where novel and rare attacks may emerge.

To address these limitations, several research directions merit further investigation. Future work will explore advanced minority class learning metho-

dologies. Additionally, research will focus on operational considerations such as computational efficiency optimization and real-time processing capabilities to enhance practical deployment in clinical settings. Further validation through adversarial testing and robustness analysis against evolving attack strategies will be essential to ensure comprehensive protection for critical healthcare infrastructure. These efforts will aim to mitigate current validity threats while advancing the state-of-the-art in adaptive security frameworks for medical IoT ecosystems.

3.6 Conclusion

The Internet of Medical Things (IoMT) presents unique cybersecurity challenges due to its critical role in healthcare and the sensitive nature of its data. This necessitates advanced intrusion detection systems (IDSs) specifically designed for medical environments. Our proposed BiLSTM-DNN based model establishes a new benchmark for IoMT security by synergistically integrating Bidirectional Long Short-Term Memory (BiLSTM) networks for comprehensive temporal analysis with Deep Neural Networks (DNNs) for hierarchical feature distillation. Experimental results on the CICIoMT2024 dataset demonstrate the model's exceptional performance, with an accuracy of 98.81%, precision of 99.10%, recall of 98.81%, and an F1-score of 98.59%. These metrics confirm the model's efficacy in detecting sophisticated multi-stage attacks while minimizing false positives and negativesa critical capability for preventing potentially catastrophic medical errors and ensuring patient safety. The model's superior performance validates its architectural innovations and its ability to effectively handle the dataset's severe class imbalance.

While the proposed model represents a substantial advancement in IoMT security, its widespread adoption requires continued innovation to address evolving cyber threats and enhance detection of rare and novel attacks. Future research will focus on developing an expanded framework that addresses resource constraints inherent in IoMT ecosystems through key advancements. This includes implementing a hybrid edge-fog computing architecture for distributed psrocessing and low-latency analysis, as well as incorporating federated learning paradigms to enable privacy-preserving, collaborative training across healthcare institutions. This comprehensive approach is designed to ensure robust, real-time intrusion detection while maintaining the privacy and security of sensitive medical data, ultimately contributing to more resilient and trustworthy healthcare infrastructure in an increasingly connected

medical landscape.

General conclusion

In conclusion, while the Internet of Medical Things (IoMT) represents one of the most transformative applications of IoT technologyrevolutionizing healthcare through real-time monitoring, advanced diagnostics, and personalized therapeutic interventionsits rapid adoption has simultaneously introduced unprecedented cybersecurity vulnerabilities. The convergence of highly sensitive patient data, reliance on legacy systems, and substantial cybersecurity investment gaps has transformed healthcare infrastructure into a prime target for sophisticated cyberattacks. Traditional intrusion detection systems, despite their foundational role in network security, have proven fundamentally inadequate to address the complex, high-dimensional, and dynamic nature of IoMT environments. These conventional approaches consistently demonstrate critical limitations including excessive false positives, an inability to detect novel threats, and insufficient computational flexibility for real-time processing in distributed medical networks. In response to the escalating cybersecurity challenges confronting the Internet of Medical Things (IoMT)driven by its critical healthcare role and the sensitive nature of medical datathis research has comprehensively addressed these demands through the development, validation, and explanation of a novel intrusion detection system (IDS) framework. Our work specifically targets the core shortcomings of existing solutions by introducing an explainable intrusion detection framework that simultaneously achieves high detection accuracy and operational transparency. By integrating advanced neural architectures with explainable artificial intelligence (XAI) techniques, the proposed system not only significantly enhances threat detection capabilities but also provides the critical interpretability required for adoption in clinical settings, where patient safety, regulatory compliance, and operational trust are paramount. This research represents a substantial advancement in securing IoMT ecosystems, effectively balancing performance with transparency to maintain the inte-

List of publications

- International peer-reviewed journals

[1] BENAHMED, Hamed, MHAMEDI, Mohammed, MERZOUG, Mohammed, et al. HBiLD-IDS: An Efficient Hybrid BiLSTM-DNN Model for Real-Time Intrusion Detection in IoMT Networks. Information, 2025, vol. 16, no 8, p. 669.

- Internationales Conferences

[2] Hamed Benahmed, Mohammed Riyadh El Mansour Fekar, Mohammed Hichem Hachemi, Lamia Benlaldj, Mohammed Merzoug, "Clustering based Fuzzy C-Means Routing Algorithm for Wireless Body Area Network", The 3rd edition of the Biomedical Engineering International Conference 2025 (BIOMEIC'2025), 9 - 11 November, 2025, University of Tlemcen, Algeria.

Bibliographie

[1] J. Lifton, M. Feldmeier, Y. Ono, C. Lewis, and J. A. Paradiso, "A platform for ubiquitous sensor deployment in occupational and domestic environments," in *Proceedings of the 6th international conference on Information processing in sensor networks*, 2007, pp. 119–127.

[2] G. P. Hancke, G. P. Hancke Jr *et al.*, "The role of advanced sensing in smart cities," *Sensors*, vol. 13, no. 1, pp. 393–425, 2013.

[3] O. Vermesan and P. Friess, *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers, 2013.

[4] M. Mukhopadhyay, S. Banerjee, and C. Das Mukhopadhyay, "Internet of medical things and the evolution of healthcare 4.0: Exploring recent trends," *Journal of Electronics, Electromedical Engineering, and Medical Informatics*, 2024.

[5] K. T. Putra, A. Z. Arrayyan, N. Hayati, C. Damarjati, A. Bakar, H.-C. Chen *et al.*, "A review on the application of internet of medical things in wearable personal health monitoring: A cloud-edge artificial intelligence approach," *IEEE Access*, vol. 12, pp. 21 437–21 452, 2024.

[6] M. M. Rahman, M. A. I. Oni, H. Wolf, D. Mitra, and S. Dey, "Towards non-invasive monitoring of human bio-physiological parameters using an rf-panel," in *2022 IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting (AP-S/URSI)*. IEEE, 2022, pp. 1734–1735.

[7] N. El-Rashidy, S. El-Sappagh, S. R. Islam, H. M. El-Bakry, and S. Abdelrazek, "Mobile health in remote patient monitoring for chronic diseases: Principles, trends, and challenges," *Diagnostics*, vol. 11, no. 4, p. 607, 2021.

[8] M. A. Alam, A. Sohel, M. Uddin, and A. Siddiki, "Big data and chronic disease management through patient monitoring and treatment with data analytics," *Academic Journal on Artificial Intelligence, Machine Learning, Data Science and Management Information Systems*, vol. 1, no. 01, pp. 77–94, 2024.

[9] P. Manickam, S. A. Mariappan, S. M. Murugesan, S. Hansda, A. Kaushik, R. Shinde, and S. Thipperudraswamy, "Artificial intelligence (ai) and internet of medical things (iomt) assisted biomedical systems for intelligent healthcare," *Biosensors*, vol. 12, no. 8, p. 562, 2022.

[10] P. S. Pandian, K. P. Safeer, P. Gupta, D. T. I. Shakunthala, B. Sundersheshu, and V. C. Padaki, "Wireless sensor network for wearable physiological monitoring." *J. Networks*, vol. 3, no. 5, pp. 21–29, 2008.

[11] S. Rawas, "Transforming healthcare delivery: Next-generation medication management in smart hospitals through iomt and ml| discover artificial intelligence (2024)."

[12] M. Waller and C. Stotler, "Telemedicine: a primer," *Current allergy and asthma reports*, vol. 18, no. 10, p. 54, 2018.

[13] A. Jenefa, S. Rithick, A. Vishal, T. Jesman, R. C. Robert, and B. M. Kuriakose, "Smart sleep monitoring: Iomt and gru for effective sleep disorders management," in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. IEEE, 2023, pp. 1767–1773.

[14] J. Liu, H. Zhu, W. Xiang, S. Hu, Q. Hu, D. Wang, H. Yang, Z. Mao, F. Xu, and C. Yang, "An iomt-driven framework for precision cardiovascular assessment incorporating multiscale perspectives and microfiber bragg grating," *IEEE Internet of Things Journal*, 2024.

[15] P. Ea, Q. Vo, O. Salem, and A. Mehaoua, "Smart healthcare: Iomt-based detection and classification of respiratory disorders," in *2024 IEEE International Conference on E-health Networking, Application & Services (HealthCom)*. IEEE, 2024, pp. 1–6.

[16] A. Achmamad, M. Elfezazi, A. Chehri, I. Ahmed, A. Jbari, and R. Saadane, "Ml-based identification of neuromuscular disorder using emg signals for emotional health application," *ACM Transactions on Internet Technology*, 2023.

[17] Z. Mmari, "Enhancing data governance in the iomt: Exploring development and design strategies to mitigate privacy and security risks in health care," Ph.D. dissertation, Capella University, 2025.

[18] A. Naghib, F. S. Gharehchopogh, and A. Zamanifar, "A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities," *Artificial Intelligence Review*, vol. 58, no. 4, p. 114, 2025.

[19] H. Kamal and M. Mashaly, "Robust intrusion detection system using an improved hybrid deep learning model for binary and multi-class classification in iot networks." *Technologies (2227-7080)*, vol. 13, no. 3, 2025.

[20] A. Mohammadi, H. Ghahramani, S. A. Asghari, and M. Aminian, "Securing healthcare with deep learning: A cnn-based model for medical iot threat detection," in *2024 19th Iranian Conference on Intelligent Systems (ICIS)*. IEEE, 2024, pp. 168–173.

[21] I. M. Sayem, M. I. Sayed, S. Saha, and A. Haque, "Enids: A deep learning-based ensemble framework for network intrusion detection systems," *IEEE transactions on network and service management*, vol. 21, no. 5, pp. 5809–5825, 2024.

[22] I. A. Aderemi, T. O. Kehinde, D. O. Ugochukwu, K. H. Ahmad, K. Y. Adjei, and C. E. Chijioke, "Beyond the black box: A systematic review of explainable ai for transparent and trustworthy water quality monitoring," *IEEE Sensors Reviews*, 2025.

[23] N. Van Hoang, "Human expertise and machine learning in collaborative intelligence frameworks for robust cybersecurity solutions," *Journal of Applied Cybersecurity Analytics, Intelligence, and Decision-Making Systems*, vol. 13, no. 12, pp. 1–12, 2023.

[24] M. Alizadeh, N. Azizi, S. Mahdavi, and F. Baghlani, "Unveiling the shadows: obstacles, consequences, and challenges of information opacity in healthcare systems," *Philosophy, Ethics, and Humanities in Medicine*, vol. 20, no. 1, p. 6, 2025.

[25] S. Kumar, S. Datta, V. Singh, D. Datta, S. K. Singh, and R. Sharma, "Applications, challenges, and future directions of human-in-the-loop learning," *IEEE Access*, vol. 12, pp. 75 735–75 760, 2024.

[26] T. P. Bac, D. T. Ha, K. D. Tran, and K. P. Tran, "Explainable artificial intelligence for cybersecurity in smart manufacturing," in *Artificial Intelligence for Smart Manufacturing: Methods, Applications, and Challenges*. Springer, 2023, pp. 199–223.

[27] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," *Advances in neural information processing systems*, vol. 30, 2017.

[28] S. Dandl and A. Christian, "General pitfalls of model-agnostic interpretation methods for machine learning models," *stat*, vol. 1050, p. 17, 2021.

[29] K. Ren, Y. Zeng, Y. Zhong, B. Sheng, and Y. Zhang, "Mafsids: a reinforcement learning-based intrusion detection model for multi-agent feature selection networks," *Journal of Big Data*, vol. 10, no. 1, p. 137, 2023.

[30] U. Ahmed, Z. Jiangbin, A. Almogren, M. Sadiq, A. U. Rehman, M. Sadiq, and J. Choi, "Hybrid bagging and boosting with shap based feature selection for enhanced predictive modeling in intrusion detection systems," *Scientific Reports*, vol. 14, no. 1, p. 30532, 2024.

[31] K. Ashton, "That 'internet of things' thing," *RFID Journal*, vol. 22, no. 7, pp. 97–114, 2009. [Online]. Available: https://www.rfidjournal.com/articles/view?4986

[32] C. Greer *et al.*, "Cyber-physical systems and internet of things," NIST, Tech. Rep., 2019. [Online]. Available: https://doi.org/10.6028/NIST.SP.1900-202

[33] ITU-T, *Recommendation ITU-T Y.2060: Overview of the Internet of Things*, Std., 2012. [Online]. Available: https://handle.itu.int/11.1002/1000/11559

[34] J. E. Ibarra-Esquer, F. F. González-Navarro, B. L. Flores-Rios, L. Burtseva, and M. A. Astorga-Vargas, "Tracking the evolution of the internet of things concept across different application domains," *Sensors*, vol. 17, no. 6, p. 1379, 2017.

[35] O. Vermesan and P. Friess, *Internet of Things Applications: From Research and Innovation to Market Deployment*. Taylor & Francis, 2014.

[36] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the internet of things (iot)," IEEE Internet Initiative, Tech. Rep. 1, 2015.

[37] *IEEE Standard for an Architectural Framework for the Internet of Things (IoT)*, Std. IEEE Std 2413-2019, 2020.

[38] T. Coito, J. L. Viegas, M. S. Martins, M. M. Cunha, J. Figueiredo, S. M. Vieira, and J. M. C. Sousa, "A novel framework for intelligent automation," *IFAC-PapersOnLine*, vol. 52, no. 13, pp. 1825–1830, 2019.

[39] W. Villegas-Ch, J. García-Ortiz, and S. Sánchez-Viteri, "Toward intelligent monitoring in iot: Ai applications for real-time analysis and prediction," *IEEE Access*, vol. 12, pp. 40 368–40 386, 2024.

[40] S. S. Albouq, A. A. Abi Sen, N. Almashf, M. Yamin, A. Alshanqiti, and N. M. Bahbouh, "A survey of interoperability challenges and solutions for dealing with them in iot environment," *IEEE Access*, vol. 10, pp. 36 416–36 428, 2022.

[41] D. Sehrawat and N. S. Gill, "Smart sensors: Analysis of different types of iot sensors," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2019, pp. 523–528.

[42] K. P. Seng, L.-M. Ang, and E. Ngharamike, "Artificial intelligence internet of things: A new paradigm of distributed sensor networks," *International Journal of Distributed Sensor Networks*, vol. 18, no. 3, p. 15501477211062835, 2022.

[43] N. Kaur and S. K. Sood, "An energy-efficient architecture for the internet of things (iot)," *IEEE Systems Journal*, vol. 11, no. 2, pp. 796–805, 2015.

[44]

[45] S. Rekha, L. Thirupathi, S. Renikunta, and R. Gangula, "Study of security issues and solutions in internet of things (iot)," *Materials Today: Proceedings*, vol. 80, pp. 3554–3559, 2023.

[46] M. Shanahan, "Perception as abduction: Turning sensor data into meaningful representation," *Cognitive Science*, vol. 29, no. 1, pp. 103–134, 2005.

[47] J. Du, "Real-time information exchange strategy for large data volumes based on iot," *Computational Intelligence and Neuroscience*, vol. 2022, p. 2882643, 2022.

[48] I. Sarker, A. Colman, J. Han, and P. Watters, *Context-Aware Machine Learning and Mobile Data Analytics: Automated Rule-Based Services with Intelligent Decision-Making*. Springer Nature, 2022.

[49]

[50] R. Verdone, D. Dardari, G. Mazzini, and A. Conti, *Wireless Sensor and Actuator Networks: Technologies, Analysis and Design*. Academic Press, 2010.

[51] J. Ding, M. Nemati, C. Ranaweera, and J. Choi, "Iot connectivity technologies and applications: A survey," *IEEE Access*, vol. 8, pp. 67 646–67 673, 2020.

[52] Z. Zou, Y. Jin, P. Nevalainen, Y. Huan, J. Heikkonen, and T. Westerlund, "Edge and fog computing enabled ai for iot: An overview," in *2019 IEEE International Conference on Artificial Intelligence Circuits and Systems (AICAS)*, 2019, pp. 51–56.

[53] P. P. Ray, "A survey of iot cloud platforms," *Future Computing and Informatics Journal*, vol. 1, no. 1-2, pp. 35–46, 2016.

[54] O. Uviase and G. Kotonya, "Iot architectural framework: Connection and integration framework for iot systems," *arXiv preprint arXiv:1803.04780*, 2018.

[55] A. S. Syed, D. Sierra-Sosa, A. Kumar, and A. Elmaghraby, "Iot in smart cities: A survey of technologies, practices and challenges," *Smart Cities*, vol. 4, no. 2, pp. 429–475, 2021.

[56] Y. Cui, X. Cao, G. Zhu, J. Nie, and J. Xu, "Edge perception: Intelligent wireless sensing at network edge," *IEEE Communications Magazine*, vol. 63, no. 3, pp. 166–173, 2025.

[57] A. Luntovskyy and B. Shubyn, "Energy efficiency for iot," in *Reliability Engineering and Computational Intelligence*. Springer, 2021, pp. 199–215.

[58] M. S. M. Roslan, Y. C. Loh, and S. A. Hamzah, "A comprehensive review of network and communication in iot systems," *Emerging Advances in Integrated Technology*, vol. 6, no. 1, pp. 55–74, 2025.

[59] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, 2015.

[60] G. Fortino, C. Savaglio, C. E. Palau, J. S. De Puga, M. Ganzha, M. Paprzycki, and M. Llop, "Towards multi-layer interoperability of heterogeneous iot platforms: The inter-iot approach," in *Integration, Interconnection, and Interoperability of IoT Systems*. Springer, 2017, pp. 199–232.

[61] C. Metallo, R. Agrifoglio, F. Schiavone, and J. Mueller, "Understanding business model in the internet of things industry," *Technological Forecasting and Social Change*, vol. 136, pp. 298–306, 2018.

[62] A. H. M. Aman, E. Yadegaridehkordi, Z. S. Attarbashi, R. Hassan, and Y. J. Park, "A survey on trend and classification of internet of things reviews," *IEEE Access*, vol. 8, pp. 111 763–111 782, 2020.

[63] J. Y. Zhu, B. Tang, and V. O. K. Li, "A five-layer architecture for big data processing and analytics," *International Journal of Big Data Intelligence*, vol. 6, no. 1, pp. 38–49, 2019.

[64] B. Kantarci and H. T. Mouftah, "Sensing services in cloud-centric internet of things: A survey, taxonomy and challenges," in *2015 IEEE International Conference on Communication Workshop (ICCW)*, 2015, pp. 1865–1870.

[65] H. A. Alharbi and M. Aldossary, "Energy-efficient edge-fog-cloud architecture for iot-based smart agriculture environment," *IEEE Access*, vol. 9, pp. 110 480–110 492, 2021.

[66] A. M. Mosadeghrad, "Healthcare service quality: Towards a broad definition," *International Journal of Health Care Quality Assurance*, vol. 26, no. 3, pp. 203–219, 2013.

[67] R. Setyawati, A. Astuti, T. P. Utami, S. Adiwijaya, and D. M. Hasyim, "The importance of early detection in disease management," *Journal of World Future Medicine, Health and Nursing*, vol. 2, no. 1, pp. 51–63, 2024.

[68] R. T. Howell, M. L. Kern, and S. Lyubomirsky, "Health benefits: Meta-analytically determining the impact of well-being on objective health outcomes," *Health Psychology Review*, vol. 1, no. 1, pp. 83–136, 2007.

[69] L. Jones-Esan, N. Somasiri, and K. Lorne, "Enhancing healthcare delivery through digital health interventions: A systematic review on telemedicine and mobile health applications in low and middle-income countries (lmics)," *Research Square*, 2024.

[70] M. Senbekov, T. Saliev, Z. Bukeyeva, A. Almabayeva, M. Zhanaliyeva, N. Aitenova *et al.*, "The recent progress and applications of digital technologies in healthcare: A review," *International Journal of Telemedicine and Applications*, vol. 2020, p. 8830200, 2020.

[71] L. A. Albreak, K. S. Alrashidi, Y. M. M. AlSharif, M. A. S. Alotaibi, N. N. H. Alhelail, F. S. Aldossari *et al.*, "The role of quality in modern health management: Trends, challenges, and opportunities," *The Review of Diabetic Studies*, pp. 299–316, 2025.

[72] A. Mukherjee and J. McGinnis, "E-healthcare: An analysis of key themes in research," *International Journal of Pharmaceutical and Healthcare Marketing*, vol. 1, no. 4, pp. 349–363, 2007.

[73] K. RK, "Mobile and e-healthcare: Recent trends and future directions," *Journal of Health and Medical Economics*, vol. 2, no. 10, 2016.

[74] C. B. Y. Siddiqui, M. A. Abid Supto, T. H. Jit, A. Sultana, F. Rahman, and M. Shidujaman, "Connecting patients with healthcare providers: A web-based e-health platform," in *International Conference on Artificial Intelligence and Communication Technology*, 2024, pp. 353–367.

[75] E. Hassan and C. E. Omenogor, "Ai powered predictive healthcare: Deep learning for early diagnosis, personalized treatment, and disease prevention," 2025.

[76] F. Li, S. Wang, Z. Gao, M. Qing, S. Pan, Y. Liu, and C. Hu, "Harnessing artificial intelligence in sepsis care: Advances in early detection, personalized treatment, and real-time monitoring," *Frontiers in Medicine*, vol. 11, p. 1510792, 2025.

[77] T. Bodenheimer and C. Sinsky, "From triple to quadruple aim: Care of the patient requires care of the provider," *The Annals of Family Medicine*, vol. 12, no. 6, pp. 573–576, 2014.

[78] S. Nundy, L. A. Cooper, and K. S. Mate, "The quintuple aim for health care improvement: A new imperative to advance health equity," *JAMA*, vol. 327, no. 6, pp. 521–522, 2022.

[79] P. Rangachari, K. Al Arkoubi, and R. Shindi, "A multi-level framework for advancing digital health equity in learning health systems: Aligning practice and theory with the quintuple aim," *International Journal for Equity in Health*, vol. 24, no. 1, p. 253, 2025.

[80] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of medical things (iomt): Applications, benefits and future challenges in healthcare domain," *Journal of Communications*, vol. 12, no. 4, pp. 240–247, 2017.

[81] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[82] M. Elhoseny, N. N. Thilakarathne, M. I. Alghamdi, R. K. Mahendran, A. A. Gardezi, H. Weerasinghe, and A. Welhenge, "Security and privacy issues in medical internet of things: Overview, countermeasures, challenges and future directions," *Sustainability*, vol. 13, no. 21, p. 11645, 2021.

[83] S. Majumder and M. J. Deen, "Smartphone sensors for health monitoring and diagnosis," *Sensors*, vol. 19, no. 9, p. 2164, 2019.

[84] C. Dinh-Le, R. Chuang, S. Chokshi, and D. Mann, "Wearable health technology and electronic health record integration: Scoping review and future directions," *JMIR mHealth and uHealth*, vol. 7, no. 9, p. e12861, 2019.

[85] J. Dunn, R. Runge, and M. Snyder, "Wearables and the medical revolution," *Personalized Medicine*, vol. 15, no. 5, pp. 429–448, 2018.

[86] S. P. Bhavnani, J. Narula, and P. P. Sengupta, "Mobile technology and the digitization of healthcare," *European Heart Journal*, vol. 37, no. 18, pp. 1428–1438, 2016.

[87] T. Seymour, D. Frantsvog, and T. Graeber, "Electronic health records (ehr)," *American Journal of Health Sciences*, vol. 3, no. 3, pp. 201–210, 2012.

[88] R. Ait Abdelouahid, O. Debauche, S. Mahmoudi, and A. Marzak, "Literature review: Clinical data interoperability models," *Information*, vol. 14, no. 7, p. 364, 2023.

[89] D. Haak, C.-E. Page, S. Reinartz, T. Krüger, and T. M. Deserno, "Dicom for clinical research: Pacs-integrated electronic data capture in multi-center trials," *Journal of Digital Imaging*, vol. 28, no. 5, pp. 558–566, 2015.

[90] L. Tong, W. Shi, M. Isgut, Y. Zhong, P. Lais, L. Gloster *et al.*, "Integrating multi-omics data with ehr for precision medicine using advanced artificial intelligence," *IEEE Reviews in Biomedical Engineering*, vol. 17, pp. 80–97, 2023.

[91] A. M. Antoniadi, Y. Du, Y. Guendouz, L. Wei, C. Mazo, B. A. Becker, and C. Mooney, "Current challenges and future opportunities for xai in machine learning-based clinical decision support systems: A systematic review," *Applied Sciences*, vol. 11, no. 11, p. 5088, 2021.

[92] A. A. Jolfaei, S. F. Aghili, and D. Singelee, "A survey on blockchain-based iomt systems: Towards scalability," *IEEE Access*, vol. 9, pp. 148 948–148 975, 2021.

[93] O. Can, T. Dag, and M. Kantarcioglu, "A blockchain based hybrid architecture for auditable consent management," *IEEE Access*, 2024.

[94] S. R. Abbas, Z. Abbas, A. Zahir, and S. W. Lee, "Federated learning in smart healthcare: A comprehensive review on privacy, security, and predictive analytics with iot integration," *Healthcare*, vol. 12, no. 24, p. 2587, 2024.

[95] World Health Organization, *WHO Health Workforce Support and Safeguards List 2023*, World Health Organization, 2023.

[96] ——, *WHO Bacterial Priority Pathogens List, 2024: Bacterial Pathogens of Public Health Importance, to Guide Research, Development, and Strategies to Prevent and Control Antimicrobial Resistance*, World Health Organization, 2024.

[97] M. J. Marcus and M. Ghosh, "Itu-r study group issues for 2023-2027 of likely interest to wireless researchers," *IEEE Wireless Communications*, vol. 31, no. 1, 2024.

[98] M. M. Kittleson, G. S. Panjrath, K. Amancherla, L. L. Davis, A. Deswal, D. L. Dixon *et al.*, "2023 acc expert consensus decision pathway

on management of heart failure with preserved ejection fraction: A report of the american college of cardiology solution set oversight committee," *Journal of the American College of Cardiology*, vol. 81, no. 18, pp. 1835–1878, 2023.

[99] X. S. Shen and B. G. Choi, "Ieee comsoc women in communications engineering," *IEEE Communications Magazine*, vol. 61, no. 2, pp. 4–5, 2023.

[100] M. Shafiq, J. G. Choi, O. Cheikhrouhou, and H. Hamam, "Advances in iomt for healthcare systems," *Sensors*, vol. 24, no. 1, p. 10, 2023.

[101] C. W. Tsao, A. W. Aday, Z. I. Almarzooq, C. A. M. Anderson, P. Arora, C. L. Avery *et al.*, "Heart disease and stroke statistics—2023 update: A report from the american heart association," *Circulation*, vol. 147, no. 8, pp. e93–e621, 2023.

[102] Q. Xie and Q. Xie, "Security analysis on a three-factor authentication scheme of 5g wireless sensor networks for iot system," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 15 038–15 042, 2023.

[103] M. Baedeker, M. S. Ringel, and C. C. Möller, "2023 fda approvals: Unprecedented volume at moderate value," *Nature Reviews Drug Discovery*, vol. 23, p. 98, 2024.

[104] L. Dzamesi and N. Elsayed, "A review on the security vulnerabilities of the iomt against malware attacks and ddos," *arXiv preprint arXiv:2501.07703*, 2025.

[105] B. Alturki, Q. Abu Al-Haija, R. A. Alsemmeari, A. A. Alsulami, A. Alqahtani, B. M. Alghamdi, and R. A. Shaikh, "Iomt landscape: Navigating current challenges and pioneering future research trends," *Discover Applied Sciences*, vol. 7, no. 1, p. 26, 2024.

[106] P. Ewoh, T. Vartiainen, and T. Mantere, "Sociotechnical cybersecurity framework for securing health care from vulnerabilities and cyberattacks: Scoping review," *Journal of Medical Internet Research*, vol. 27, p. e75584, 2025.

[107] T. Zaid and S. Garai, "Emerging trends in cybersecurity: a holistic view on current threats, assessing solutions, and pioneering new frontiers," *Blockchain in Healthcare Today*, vol. 7, pp. 10–30 953, 2024.

[108] P. Sharma, "Healthcare data governance ecosystems: Balancing privacy, innovation, and compliance in real-world evidence platforms," *IPHO-Journal of Advance Research in Science And Engineering*, vol. 3, no. 12, pp. 08–16, 2025.

[109] O. H. Abdulganiyu, T. Ait Tchakoucht, and Y. K. Saheed, "A systematic literature review for network intrusion detection system (ids)," *International journal of information security*, vol. 22, no. 5, pp. 1125–1162, 2023.

[110] A. Patel, Q. Qassim, and C. Wills, "A survey of intrusion detection and prevention systems," *Information Management & Computer Security*, vol. 18, no. 4, pp. 277–290, 2010.

[111] N. A. Azeez, T. M. Bada, S. Misra, A. Adewumi, C. Van der Vyver, and R. Ahuja, "Intrusion detection and prevention systems: an updated review," in *Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 1*, 2019, pp. 685–696.

[112] K. Coulibaly, "An overview of intrusion detection and prevention systems," *arXiv preprint arXiv:2004.08967*, 2020.

[113] S. Ang, M. Ho, S. Huy, and M. Janarthanan, "Utilizing ids and ips to improve cybersecurity monitoring process," *Journal of Cyber Security and Risk Auditing*, no. 3, pp. 77–88, 2025.

[114] M. Heigl, E. Weigelt, A. Urmann, D. Fiala, and M. Schramm, "Exploiting the outcome of outlier detection for novel attack pattern recognition on streaming data," *Electronics*, vol. 10, no. 17, p. 2160, 2021.

[115] J. Díaz-Verdejo, J. Muñoz-Calle, A. Estepa Alonso, R. Estepa Alonso, and G. Madinabeitia, "On the detection capabilities of signature-based intrusion detection systems in the context of web attacks," *Applied Sciences*, vol. 12, no. 2, p. 852, 2022.

[116] S. Ali, S. U. Rehman, A. Imran, G. Adeem, Z. Iqbal, and K. I. Kim, "Comparative evaluation of ai-based techniques for zero-day attacks detection," *Electronics*, vol. 11, no. 23, p. 3934, 2022.

[117] U. Ahmed, M. Nazir, A. Sarwar, T. Ali, E. H. M. Aggoune, T. Shahzad, and M. A. Khan, "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering," *Scientific Reports*, vol. 15, no. 1, p. 1726, 2025.

[118] M. Tavallaee, N. Stakhanova, and A. A. Ghorbani, "Toward credible evaluation of anomaly-based intrusion-detection methods," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 40, no. 5, pp. 516–524, 2010.

[119] S. Seng, J. Garcia-Alfaro, I. Gazeau, and L. Desmonts, "A stateful protocol-based detection engine combining behavior use cases and system specifications," *Internet Technology Letters*, p. e633, 2025.

[120] J. Shahid, R. Ahmad, A. K. Kiani, T. Ahmad, S. Saeed, and A. M. Almuhaideb, "Data protection and privacy of the internet of healthcare things (iohts)," *Applied Sciences*, vol. 12, no. 4, p. 1927, 2022.

[121] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "A survey on security threats and countermeasures in internet of medical things (iomt)," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 6, p. e4049, 2022.

[122] R. Baines, P. Hoogendoorn, S. Stevens, A. Chatterjee, L. Ashall-Payne, T. Andrews, and S. Leigh, "Navigating medical device certification: a qualitative exploration of barriers and enablers amongst innovators, notified bodies and other stakeholders," *Therapeutic Innovation & Regulatory Science*, vol. 57, no. 2, pp. 238–250, 2023.

[123] S. Mahmood, M. Gohar, O. A. Khashan, N. Alzahrani, A. Ghani, and F. Al-Turjman, "Securing edge devices in iot and 6g: A trust-based approach for resource-constrained environments," *IEEE Open Journal of the Communications Society*, 2025.

[124] K. Gupta, V. Mishra, and A. Makkar, "A global cybersecurity standardization framework for healthcare informatics," *IEEE Journal of Biomedical and Health Informatics*, 2024.

[125] A. N. Alsheavi, A. Hawbani, W. Othman, X. Wang, G. Qaid, L. Zhao, and M. A. Al-Qaness, "Iot authentication protocols: Challenges, and comparative analysis," *ACM Computing Surveys*, vol. 57, no. 5, pp. 1–43, 2025.

[126] P. Chatterjee, D. Das, S. Banerjee, U. Ghosh, A. B. Mpembele, and T. Rogers, "An approach towards the security management for sensitive medical data in the iomt ecosystem," in *Proceedings of the Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, 2023, pp. 400–405.

[127] M. M. Ozcelik, I. Kok, and S. Ozdemir, "A survey on internet of medical things (iomt): Enabling technologies, security and explainability issues, challenges, and future directions," *Expert Systems*, vol. 42, no. 5, p. e70010, 2025.

[128] N. Elsayed, L. Dzamesi, Z. ElSayed, and M. Ozer, "Extreme learning machine based system for ddos attacks detections on iomt devices," *arXiv preprint arXiv:2507.05132*, 2025.

[129] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "Ransomware detection and mitigation using software-defined networking: The case

of wannacry," *Computers & Electrical Engineering*, vol. 76, pp. 111–121, 2019.

[130] X. Zhang, M. M. Yadollahi, S. Dadkhah, H. Isah, D. P. Le, and A. A. Ghorbani, "Data breach: analysis, countermeasures and challenges," *International Journal of Information and Computer Security*, vol. 19, no. 3-4, pp. 402–442, 2022.

[131] H. Saeed, M. Naseer, A. Rasool, A. Alsirhani, F. Alserhani, G. N. Alwakid, and Y. Zhao, "A novel adaptive hybrid intrusion detection system with lightweight optimization for enhanced security in internet of medical things," *Scientific Reports*, 2025.

[132] G. Zachos, I. Essop, G. Mantas, K. Porfyrakis, J. C. Ribeiro, and J. Rodriguez, "An anomaly-based intrusion detection system for internet of medical things networks," *Electronics*, vol. 10, no. 21, p. 2562, 2021.

[133] G. Zachos, G. Mantas, K. Porfyrakis, and J. Rodriguez, "Implementing anomaly-based intrusion detection for resource-constrained devices in iomt networks," *Sensors*, vol. 25, no. 4, p. 1216, 2025.

[134] B. T. Hasan, A. M. A. Al-Sabaawi, and Z. J. Al-Araji, "Lightweight deep learning for iot-based medical diagnosis: A survey," *Mesopotamian Journal of Artificial Intelligence in Healthcare*, vol. 2025, pp. 244–259, 2025.

[135] A. M. Alwakeel, "Adaptive edge-fog healthcare networks: a novel framework for emergency response management," *Journal of Cloud Computing*, vol. 14, no. 1, p. 48, 2025.

[136] R. Nabha, A. Laouiti, and A. E. Samhat, "Internet of things-based healthcare systems: An overview of privacy-preserving mechanisms," *Applied Sciences*, vol. 15, no. 7, p. 3629, 2025.

[137] L. Alsbatin, B. M. Alrifai, F. Zawaideh, and T. A. Alawneh, "Advancing iomt security: Machine learning-based detection and classification of multi-protocol cyberattacks," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 16, no. 2, pp. 228–247, 2025.

[138] M. Boumaiz, M. E. Ghazi, A. Bouayad, Y. Balboul, and M. El Bekkali, "Energy-efficient strategies in wireless body area networks: A comprehensive survey," *IoT*, vol. 6, no. 3, p. 49, 2025.

[139] L. P. Siqueira, C. L. Batista, P. H. Lui, J. F. Kazienko, S. E. Quincozes, V. E. Quincozes, and S. Nomura, "A comprehensive survey on

intrusion detection systems for healthcare 5.0: Concepts, challenges, and practical applications," *Sensors*, vol. 25, no. 20, p. 6261, 2025.

[140] T. Tervoort, M. T. De Oliveira, W. Pieters, P. Van Gelder, S. D. Olabarriaga, and H. Marquering, "Solutions for mitigating cybersecurity risks caused by legacy software in medical devices: a scoping review," *IEEE access*, vol. 8, pp. 84 352–84 361, 2020.

[141] S. Mohammed and N. Malhotra, "Ethical and regulatory challenges in machine learning-based healthcare systems: A review of implementation barriers and future directions," *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, p. 100215, 2025.

[142] E. N. Chukwuani, O. R. Odunsi, and C. D. Ikemefuna, "Machine learning techniques for real-time malware classification and threat detection in distributed systems," 2025.

[143] S. B. Sharma and A. K. Bairwa, "Leveraging ai for intrusion detection in iot ecosystems: A comprehensive study," *IEEE Access*, 2025.

[144] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms," *Knowledge and Information Systems*, pp. 1–87, 2025.

[145] H. N. Fakhouri, B. Alhadidi, K. Omar, S. N. Makhadmeh, F. Hamad, and N. Z. Halalsheh, "Ai-driven solutions for social engineering attacks: Detection, prevention, and response," in *2024 2nd international conference on cyber resilience (ICCR)*, 2024, pp. 1–8.

[146] J. Sivakumar, N. R. Salman, F. R. Salman, H. R. Salimova, and E. Ghimire, "Ai-driven cyber threat detection: enhancing security through intelligent engineering systems," *Journal of Information Systems Engineering and Management*, vol. 10, no. 19, pp. 790–798, 2025.

[147] I. Mahmoudi, D. E. Boubiche, S. Athmani, H. Toral-Cruz, and F. I. Chan-Puc, "Toward generative ai-based intrusion detection systems for the internet of vehicles (iov)," *Future Internet*, vol. 17, no. 7, p. 310, 2025.

[148] G. Nagar, "Leveraging artificial intelligence to automate and enhance security operations: Balancing efficiency and human oversight," *Valley International Journal Digital Library*, pp. 78–94, 2018.

[149] K. Hasan, F. Hossain, A. Amin, Y. Sutradhar, I. J. Jeny, and S. Mahmud, "Enhancing proactive cyber defense: A theoretical framework for ai-driven predictive cyber threat intelligence," *Journal of Technologies Information and Communication*, vol. 5, no. 1, p. 33122, 2025.

[150] S. H. Almotiri, "Ai driven iomt security framework for advanced malware and ransomware detection in sdn," *Journal of Cloud Computing*, vol. 14, no. 1, p. 19, 2025.

[151] H. Ammar and A. Cherif, "Optimizing iomt security: Performance trade-offs between neural network architectural design, dimensionality reduction, and class imbalance handling," *IoT*, vol. 6, no. 4, p. 74, 2025.

[152] T. T. Nguyen, U. H. Tran, and H. N. Nguyen, "Adversarial attack and defense in ai-powered intrusion detection," *Journal of Computer Science and Cybernetics*, vol. 41, no. 4, pp. 387–402, 2025.

[153] A. Zentner, "From opacity to transparency: Advancing explainable ai through black-box, white-box, and glass-box models," 2025.

[154] A. A. Pise, S. Singh, K. Hemachandran, S. Gadilkar, Z. B. Esther, G. S. Pise, and J. Imuede, "Adapting to evolving cyber threat landscapes with dynamic security protocol management in large-scale iot sensor networks," *International Journal of Wireless & Ad Hoc Communication*, vol. 7, no. 2, 2023.

[155] Z. Wang, J. Ma, X. Wang, J. Hu, Z. Qin, and K. Ren, "Threats to training: A survey of poisoning attacks and defenses on machine learning systems," *ACM Computing Surveys*, vol. 55, no. 7, pp. 1–36, 2022.

[156] S. Jayousi, C. Barchielli, S. Guarducci, M. Alaimo, S. Caputo, P. Zoppi, and L. Mucchi, "From innovation to integration: bridging the gap between iomt technologies and real-world health management systems," *Sensors*, vol. 25, no. 21, p. 6660, 2025.

[157] A. K. Polinati, "Ai-powered anomaly detection in cybersecurity: Leveraging deep learning for intrusion prevention," *International Journal of Communication Networks and Information Security*, vol. 17, no. 3, pp. 301–323, 2025. [Online]. Available: https://orchid.org/0009-0005-0165-0675

[158] C. Janiesch, P. Zschech, and K. Heinrich, "Machine learning and deep learning," *Electronic markets*, vol. 31, no. 3, pp. 685–695, 2021.

[159] X. Yang, S. Zhang, J. Liu, Q. Gao, S. Dong, and C. Zhou, "Deep learning for smart fish farming: applications, opportunities and challenges," *Reviews in Aquaculture*, vol. 13, no. 1, pp. 66–90, 2021.

[160] R. Caruana and A. Niculescu-Mizil, "An empirical comparison of supervised learning algorithms," in *Proceedings of the 23rd international conference on Machine learning*, 2006, pp. 161–168.

[161] D. Pandey, K. Niwaria, and B. Chourasia, "Machine learning algorithms: a review," *Mach. Learn*, vol. 6, no. 2, 2019.

[162] A. J. Mohammed, M. H. Arif, and A. A. Ali, "A multilayer perceptron artificial neural network approach for improving the accuracy of intrusion detection systems," *IAES International Journal of Artificial Intelligence*, vol. 9, no. 4, p. 609, 2020.

[163] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A survey of cnn-based network intrusion detection," *Applied Sciences*, vol. 12, no. 16, p. 8162, 2022.

[164] S. M. Kasongo, "A deep learning technique for intrusion detection system using a recurrent neural networks based framework," *Computer Communications*, vol. 199, pp. 113–125, 2023.

[165] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (lstm)," *Journal of Big Data*, vol. 8, no. 1, 2021.

[166] F. S. Alrayes, M. Zakariah, S. U. Amin, Z. I. Khan, and M. Helal, "Intrusion detection in iot systems using denoising autoencoder," *IEEE Access*, 2024.

[167] M. Jamoos, A. M. Mora, M. AlKhanafseh, and O. Surakhi, "A new data-balancing approach based on generative adversarial network for network intrusion detection system," *Electronics*, vol. 12, no. 13, p. 2851, 2023.

[168] M. Sajid, K. R. Malik, A. Almogren, T. S. Malik, A. H. Khan, J. Tanveer, and A. U. Rehman, "Enhancing intrusion detection: a hybrid machine and deep learning approach," *Journal of Cloud Computing*, vol. 13, no. 1, p. 123, 2024.

[169] V. Z. Mohale and I. C. Obagbuwa, "A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity," *Frontiers in Artificial Intelligence*, vol. 8, p. 1526221, 2025.

[170] E. Obuse, E. D. Etim, I. A. Essien, E. Cadet, J. O. Ajayi, E. D. Erigha, and L. A. Babatunde, "Explainable ai for cyber threat intelligence and risk assessment," *Journal of Frontiers in Multidisciplinary Research*, vol. 1, no. 2, pp. 15–30, 2020.

[171] N. Khan, K. Ahmad, A. A. Tamimi, M. M. Alani, A. Bermak, and I. Khalil, "Explainable ai-based intrusion detection system for industry 5.0: An overview of the literature, associated challenges, the

existing solutions, and potential research directions," *arXiv preprint arXiv:2408.03335*, 2024.

[172] S. Ennaji, F. De Gaspari, D. Hitaj, A. Kbidi, and L. V. Mancini, "Adversarial challenges in network intrusion detection systems: Research insights and future prospects," *IEEE Access*, 2025.

[173] M. H. A. Rai, Y. Noor, M. Faisal, and M. F. Nawazish, "Adversarial robustness of deep learning-based intrusion detection systems against ai-powered cyber attacks," *Spectrum of Engineering Sciences*, pp. 899–922, 2025.

[174] K. Yu, K. Nguyen, and Y. Park, "Flexible and robust real-time intrusion detection systems to network dynamics," *IEEE Access*, vol. 10, pp. 98 959–98 969, 2022.

[175] T. A. Bablu and M. T. Rashid, "Edge computing and its impact on real-time data processing for iot-driven applications," *Journal of advanced computing systems*, vol. 5, no. 1, pp. 26–43, 2025.

[176] M. B. Musthafa, S. Huda, T. T. Nguyen, Y. Kodera, and Y. Nogami, "Optimized ensemble deep learning for real-time intrusion detection on resource-constrained raspberry pi devices," *IEEE Access*, 2025.

[177] M. A. Alam, A. R. Nabil, A. A. Mintoo, and A. Islam, "Real-time analytics in streaming big data: techniques and applications," *Journal of Science and Engineering Research*, vol. 1, no. 01, pp. 104–122, 2024.

[178] A. I. Zreikat, Z. AlArnaout, A. Abadleh, E. Elbasi, and N. Mostafa, "The integration of the internet of things (iot) applications into 5g networks: A review and analysis," *Computers*, vol. 14, no. 7, p. 250, 2025.

[179] U. Islam, H. Ullah, N. Khan, I. Ahmad, and K. Saleem, "Adaptive federated learning framework for privacy-preserving consumer-centric iomt: A novel secure data collaboration model," *IEEE Transactions on Consumer Electronics*, 2025.

[180] M. K. Quan, P. N. Pathirana, M. Wijayasundara, S. Setunge, D. C. Nguyen, C. G. Brinton, others, and H. V. Poor, "Federated learning for cyber physical systems: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2025.

[181] N. Khan, S. Nisar, M. A. Khan, Y. A. U. Rehman, F. Noor, and G. Barb, "Optimizing federated learning with aggregation strategies: A comprehensive survey," *IEEE Open Journal of the Computer Society*, 2025.

[182] T. Wang, J. Guo, B. Zhang, G. Yang, and D. Li, "Deploying ai on edge: Advancement and challenges in edge intelligence," *Mathematics*, vol. 13, no. 11, p. 1878, 2025.

[183] Y. Yuehong, Y. Zeng, X. Chen, and Y. Fan, "The internet of things in healthcare: An overview," *Journal of Industrial Information Integration*, vol. 1, pp. 3–13, 2016.

[184] G. Aceto, V. Persico, and A. Pescapé, "The role of information and communication technologies in healthcare: taxonomies, perspectives, and challenges," *Journal of Network and Computer Applications*, vol. 107, pp. 125–154, 2018.

[185] A. A. El-Saleh, A. M. Sheikh, M. A. Albreem, and M. S. Honnurvali, "The internet of medical things (iomt): opportunities and challenges," *Wireless networks*, vol. 31, no. 1, pp. 327–344, 2025.

[186] W. Villegas-Ch, J. Govea, and A. Jaramillo-Alcazar, "Tamper detection in industrial sensors: an approach based on anomaly detection," *Sensors*, vol. 23, no. 21, p. 8908, 2023.

[187] U. Tariq, I. Ullah, M. Yousuf Uddin, and S. J. Kwon, "An effective self-configurable ransomware prevention technique for iomt," *Sensors*, vol. 22, no. 21, p. 8516, 2022.

[188] Y. Cao, L. Zhang, X. Zhao, K. Jin, and Z. Chen, "An intrusion detection method for industrial control system based on machine learning," *Information*, vol. 13, no. 7, p. 322, 2022.

[189] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "A systematic review of data protection and privacy preservation schemes for smart grid communications," *Sustainable cities and society*, vol. 38, pp. 806–835, 2018.

[190] F. Tsimpourlas, L. Papadopoulos, A. Bartsokas, and D. Soudris, "A design space exploration framework for convolutional neural networks implemented on edge devices," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 11, pp. 2212–2221, 2018.

[191] Y. Zhang, Y. Liu, X. Guo, Z. Liu, X. Zhang, and K. Liang, "A bilstm-based ddos attack detection method for edge computing," *Energies*, vol. 15, no. 21, p. 7882, 2022.

[192] W. Feng, S. Tang, S. Wang, Y. He, D. Chen, Q. Yang, and S. Fu, "Characterizing perception deep learning algorithms and applications for vehicular edge computing," *Algorithms*, vol. 18, no. 1, p. 31, 2025.

[193] J. Dom.nech, O. Le.n, M. Siddiqui, and J. Pegueroles, "Evaluating and enhancing intrusion detection systems in iomt: The importance of domain-specific datasets," *Internet of Things*, vol. 32, p. 101631, 2025.

[194] S. Lipsa, R. Dash, and N. Ivković, "An interpretable dimensional reduction technique with an explainable model for detecting attacks in internet of medical things devices," *Scientific Reports*, vol. 15, p. 8718, 2025.

[195] N. Faruqui, M. Abu Yousuf, Whaiduzzaman, A. Azad, S. Alyami, P. Liò, M. Kabir, and M. Moni, "Safetymed: A novel iomt intrusion detection system using cnn-lstm hybridization," *Electronics*, vol. 12, no. 15, p. 3541, 2023.

[196] J. Shaikh, C. Wang, M. Sima, M. Arshad, M. Owais, D. Hassan, R. Alkanhel, and M. Muthanna, "A deep reinforcement learning-based robust intrusion detection system for securing iomt healthcare networks," *Frontiers in Medicine*, vol. 12, p. 1524286, 2025.

[197] N. Sharma and P. Shambharkar, "Multi-attention deepcrnn: An efficient and explainable intrusion detection framework for internet of medical things environments," *Knowledge and Information Systems*, vol. 67, pp. 5783–5849, 2025.

[198] G. Akar, S. Sahmoud, M. Onat, Ç. Cavusoglu, and E. Malondo, "L2d2: A novel lstm model for multi-class intrusion detection systems in the era of iomt," *IEEE Access*, vol. 13, pp. 7002–7013, 2025.

[199] A. Jony and A. Arnob, "A long short-term memory based approach for detecting cyber attacks in iot using cic-iot-2023 dataset," *Journal of Edge Computing*, vol. 3, pp. 28–42, 2024.

[200] S. Khanday, H. Fatima, and N. Rakesh, "A novel data preprocessing model for lightweight sensory iot intrusion detection," *International Journal of Mathematical, Engineering and Management Sciences*, vol. 9, pp. 188–204, 2024.

[201] S. Tseng, Y. Wang, and Y. Wang, "Multi-class intrusion detection based on transformer for iot networks using cic-iot-2023 dataset," *Future Internet*, vol. 16, no. 7, p. 284, 2024.

[202] M. Alsharaiah, M. Almaiah, R. Shehab, M. Obeidat, F. El-Qirem, and T. Aldhyani, "An explainable ai-driven transformer model for spoofing attack detection in internet of medical things (iomt) networks," *Discover Applied Sciences*, vol. 7, p. 488, 2025.

[203] H. Naeem, A. Alsirhani, F. Alserhani, F. Ullah, and O. Krejcar, "Augmenting internet of medical things security: Deep ensemble integra-

tion and methodological fusion," *Computer Modeling in Engineering & Sciences*, vol. 141, pp. 2185–2223, 2024.

[204] H. Sayegh, W. Dong, and A. Al-Madani, "Enhanced intrusion detection with lstm-based model, feature selection, and smote for imbalanced data," *Applied Sciences*, vol. 14, no. 2, p. 479, 2024.

[205] A. Gueriani, H. Kheddar, and A. Mazari, "Enhancing iot security with cnn and lstm-based intrusion detection systems," in *Proceedings of the 2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, El Oued, Algeria, 2024, pp. 1–7.

[206] R. Anwar, M. Abrar, A. Salam, and F. Ullah, "Federated learning with lstm for intrusion detection in iot-based wireless sensor networks: A multi-dataset analysis," *PeerJ Computer Science*, vol. 11, p. e2751, 2025.

[207] S. Abbas, A. Al Hejaili, G. Sampedro, M. Abisado, A. Almadhor, T. Shahzad, and K. Ouahada, "A novel federated edge learning approach for detecting cyberattacks in iot infrastructures," *IEEE Access*, vol. 11, pp. 112 189–112 198, 2023.

[208] N. Saran and N. Kesswani, "Intrusion detection system for internet of medical things using gru with attention mechanism-based hybrid deep learning technique," *Jordanian Journal of Computers and Information Technology*, vol. 11, no. 2, pp. 136–150, 2024.

[209] S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi, and A. A. Ghorbani, "Ciciomt2024: A benchmark dataset for multi-protocol security assessment in iomt," *Internet of Things*, vol. 28, p. 101351, 2024.

[210] M. Mohsin and A. I. Jony, "A comparative analysis of medical iot device attacks using machine learning models," *Malaysian Journal of Science and Advanced Technology*, pp. 429–439, 2024.

[211] N. S. Tany, S. Suresh, D. N. Sinha, C. Shinde, C. Stolojescu-Crisan, and R. Khondoker, "Cybersecurity comparison of brain-based automotive electrical and electronic architectures," *Information*, vol. 13, no. 11, p. 518, 2022.

[212] H. Benahmed, M. Mhamedi, M. Merzoug, M. Hadjila, A. Bekkouche, A. Etchiali, and S. Mahmoudi, "Hbild-ids: An efficient hybrid bilstm-dnn model for real-time intrusion detection in iomt networks," *Information*, vol. 16, no. 8, p. 669, 2025.

Résumé

L'essor de l'Internet des objets médicaux (IoMT) représente un défi majeur et croissant pour la cybersécurité. Les systèmes de détection d'intrusion (IDS) traditionnels sont manifestement inadaptés à ce domaine, incapables de gérer efficacement les caractéristiques uniques du trafic réseau IoMT, notamment sa forte dimensionnalité, ses dépendances temporelles et son hétérogénéité inhérente. Cette recherche comble cette lacune en introduisant un nouveau cadre hybride d'apprentissage profond, basé sur l'intégration synergique d'un réseau de mémoire bidirectionnelle à long terme (BiLSTM) et d'un réseau neuronal profond (DNN). Cette architecture innovante est soigneusement conçue pour surmonter les limites des modèles existants en capturant simultanément les séquences temporelles et les caractéristiques spatiales intégrées au trafic réseau IoMT. L'un des principaux apports de ces travaux réside dans la transparence intrinsèque du cadre. Il dépasse l'opacité des modèles traditionnels de type ń boîte noire ż en intégrant les principes de l'IA explicable (XAI) et en s'appuyant sur les explications additives de SHapley (SHAP). Cette intégration fournit des justifications interprétables par l'humain pour chaque alerte de sécurité, révélant les caractéristiques et les schémas de données spécifiques qui sous-tendent les prédictions du modèle. Cela favorise non seulement la confiance et garantit la responsabilisation, mais facilite également une analyse humaine efficace, permettant au personnel de sécurité de valider les alertes et d'intervenir en toute confiance sans compromettre les soins aux patients. Une évaluation rigoureuse sur le jeu de données de référence complet CICIoMT2024 valide les performances exceptionnelles du cadre, démontrant une grande précision dans la distinction entre 18 types d'attaques distincts et le trafic normal. En combinant harmonieusement des capacités de détection avancées avec une transparence opérationnelle essentielle, cette recherche marque une avancée significative en matière de cybersécurité et d'IA fiable, apportant une solution robuste et vérifiable, essentielle à la protection des données de santé sensibles et au fonctionnement résilient des services médicaux critiques.

Mots clés : e-Santé, Internet des objets médicaux (IoMT), Système de détection d'intrusion (IDS), BiLSTM, DNN, Black-Box, Intelligence artificielle explicative (XAI), SHAP.

Abstract

The burgeoning landscape of the Internet of Medical Things (IoMT) presents a critical and escalating challenge to cybersecurity. Traditional Intrusion Detection Systems (IDS) are demonstrably inadequate for this domain, as they are unable to effectively manage the unique characteristics of IoMT network traffic, including its high dimensionality, temporal dependencies, and inherent heterogeneity. This research addresses this deficiency by introducing a novel hybrid deep learning framework, built upon a synergistic integration of a Bidirectional Long Short-Term Memory (BiLSTM) network with a Deep Neural Network (DNN).This innovative architecture is meticulously designed to overcome the limitations of existing models by concurrently capturing both the temporal sequences and spatial features embedded within IoMT network traffic. A core contribution of this work is the framework's intrinsic transparency. It moves beyond the opaqueness of traditional "black box" models by incorporating Explainable AI (XAI) principles, leveraging SHapley Additive exPlanations (SHAP). This integration provides human-interpretable justifications for every security alert, revealing the specific features and data patterns that drive the model's predictions. This not only cultivates trust and ensures accountability but also facilitates an effective human-in-the-loop analysis, empowering security personnel to confidently validate alerts and respond without compromising patient care. Rigorous evaluation on the comprehensive CICIoMT2024 benchmark dataset validates the framework's exceptional performance, demonstrating high accuracy in discriminating between 18 distinct attack types and normal traffic. By seamlessly combining advanced detection capabilities with essential operational transparency, this research marks a significant advancement in both cybersecurity and trustworthy AI, contributing a robust and auditable solution vital for safeguarding sensitive healthcare data and ensuring the resilient operation of critical medical services.

Keywords: e-Healthcare, Internet of Medical Things (IoMT), Intrusion Detection System (IDS), BiLSTM, DNN, Black-Box, Explainability Artificial Intelligence (XAI), SHAP.

ملخص

يُمثل المشهد المزدهر لإنترنت الأشياء الطبية (IoMT) تحديًا حاسمًا ومتصاعدًا للأمن السيبراني. ومن الواضح أن أنظمة كشف التسلل (IDS) التقليدية غير كافية لهذا المجال، لأنها غير قادرة على إدارة الخصائص الفريدة لحركة مرور شبكة إنترنت الأشياء الطبية (IoMT) بفعالية، بما في ذلك أبعادها العالية، وتبعياتها الزمنية، وتباينها المتأصل. يعالج هذا البحث هذا النقص من خلال تقديم إطار عمل هجين جديد للتعلم العميق، مبني على تكامل تآزري لشبكة ذاكرة طويلة وقصيرة المدى ثنائية الاتجاه (BiLSTM) مع شبكة عصبية عميقة (DNN). وقد صُممت هذه البنية المبتكرة بدقة للتغلب على قيود النماذج الحالية من خلال التقاط كل من التسلسلات الزمنية والميزات المكانية المضمنة في حركة مرور شبكة إنترنت الأشياء الطبية (IoMT) في وقت واحد. ومن المساهمات الأساسية لهذا العمل الشفافية الجوهرية للإطار. يتجاوز هذا النموذج غموض نماذج "الصندوق الأسود" التقليدية من خلال دمج مبادئ الذكاء الاصطناعي القابل للتفسير (XAI)، والاستفادة من تفسيرات SHapley الإضافية (SHAP). يوفر هذا التكامل مبررات قابلة للتفسير البشري لكل تنبيه أمني، كاشفًا عن السمات وأنماط البيانات المحددة التي تُحرك تنبؤات النموذج. هذا لا يعزز الثقة ويضمن المساءلة فحسب، بل يُسهّل أيضًا إجراء تحليل فعال بمشاركة بشرية، مما يُمكّن موظفي الأمن من التحقق من صحة التنبيهات والاستجابة لها بثقة دون المساس برعاية المرضى. يُثبت التقييم الدقيق لمجموعة بيانات CICIoMT2024 الشاملة الأداء الاستثنائي للإطار، مُظهرًا دقة عالية في التمييز بين 18 نوعًا مختلفًا من الهجمات وحركة المرور العادية. من خلال الجمع بسلاسة بين قدرات الكشف المتقدمة والشفافية التشغيلية الأساسية، يُمثل هذا البحث تقدمًا كبيرًا في كل من الأمن السيبراني والذكاء الاصطناعي الموثوق، مما يُسهم في إيجاد حل قوي وقابل للتدقيق، وهو أمر حيوي لحماية بيانات الرعاية الصحية الحساسة وضمان التشغيل المرن للخدمات الطبية الحيوية.

الكلمات المفتاحية: الرعاية الصحية الإلكترونية، إنترنت الأشياء الطبية (IoMT)، نظام كشف التطفل (IDS)، BiLSTM، DNN، الصندوق الأسود، الذكاء الاصطناعي القابل للتفسير (XAI)، SHAP.