

Recent Advances in Artificial Intelligence-Driven Internet of Medical Things Networking

Giovanni Stanco, Stefania Zinno[†], Alessio Botta, Giorgio Ventre
DIETI, DISS[†], University of Napoli Federico II, Naples, Italy
{giovanni.stanco, stefania.zinno, alessio.botta, giorgio.ventre}@unina.it,

Abstract—The emergence of the Internet of Medical Things (IoMT) is transforming modern biomedical engineering. By connecting wearable sensors and remote monitoring systems, IoMT enables novel approaches for accurate diagnosis and therapy. The deployment of IoMT devices connected by wireless networks has led to the generation of large amounts of data, which require Artificial Intelligence (AI) techniques to be properly processed. AI plays a vital role in optimizing the communication and exchange of the gathered data via wireless networks, improving the network capabilities and mitigating security risks. The introduction of AI-based techniques, however, must face the inherent limitations of IoMT scenarios, in which constrained devices exploit vulnerable wireless networks to transmit highly sensitive data. Our work provides a review of the current state-of-the-art in IoMT, detailing the most adopted network topologies and the multiple ways in which AI is leveraged for optimizing resource management and overcoming security vulnerabilities.

Index Terms—IoMT, wireless networks, Artificial Intelligence

I. INTRODUCTION

The convergence of the Internet of Things (IoT) and healthcare has given rise to the Internet of Medical Things (IoMT), a transformative paradigm reshaping modern biomedical engineering. By interconnecting wearable sensors, implantable devices, and remote monitoring systems, IoMT offers new remarkable advantages in healthcare, including real-time patient monitoring, early disease detection, and personalized therapeutic plans [1].

The deployment and success of IoMT solutions led to the generation of large amounts of data from patients and medical procedures, which can provide useful insights to healthcare staff and decision-makers when properly collected, stored, and processed.

The integration of Artificial Intelligence (AI) and Machine Learning (ML) within the biomedical domain has catalyzed this revolution. AI algorithms are able to process vast amounts of heterogeneous physiological data, enabling predictive analytics in clinical decision support systems, significantly improving patient outcomes [2].

Despite these undeniable benefits, the widespread adoption of IoMT is heavily constrained by the vulnerabilities inherent in wireless communication protocols. IoMT devices typically rely on wireless networks, such as Bluetooth Low Energy (BLE), ZigBee, and Wi-Fi, to transmit sensitive personal health data. Wireless channels are notoriously susceptible to cyber-threats, such as eavesdropping, data tampering, Man-in-the-Middle (MitM) attacks, and Denial-of-Service (DoS). In a medical context, a breach in communication security does not

merely imply a loss of privacy, but it also poses a threat to patient life, for instance through the malicious manipulation of life-critical devices (e.g., pacemakers or insulin pumps) [3].

To introduce new functionalities and mitigate critical risks, AI has emerged as a powerful tool to enhance the capabilities and the security of wireless communications in IoMT. AI-driven mechanisms offer novel solutions to meet new goals from possible use cases. However, deploying AI within wireless IoMT ecosystems introduces important challenges. IoMT nodes are fundamentally resource-constrained devices with strict limitations on computational power, memory, and energy consumption. Running complex, resource-intensive AI models directly at the network edge represents a bottleneck. Furthermore, ensuring the privacy of the data used to train these models and defending the AI systems themselves from adversarial attacks remain critical open research questions [4]. This paper provides a comprehensive overview of the current state-of-the-art in IoMT and its prevalent network topologies. We investigate how IoT is being leveraged to enhance the capabilities of the most adopted networks, optimizing resource management and overcoming security vulnerabilities, with special focus on healthcare applications.

The remainder of this paper is organized as follows. Section II details the current status of IoMT, highlighting its benefits in healthcare systems and the challenges threatening its successful deployment. Section III reviews the most common network technologies for IoMT, while Section IV summarizes the most recent AI-based advancements proposed for the considered networks. Section V concludes our work.

II. CURRENT STATUS OF IoMT

A. *IoT in Biomedical Applications*

IoMT devices and systems help to improve the quality of healthcare services, providing care to remote patients and automating routine tasks. Their adoption also helps patients with chronic symptoms, reducing the number of in-person visits, and supports constant and accurate care in diagnostics, surgery, and rehabilitation [5].

By wearing connected wearable devices, it is possible to gather vital parameters from patients even outside healthcare facilities to suggest personalized treatments and reactive actions. The collection of health data from a network of body-worn sensors can enrich the observations that human operators could gather in clinical environments, enabling personalized care, improvements in diagnostics, and cost reduction [6].

Another efficient approach to use IoMT is through asset tracking and equipment management. Implementing this approach, it is easier to handle inventory, apply predictive maintenance, and monitor storage conditions for medications and other supplies [7].

B. IoMT in Modern Healthcare

The market size of IoMT was USD 77.49 billion in 2025, with predictions to grow thanks to the increasing adoption of remote patient monitoring solutions and the launch of new products [8]. The development of such an approach in recent years was also triggered by the COVID-19 pandemic, which facilitated digital transformation, expanding new applications and opportunities, and led to a significant increase in IoMT device demand. The situation of the last year boosted the advancements in telemedicine and introduced a new approach to health management, reducing the burden on overworked healthcare staff and medical institutions.

C. Security Threats

The advantages of better healthcare and remote patient monitoring are unfortunately counterbalanced by the increasing risks related to the interconnection of critical devices in various networks [9]. Constant effort is being put in to identify security threats and reduce the consequent risks. This worry is wisely motivated, since healthcare data cover sensitive information including Electronic Health Records (EHRs), diagnostic images, prescription histories, and billing records. The risks connected to the hacking of healthcare data are due to their high value on the black market, on the legacy platforms still operated by healthcare organizations, and the unaffordable critical downtime that forces healthcare professionals to succumb to the demands of cybercriminals [10]. The security threats and the risks of privacy compromise represent one of the main obstacles to the successful and widespread deployment of IoT systems in general, and of IoMT systems in particular, due to the sensitive data handled in such scenarios.

Current security threats range from data exposure due to Cloud misconfigurations to social engineering attacks, exploiting human vulnerabilities to gain access to sensitive data. Cyberthreats that are specifically related to IoMT devices include tampering with life-critical devices, e.g., on-person sensors and actuators. Vital sensors and actuators such as defibrillators, insulin pumps, and pacemakers are often connected via a wireless communication network to enable remote monitoring capabilities. This series of sensors and monitoring units represents a potential entry point into large hospital networks for the theft of sensitive EHRs or for launching ransomware attacks capable of holding entire, often mission-critical, systems hostage [11]. The main causes at the basis of such attacks are limited hardware resources to run sophisticated security protocols and encryption algorithms, outdated firmware, and unauthorized network access.

III. CURRENT IOMT NETWORK TECHNOLOGIES

IoT applications require different networking technologies that can meet their needs [12]. Similarly, medical appli-

cations cover a large variety of purposes, from low-power body implants to hospital imaging systems. IoMT solutions rely on a multi-tiered communication architecture for data collection, transmission, and analysis. Table I summarizes the most popular networks, classifying them according to two important features: the covered range and the power consumption, two fundamental factors in IoT communications. Table I also reports the most common use cases for every network technology, while further details of each network technology are reported in the following.

A. Bluetooth Low Energy

BLE is a wireless technology suitable for the communication of consumer and clinical wearable health monitors. BLE offers an operating range of up to five meters, but with reduced power consumption and a lower data rate than legacy Bluetooth [13], [14]. BLE operates in the unlicensed 2.4 GHz Industrial Scientific Medical (ISM) band and transmits across 40 RF channels: 37 channels are dedicated to data transfer, while 3 are reserved for device broadcasting and connection setup [13]. Frequency Hopping Spread Spectrum is used for switching from one channel to another. BLE devices can communicate in broadcasting mode, in which a primary broadcaster device sends advertising packets and manages connections to peripheral devices, or communication mode. Multiple topology options are available for multiple communication needs, including point-to-point, broadcast, and mesh. BLE makes use of three security keys: the initial Temporary Key (TK), the Short Term Key (STK), and the Long Term Key (LTK) [15]. During the initial connection, the pairing process involves the exchange of security features and capabilities, while the keys for future connections are saved during the bonding phase, protecting against malicious eavesdroppers and other basic attacks. The pairing process can be performed in three distinct approaches: Just Works, in which no device authentication is needed; Passkey, requiring a 6-digit passkey; and Out of Band, in which the devices share the TK by using other technologies. A popular approach for extra security is the combination of link-layer encryption and application-layer encryption [16].

B. IEEE 802.15.6

IEEE 802.15.6 is specifically designed for Wireless Body Area Networks (WBANs) operating on, around, or inside the human body with the goal of continuously collecting vital parameters from patients and forwarding them to a remote monitoring station for diagnostics and further services. IEEE 802.15.6 offers low-power, short-range communication, taking into account human tissue signal absorption and strict specific absorption rate thermal safety for reliable transmission around a human body. The employed frequency bands are ISM bands and safe frequency bands approved by medical and regulatory authorities. 802.15.6 defines three PHY layers (Narrowband, Ultra Wideband, and Human Body Communications) for different application requirements, and a Medium Access Control (MAC) layer for channel access [17]. Time resources on

TABLE I
OVERVIEW OF THE MAIN WIRELESS COMMUNICATION TECHNOLOGIES EMPLOYED IN IoMT ENVIRONMENTS.

<i>Network</i>	<i>Range</i>	<i>Power consumption</i>	<i>Use case</i>
BLE	Short	Low	Wearable sensors
IEEE 802.15.6	Ultra-Short	Low	In-body implants, body-surface sensors
Wi-Fi	Medium	Medium/High	bedside monitors, DICOM imaging, clinical workstations
ZigBee	Short	Low	Asset tracking, environmental sensors
LoRaWAN	Long	Low	Remote patient monitoring
NB-IoT	Long	Low	Remote patient monitoring
5G	Long	Medium	Ambulances, real-time telesurgery

the channel are divided into superframes bounded by equal-length beacons. Three security levels are available: unsecured communication, authentication only, and authentication and encryption.

C. Wi-Fi

IEEE 802.11 serves, in healthcare scenarios, as the main pillar in the exchange of clinical data such as uncompressed bulky diagnostic files. Wi-Fi is largely used for providing Internet access to multiple devices hosted in a local network [18]. Wi-Fi standards have evolved over time, with most recent standards supporting hundreds of Mbps of throughput, at the expense of high power consumption. Because of its popularity and the widespread deployment of its access points, Wi-Fi has been widely proposed for monitoring devices in IoMT.

D. ZigBee

ZigBee plays a specialized role for asset and equipment tracking and for environmental monitoring in medical environments, but it is not widely adopted for consumer wearables as no commercial smartphones include native ZigBee chips. Defined by the ZigBee Alliance [19], the ZigBee standard is characterized by limited data rates, low complexity, and reduced energy consumption. The MAC and physical layers are based on the 802.15.4 standard, while the application and network layers are defined by the ZigBee Alliance, as well as the frame formats for transporting data. Operating within unlicensed ISM bands, ZigBee networks can support up to 65,000 devices [20]. ZigBee supports varying data rates, ranging from 20 to 250 kbps, and accommodates multiple topologies: star, tree, and mesh. Exploiting a mesh topology, the network possesses self-healing capabilities, rerouting data through neighboring nodes. ZigBee network devices can fulfill three distinct roles: Coordinator, Router, and End Devices. The network layer manages the secure transmission of frames, adding a header to a network layer protocol data unit when security is required. Upper layers establish the required security level, configuring the appropriate frame counters and cryptographic keys and deciding whether to encrypt the payload. Three distinct cryptographic keys are employed to ensure secure communication: Master, Link, and Network keys. To provide cryptography, ZigBee exploits Counter mode with Cipher-block chaining message authentication code (CCM*) of AES-128.

E. LoRaWAN

LoRaWAN is the ideal solution for wide-area hospital asset tracking and for intermittent telemetry transmission, thanks to its low power and low latency characteristics [21]. LoRaWAN is a Low Power Wide Area Network (LPWAN) technology employing the physical layer standardized by the LoRa Alliance, spreading a narrowband signal over a wider bandwidth to provide orthogonal separation between signals [22]. LoRaWAN, with its network architecture and communication protocol, supports scalable private or public wireless networks, enabling bidirectional communication between the end device and the gateway [23]. Operating at the unlicensed Sub-GHz ISM radio bands, LoRaWAN devices must comply with duty-cycling rules to access the channel [24]. LoRaWAN relies on a long-range star topology, where end devices broadcast messages to all in-range gateways via a single LoRa hop. These gateways then forward the messages to a central core network using standard IP backhaul connections. Two approaches are available for activating an end device before communicating with the central core network: communicating the pre-configured session keys or sending a join request message for negotiating the cryptographic material. LoRaWAN employs multiple keys for the encryption of messages and for verifying their integrity. Frame counters for avoiding the replay of both downlink and uplink messages are also adopted.

F. NB-IoT

Narrowband Internet of Things (NB-IoT), operating on the licensed cellular network infrastructure, offers carrier-grade security and higher reliability for Remote Patient Monitoring and the transmission of vital parameters back to the hospital. It is particularly suitable for handling a massive number of connected devices that transmit limited amounts of data, and its most recent features extend its applicability to wearables and tracking services [25]. NB-IoT is based on a limited set of the Long Term Evolution (LTE) functionalities, focusing on enhancing spectrum efficiency and scalability, and on reducing power consumption. NB-IoT flexibly exploits distinct sections of the available spectrum on the 700, 800, and 900 MHz bands. NB-IoT can be deployed within existing LTE networks by reusing a small fraction of the available spectrum. NB-IoT prolongs the lifetime of the battery-operated nodes by using very aggressive sleep algorithms and by reducing their transmit power through Power Saving Mode (PSM) and

extended Discontinuous Reception (eDRX) [26]. The NB-IoT architecture consists of User equipments (UEs) transmitting data; base stations (eNodeB); Cloud resources for storing data and performing data analysis; and finally application servers developed by various companies. Exploiting licensed spectrum bands, NB-IoT communications avoid duty cycle restrictions or interference, providing a higher Quality of Service (QoS) than other LPWANs. Confidentiality is provided by the cryptographic algorithms ATR-128 CTR mode or SNOW 3G, while frequency hopping techniques provide data availability.

G. 5G

5G, proposed in 3rd Generation Partnership Project (3GPP) Release 15 as the standard for the next generation of mobile communications [27], supports critical IoMT applications, including robotic telesurgery and AI-assisted diagnostics, that require strict QoS guarantees. Pillars to the use cases enabled by 5G are high data rates, low latency, the management of a large number of connected devices, and rigorous security mechanisms [28]. To satisfy these demands, high spectral efficiency, dense network deployment, and effective coordination have to be carefully implemented [29]. 5G leverages mm-wave frequencies to offer wider bandwidth allocations and higher data rates. However, high propagation losses at these frequencies require a dense deployment of antennas to provide coverage. To meet the performance and costs required specifically for IoT applications, 5G Reduced Capability (RedCap) was introduced [30]. This new technology, based on the 5G standalone architecture, provides higher data rates than mMTC, reduced latency than LTE, and reduced power consumption for battery-operated devices. Paramount to 5G is the principle of security by design, with rigorous protections implemented across both the UE-to-base-station communication and the Radio Access Network (RAN)-to-core network link. Advanced network authentication, key management procedures, and monitoring systems such as firewalls and Intrusion Detection Systems (IDSs) are therefore required [31].

IV. AI-DRIVEN ENHANCEMENTS IN IOMT NETWORKING

The integration of AI and ML techniques in the biomedical field has already provided support in informed diagnostics and data-driven decisions. One of the most common uses is the predictive analysis based on data and symptom observation [32], [33]. Limitations to this approach include the need of vast and accurate datasets for the training phase and the high cost of computing infrastructures able to support advanced AI techniques [34].

ML has also been introduced in advanced security methods for IoT systems, for distinguishing normal from abnormal behaviour, based on the observed interaction in an IoT system. Furthermore, ML methods can predict future attacks stemming from existing ones, increasing the defensive capabilities of an IoT system [35].

This section explores the integration of AI within IoMT networks, illustrating how AI-driven enhancements can propel

the efficiency, scalability, and reliability of next-generation healthcare systems.

1) *Localization*: In indoor environments prone to signal occlusion and interference, using a neural network-based classification improves the performance of a localization system based on BLE devices [36]. Tree-based and ensemble ML models applied to BLE networks have been proven to have better performance in localization systems based on Received Signal Strength Indication (RSSI) readings [37]. Localization, based on the use of fingerprinting and neural networks, enables the adoption of a dynamic interface for BLE networks that varies according to the target device, simplifying device management [38]. Multiple ML algorithms have also been compared for localization based on 5G RSSI values, with ensemble Least-Squares Boosting (LSBoost) showing the best results [39]. AI-based localization has been introduced in ZigBee as well: real fingerprinting data based on the RSSI values have been demonstrated to be the most reliable source for accurate localization [40].

2) *Communications*: To mitigate the severe levels of interference that could be triggered in dense deployments, ML algorithms have been leveraged for developing a propagation model for LoRaWAN [41]. For a correct design of the propagation model, the ML model should be carefully selected according to the dataset size, the computational power, and the specific problem requirements. AI-based interference management has also been proposed for 5G systems to handle both intentional and unintentional interference, encompassing all phases from detection to mitigation [42]. These methods are not limited exclusively to IoT networks, but extend across the full spectrum of 5G use cases. AI enables also adaptive routing algorithms able to make data-driven decisions. Techniques at the basis of such routing algorithms for 802.15.6 can be supervised, unsupervised, or adopt Deep Learning (DL) or Reinforcement Learning (RL) [43].

3) *Security*: As previously stated, privacy is a strict requirement for IoMT systems. An AI framework is proposed specifically for 5G-based IoT systems, handling both privacy preservation and trust management, allowing only authorized devices to communicate within the network [44]. Fundamental for security and privacy, cryptographic keys must be carefully managed. Changing keys dynamically is a promising solution, but it requires decision-making capabilities. RL has been proposed as an approach for key rotation in a ZigBee network. This advancement in key management enables ZigBee networks to be better protected against cybersecurity attacks, reducing intrusion detection rates and response times [45]. Another scenario in which AI can play a pivotal role is Intrusion Detection. For example, gathering Wi-Fi signals, preprocessing them, and applying a ML pipeline is a feasible way to design and develop an IDS, preventing unauthorized users from compromising legitimate IoMT systems [46], [47].

4) *Energy consumption*: The optimization of energy consumption has been a relevant topic for NB-IoT to achieve multi-year operation for an end device on a single battery. Packet transmission can be optimized to improve the energy

efficiency of NB-IoT end devices, in particular to counterbalance the effects of interference, network congestion, and repeated transmissions. To this end, AI-based algorithms adjust transmission intervals through real-time monitoring [48] and estimate energy consumption for enabling energy-aware device management [49]. Another approach for optimal power management in NB-IoT involves RL, in particular the Soft Actor-Critic algorithm [50]. RL approaches have furthermore been proposed for device scheduling and resource allocations for uplink transmissions, keeping the transmission delay in an acceptable range without prior training [51].

Resource optimization and power consumption in LoRaWAN could also benefit from the adoption of ML, in order to adapt to evolving environmental and network conditions [52].

Electronic components for 802.15.6 can exploit AI to reduce their consumption: in particular, DL can reduce the computation process of a transceiver, improving its performance and therefore reducing its consumption, and can support the recovery of timing information for synchronization purposes [53].

Discussion

Our review and analysis show how AI has been integrated so far in networks suitable for IoMT systems to enhance their functionalities, in particular focusing on four critical operational domains: localization, communication, security, and energy consumption. Each of these domains represents a fundamental performance metric for the overall efficacy and reliability of IoMT systems.

Regarding localization, accurately estimating the spatial positions of medical assets and personnel optimizes resource management within clinical environments. More critically, patient localization enhances physical safety, enables continuous monitoring, and supports automated guidance during rehabilitation protocols.

In rapidly evolving IoMT ecosystems, dense deployment and the mitigation of signal interference represent two requirements to maintaining high service quality. High device density within constrained clinical settings demands robust coexistence mechanisms, whereas interference can disrupt critical data transmissions and compromise the safety and reliability of the overall healthcare infrastructure.

Security remains fundamental due to the highly sensitive data transmitted and processed across IoMT systems. Ensuring data confidentiality requires rigorous cryptographic key management, while unauthorized entities must be efficiently detected and prevented from gaining access to patient records.

Energy consumption represents another important design constraint. Enabling low-power devices to operate on long-life batteries without periodic manual maintenance reduces operational overhead for healthcare organizations and promotes long-term sustainability across IoMT deployments.

Ultimately, optimizing these core domains is vital for advancing next-generation IoMT networks. Our review demonstrates how AI-driven techniques can be leveraged to establish more efficient, resilient, and trustworthy IoMT systems.

V. CONCLUSIONS

This work has presented a comprehensive review of recent AI-driven advancements applicable to wireless IoT networks within the biomedical sector. While AI has been successfully deployed in healthcare primarily for medical data management and predictive analytics, this review highlights its role in optimizing data transmission and network infrastructures. Specifically, current AI applications target four main operational domains: localization, communication, security, and energy efficiency. Optimizing these domains through intelligent mechanisms is essential for the successful, reliable, and scalable deployment of next-generation IoMT systems.

REFERENCES

- [1] V. K. Venkatesan, P. F. Katina, and J. Zhao, Eds., *Convergence of Internet of Medical Things (IoMT) and Generative AI*. Hershey, PA: IGI Global, 2025.
- [2] J. He, S. L. Baxter, J. Xu, J. Xu, X. Zhou, and K. Zhang, "The practical implementation of Artificial Intelligence technologies in medicine," *Nature Medicine*, vol. 25, no. 1, pp. 30–36, 2019. [Online]. Available: <https://doi.org/10.1038/s41591-018-0307-0>
- [3] S. A. Wagan, J. Koo, I. F. Siddiqui, M. Attique, D. R. Shin, and N. M. F. Qureshi, "Internet of Medical Things and trending converged technologies: A comprehensive review on real-time applications," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, Part B, pp. 9228–9251, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1319157822003263>
- [4] M. Pawlicki, A. Pawlicka, R. Kozik, and M. Choraś, "A meta-survey of adversarial attacks against artificial intelligence algorithms, including diffusion models," *Neurocomputing*, vol. 653, p. 131231, 2025. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0925231225019034>
- [5] Apriorit. (2026, Jan.) Top 4 healthcare technology trends to watch in 2026. Apriorit. [Online]. Available: <https://www.apriorit.com/dev-blog/healthcare-technology-trends>
- [6] H. Habibzadeh, K. Dinesh, O. Rajabi Shishvan, A. Boggio-Dandry, G. Sharma, and T. Soyata, "A survey of Healthcare Internet of Things (HIoT): A clinical perspective," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 53–71, 2020.
- [7] A. Paulouski, "Best applications for the internet of things in business," <https://softteco.com/blog/how-iot-applications-benefit-industries-today>, 2026, accessed: 2026-07-08.
- [8] Fortune Business Insights. (2026) Internet of Medical Things (IoMT) Market Size, Share & Industry Analysis. Last updated: June 08, 2026. Report ID: FBI101844. [Online]. Available: <https://www.fortunebusinessinsights.com/industry-reports/internet-of-medical-things-iomt-market-101844>
- [9] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in iomt communications: A survey," *Sensors*, vol. 20, no. 17, p. 4828, 2020.
- [10] EC-Council University. (2026, Jan.) Healthcare data security in 2026: Protecting sensitive medical information from cyber risks. EC-Council University. [Online]. Available: <https://www.eccu.edu/blog/healthcare-data-security-in-2026/>
- [11] Telsy, "L'Internet of medical things (IoMT)," <https://www.telsy.com/linternet-of-medical-things-iomt/>, Nov. 2025, accessed: 2026-07-09.
- [12] G. Stanco, A. Navarro, F. Frattini, G. Ventre, and A. Botta, "A comprehensive survey on the security of Low Power Wide Area Networks for the Internet of Things," *ICT Express*, vol. 10, no. 3, pp. 519–552, 2024.
- [13] Bluetooth SIG, Inc., "Bluetooth Technology Overview," Available: <https://www.bluetooth.com/learn-about-bluetooth/tech-overview/>, Accessed: 2026-07-29.
- [14] K. Townsend, R. Davidson, and C. Cufi, *Getting Started with Bluetooth Low Energy*. O'Reilly, 2014. [Online]. Available: <https://books.google.it/books?id=XjY4nwEACAAJ>
- [15] G. Kwon, J. Kim, J. Noh, and S. Cho, "Bluetooth low energy security vulnerability and improvement method," in *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*. IEEE, 2016, pp. 1–4.

- [16] A. Rose, J. Bindewald, B. Ramsey, M. Rice, and B. Mullins, "Securing Bluetooth Low Energy locks from unauthorized access and surveillance," in *Critical Infrastructure Protection XI*, M. Rice and S. Sheno, Eds. Cham: Springer International Publishing, 2017, pp. 319–338.
- [17] K. S. Kwak, S. Ullah, and N. Ullah, "An overview of IEEE 802.15. 6 standard," in *2010 3rd international symposium on applied sciences in biomedical and communication technologies (ISABEL 2010)*. IEEE, 2010, pp. 1–6.
- [18] "Ieee standard for information technology–telecommunications and information exchange between systems - local and metropolitan area networks–specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications," *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)*, pp. 1–4379, 2021.
- [19] C. S. Alliance, "ZigBee - Complete IoT Solution," available at <https://csa-iot.org/all-solutions/zigbee/>. Accessed: 2026-07-29. [Online]. Available: <https://csa-iot.org/all-solutions/zigbee/>
- [20] ZigBee Standards Organization, "ZigBee Smart Energy Standard," available: <https://zigbeealliance.org/wp-content/uploads/2019/11/docs-07-5356-19-0zse-zigbee-smart-energy-profile-specification.pdf>, Accessed: 2026-08-04.
- [21] G. Stanco, A. Botta, F. Frattini, U. Giordano, and G. Ventre, "On the performance of IoT LPWAN technologies: the case of Sigfox, LoRaWAN and NB-IoT," in *ICC 2022 - IEEE International Conference on Communications*. IEEE, 2022, pp. 2096–2101.
- [22] LoRa Alliance, "LoRa Alliance," Available: <https://loro-alliance.org/>, Accessed on: Jul. 11, 2023.
- [23] K. E. Nolan, W. Guibene, and M. Y. Kelly, "An evaluation of low power wide area network technologies for the Internet of Things," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2016, pp. 439–444.
- [24] The Things Industries, "Duty Cycle," Available: <https://www.thethingsnetwork.org/docs/lorawan/duty-cycle/>, Accessed on: Jul. 11, 2023.
- [25] A. Díaz Zayas, F. J. Rivas Tocado, and P. Rodríguez, "Evolution and testing of NB-IoT solutions," *Applied Sciences*, vol. 10, no. 21, 2020.
- [26] K. K. Nair, A. M. Abu-Mahfouz, and S. Lefophane, "Analysis of the Narrow Band Internet of Things (NB-IoT) Technology," in *2019 Conference on Information Communications Technology and Society (ICTAS)*. IEEE, 2019, pp. 1–6.
- [27] *System architecture for the 5G System (5GS)*, 3GPP, 2022, v16.12.0.
- [28] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.
- [29] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3682–3722, 2019.
- [30] GSM Association, "5G RedCap and eRedCap: The future of efficient IoT connectivity," https://www.gsm.com/solutions-and-impact/technologies/internet-of-things/gsm_resources/redcap-eredcap-for-iot/, Mar. 2025, accessed on: 2026-07-31.
- [31] J. Sanchez-Gomez, D. G. Carrillo, R. Sanchez-Iborra, J. L. Hernández-Ramos, J. Granjal, R. Marin-Perez, and M. A. Zamora-Izquierdo, "Integrating LPWAN technologies in the 5G ecosystem: A survey on security challenges and solutions," *IEEE Access*, vol. 8, pp. 216437–216460, 2020.
- [32] S. Rotbei, L. Napolitano, S. Zinno, P. Verze, and A. Botta, "Predicting patient sexual function after prostate surgery using machine learning," in *2023 IEEE Symposium on Computers and Communications (ISCC)*, 2023, pp. 1–6.
- [33] S. Zinno, S. Rotbei, G. Stanco, G. Ventre, G. D'Urso, and A. Botta, "Exploring depression severity during lockdown through explainable ai," in *2025 21th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2025, pp. 1–6.
- [34] T. Shah, K. Dumasia, H. Lad, K. Shah, K. Nadiyadra, and V. Suratwala, "A systematic review of emerging trends of IoT in healthcare and IoMT frameworks," *Discover Public Health*, vol. 23, no. 1, p. 52, 2026.
- [35] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of Machine and Deep Learning Methods for Internet of Things (IoT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.
- [36] Q. Hu, F. Wu, R. K. Wong, R. C. Millham, and J. Fiaidhi, "A novel indoor localization system using Machine Learning based on Bluetooth Low Energy with Cloud computing," *Computing*, vol. 105, no. 3, pp. 689–715, 2023.
- [37] M. Patel and U. Korat, "Enhancing indoor localization accuracy with bluetooth low energy rssi signals analysis using machine learning algorithms," in *2026 14th International Symposium on Digital Forensics and Security (ISDFS)*, 2026, pp. 1–6.
- [38] G. Pau, F. Arena, M. Collotta, and X. Kong, "A practical approach based on Bluetooth Low Energy and neural networks for indoor localization and targeted devices' identification by smartphones," *Entertainment Computing*, vol. 43, p. 100512, 2022.
- [39] O. Altay, M. Erel-Özçevik, E. Varol Altay, and Y. Özçevik, "Average localization error prediction for 5g networks: An investigation of different machine learning algorithms," *Wireless Personal Communications*, vol. 136, no. 1, pp. 289–319, 2024.
- [40] H. S. Fahama, K. Ansari-Asl, Y. S. Kaviani, and M. N. Soorki, "An experimental comparison of rssi-based indoor localization techniques using zigbee technology," *IEEE Access*, vol. 11, pp. 87985–87996, 2023.
- [41] S. Hosseinzadeh, M. Ashawa, N. Owah, H. Larijani, and K. Curtis, "Explainable machine learning for LoRaWAN link budget analysis and modeling," *Sensors*, vol. 24, no. 3, p. 860, 2024.
- [42] P. Lohan, B. Kantarci, M. Amine Ferrag, N. Tihanyi, and Y. Shi, "From 5g to 6g networks: A survey on ai-based jamming and interference detection and mitigation," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 3920–3974, 2024.
- [43] M. Amir and M. Ghribi, "A comprehensive survey of intelligent routing in wireless body area networks based on metaheuristics and artificial intelligence," in *2026 International Wireless Communications and Mobile Computing (IWCMC)*, 2026, pp. 157–162.
- [44] T. Le and S. Shetty, "Artificial intelligence-aided privacy preserving trustworthy computation and communication in 5g-based iot networks," *Ad Hoc Networks*, vol. 126, p. 102752, 2022.
- [45] X. Fang, L. Zheng, X. Fang, W. Chen, K. Fang, L. Yin, and H. Zhu, "Pioneering advanced security solutions for reinforcement learning-based adaptive key rotation in Zigbee networks," *Scientific Reports*, vol. 14, no. 1, p. 13931, 2024.
- [46] F. Qi, Y. Zhao, M. Z. A. Bhuiyan, H. Tao, W. Yan, and Z. Tang, "Artificial intelligence driven wi-fi csi data mining: Focusing on the intrusion detection applications," *International Journal of Communication Systems*, vol. 38, no. 17, p. e5338, 2025.
- [47] Ş. Şolpan, H. Gündüz, and K. Küçük, "Wi-Fi network intrusion detection: Enhanced with feature extraction and Machine Learning algorithms," in *2024 8th International Artificial Intelligence and Data Processing Symposium (IDAP)*, 2024, pp. 1–7.
- [48] K. A. Al-Sammak, S. H. Al-Gburi, I. Marghescu, A.-M. C. Drăgulescu, C. Marghescu, A. Martian, N. A. H. Al-Sammak, G. Suciu, and K. M. A. Alheeti, "Optimizing IoT energy efficiency: Real-time adaptive algorithms for smart meters with LoRaWAN and NB-IoT," *Energies*, vol. 18, no. 4, p. 987, 2025.
- [49] D. Bortnik, V. Nikic, S. Sobot, D. Vukobratovic, I. Mezei, and M. Lukic, "Evaluation of Machine Learning algorithms for NB-IoT module energy consumption estimation based on radio channel quality," *IEEE Access*, vol. 13, pp. 2389–2408, 2025.
- [50] S. Anbazhagan and R. Mugelan, "Adaptive power-saving mode control in NB-IoT networks using soft actor-critic reinforcement learning for optimal power management," *Scientific Reports*, vol. 15, no. 1, p. 34618, 2025.
- [51] J. J. Alcaraz, F. Losilla, and F.-J. Gonzalez-Castaño, "Transmission control in NB-IoT with model-based Reinforcement Learning," *IEEE Access*, vol. 11, pp. 57991–58005, 2023.
- [52] M. Alkhayyal and A. Mostafa, "Recent developments in AI and ML for IoT: A systematic literature review on LoRaWAN energy efficiency and performance optimization," *Sensors*, vol. 24, no. 14, p. 4482, 2024.
- [53] A. Ali, S. M. Ahmed, M. S. Sayed, and A. Shalaby, "Deep learning-based human body communication baseband transceiver for WBAN IEEE 802.15.6," *Engineering Applications of Artificial Intelligence*, vol. 115, p. 105169, 2022.