Babylonian Journal of Internet of Things
Vol.2026, **pp**. 89–137
DOI: https://doi.org/10.58496/BJIoT/2026/008; ISSN: 3006-1083
https://mesopotamian.press/journals/index.php/BJIoT

Research Article

Internet of Bio-Nano Things (IoBNT) Security: A Comprehensive Survey of Threat Models, Protocols, Mitigation Strategies, Technological Integrations, Tools, and Performance Metrics

Guma Ali [1,*], Bosco Apparatus Buruga [2]

[1] *Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda.*

[2] *Department of Library and Information Services, Muni University, Arua, Uganda.*

ARTICLE INFO

Article History

Received 07 May 2026
Revised 2 Jun 2026
Accepted 30 Jun 2026
Published 04 Jul 2026

Keywords
Internet of Bio-Nano Things (IoBNT),
Bio-nanotechnology,
IoBNT Security and privacy,
Molecular communication,
Nano-networks.

ABSTRACT

The Internet of Bio-Nano Things (IoBNT) constitutes a transformative paradigm to support applications in precision medicine, environmental monitoring, and bio-hybrid cyber-physical systems. However, it faces a complex security landscape. Existing research typically examines isolated threats, individual protocol layers, or specific communication modalities, rather than providing a unified perspective on security vulnerabilities, threat models, and mitigation strategies across the entire IoBNT stack. This study provides a comprehensive, structured, and security-centric overview of IoBNT systems by identifying and classifying security threats; analyzing existing and emerging security protocols and mitigation techniques; examining enabling technological integrations that support secure IoBNT operations; and establishing coherent performance metrics and evaluation criteria. The study adopted a comprehensive review methodology, examining 153 research papers retrieved from Frontiers, ACM Digital Library, Wiley Online Library, Nature, Springer Nature, ScienceDirect, MDPI, IEEE Xplore Digital Library, and Google Scholar, with a focus on publications from 2023 to 2026 that addressed security aspects of the IoBNT. The survey examines contemporary security challenges and defenses in the IoBNT ecosystem. It synthesizes state-of-the-art mitigation strategies alongside reinforcing technological integrations for predictive bio-cyber risk assessment and quantum-safe mechanisms that support long-term resilience. The analysis also surveys tools, simulation frameworks, testbeds, and experimental platforms used to model, validate, and benchmark IoBNT security solutions, while consolidating standardized performance metrics. Finally, it maps the current research landscape, identifies open challenges, and outlines future directions for developing secure, reliable, and ethically aligned IoBNT systems. This survey offers important implications for both researchers and practitioners by delivering a holistic security perspective that informs the design of robust, interoperable, and trustworthy IoBNT systems.

1. INTRODUCTION

The Internet of Things (IoT) has fundamentally changed how humans interact with their environment by enabling interconnected devices to sense, collect, and exchange data. Extending this paradigm, the Internet of Nano Things (IoNT) introduces nano-scale devices capable of communicating and collaborating at the cellular and molecular levels [1]. Advances in nanotechnology, biotechnology, and information technology have accelerated interdisciplinary research in electrical and communication engineering, giving rise to the Internet of Bio-Nano Things (IoBNT) [2]. Jamshidi et al. [3] and Sun et al. [4] define IoBNT as an advanced paradigm integrating nanotechnology, molecular communication, synthetic biology, biosensing, and IoT. This integration enables the development of nano-scale biological devices, referred to as bio-nano things (BNTs), which can sense, actuate, process, and transmit information across molecular, cellular, bio-nanomachine, and macroscale interfaces. Importantly, IoBNT enables seamless interaction between biological systems and the Internet's electrical domain.

This paradigm enables nano-scale orchestration of molecular communication and networking, supporting precise control and engineering of biological cells. IoBNT deploys sensing and processing devices that operate within biological environments to exchange information [5]. By leveraging clusters of biocompatible, embedded artificial or biological computing devices, IoBNT facilitates intra-body sensing, communication, and actuation [6]. These capabilities improve the monitoring of molecular and cellular changes and enhance the fidelity of digital twin modeling and simulation. In addition, IoBNT bridges

*Corresponding author. Email: a.guma@muni.ac.ug

biological systems with digital models by integrating heterogeneous data streams and enabling seamless data flow. It incorporates advanced hardware-level security mechanisms to protect sensitive biological information [7]. IoBNT aims to establish robust methodologies for real-time sensing, communication, and control in biochemical systems, integrating these capabilities into the electrical Internet via molecular communication, nanosensing, intelligent swarm systems, and bio-cyber interfaces [4][8]. The development of IoBNT is further supported by complementary IoT-based paradigms, including the IoNT, the Internet of Bio-degradable Things (IoBDT), the Internet of Ingestible Things (IoIT), the Intelligent Internet of Things (IIoT), and the Internet of Everything (IoE) [9].

The IoNT market, including the specialized subset of IoBNT, is projected to grow from US$22.99 billion in 2025 to US$71.88 billion by 2030, with a compound annual growth rate (CAGR) of 25.60%. The commercialization of terahertz-band nano-antenna designs, ultra-low-power carbon nanotube sensors, and the integration of nano-scale communication protocols with conventional wireless networks drive this growth. Key components of IoBNT networks include biological or synthetic nanomaterials, implantable nano-devices, and nanomicro interfaces or gateways. Nano-things function as resource-constrained sensors and actuators within the human body and communicate using molecular mechanisms such as diffusion or electrochemical signaling. These devices convert physiological signals, including blood glucose, heart rate, and blood pressure, into network-compatible data. Implantable nano-devices communicate with nano-scale nodes via molecular signaling and interact with gateways via electromagnetic (EM) communication, including terahertz waves. Gateways, typically positioned on or near the skin, possess greater computational and energy resources and relay data both within and outside the body using EM communication [3][4].

IoBNT relies on specialized communication protocols, including molecular, chemical, optical, and conventional wireless techniques such as Bluetooth and Zigbee, to enable secure and efficient data exchange. By aggregating information from multiple nano-devices, these networks support coordinated monitoring, disease biomarker detection, condition tracking, and personalized decision-making in healthcare applications [10][11]. To enable these functions, IoBNT employs diverse communication paradigms, including molecular communication, bio-electrical and ionic pathways, Förster Resonance Energy Transfer (FRET), optical nano-scale signaling, neural spike-based biochannels, and hybrid bio–cyber architectures [12-14]. Its communication models encompass molecular, electromagnetic nano-scale, chemical, and multi-modal frameworks [15-17].

IoBNT extends connectivity and control to nonconventional domains, particularly the human body, with unprecedented spatio-temporal resolution. This capability enables transformative applications such as continuous disease monitoring, targeted drug delivery, precision cancer theranostics, infection detection, immune modulation, smart wound healing, and tissue regeneration. Beyond healthcare, IoBNT supports environmental pollution monitoring, bio-nano agriculture, food safety, industrial bioprocess optimization, smart water treatment, microbial control, biosecurity, and biothreat detection [14][18][19]. The specifications of IoBNT enable precision healthcare and personalized medicine by supporting early diagnosis, continuous monitoring, and advanced neuroscience applications such as brain–computer interfaces. They also facilitate environmental exposure monitoring, data-driven public health strategies, reduced hospitalization through remote care, real-time lifestyle feedback, improved surgical guidance, and accelerated drug discovery [3][13][20].

Despite its promise, IoBNT faces severe cybersecurity challenges due to its tight coupling with biological systems. These threats include data breaches, privacy violations, unauthorized actuation, physiological manipulation, authentication attacks, molecular eavesdropping, molecular jamming, denial-of-service (DoS) attacks, nano-device cloning, nano-malware propagation, biological hijacking, side-channel attacks, and cross-domain cyber–bio threats [12][18]. Security failures in IoBNT can directly impact physiology by disrupting homeostasis, altering microbiomes, triggering unintended cellular responses, or causing toxic biochemical reactions. Compromised deployments may also lead to uncontrolled replication of bio-nanodevices, ecological disruption, or leakage of sensitive health and environmental data. These risks pose ethical, biosafety, and biosecurity concerns that extend beyond those of conventional networked systems [11][12].

Traditional security mechanisms based on cryptographic computation, electromagnetic authentication, or hardware trust anchors are often infeasible at the nano-scale due to extreme resource constraints and biocompatibility requirements [21]. Consequently, IoBNT security must integrate digital protection with biochemical safeguards, biological containment, and cross-domain threat modeling to address both cyber and biophysical attack surfaces. To address these challenges, researchers have proposed lightweight security protocols, authentication schemes, trust management frameworks, secure molecular communication mechanisms, and deep learning (DL)-based intrusion detection systems [1][22]. These protocols are reinforced by mitigation strategies spanning molecular-layer defenses, network-layer protections, physical and biological safeguards, behavioral anomaly detection, cryptographic techniques, and device hardening approaches [5][23]. Researchers have also integrated enabling technologies such as edge, fog, and cloud computing, artificial intelligence (AI), blockchain, post-quantum security, 6G and terahertz communications, digital twins, and synthetic biology to enhance IoBNT security and scalability [24-26]. To support design and evaluation, IoBNT research employs a wide range of tools, including

simulation platforms such as NS-3, OMNeT++, Contiki/Cooja, IoTSecSim, NetSim, MATLAB/Simulink, and custom Python-based simulators. Experimental testbeds include microfluidic molecular communication setups, DNA-based communication systems, synthetic cells, and nano-scale chemical computing platforms [4][27]. Performance evaluation relies on comprehensive metrics spanning molecular communication efficiency, network performance, security effectiveness, energy consumption, biocompatibility, and multi-objective optimization [4][28][29].

Researchers have made significant strides in the IoBNT. Sathish et al. [12] analyzed security and threat models for bio-nanonetworks and proposed a taxonomy of attacks and mitigation strategies. Borges et al. [30] investigated communication models and channel characterization for molecular and FRET-based signaling, quantifying capacity, noise, and latency. Thiyagaraj [10] examined the integration of IoBNT with edge AI and distributed analytics, highlighting benefits for on-device inference and anomaly detection while noting increased attack surfaces and privacy risks. Jia et al. [21] developed proof-of-concept protocols and simulations that address authentication, lightweight cryptography, and physical-layer secrecy in diffusive channels. Despite these advances, most studies remain theoretical or simulated, with experimental validation, standardization, and cross-disciplinary security frameworks still limited [9]. To date, no study has comprehensively surveyed IoBNT security across attack models, mitigation strategies, enabling technologies, tools, and evaluation metrics. This survey fills that gap by systematically analyzing existing work, benchmarking approaches, identifying limitations, and highlighting open research challenges. By consolidating foundational concepts and security advances, it provides a comprehensive reference for researchers and practitioners. It lays the groundwork for secure, scalable, and resilient IoBNT deployments across biomedical, environmental, and industrial domains.

This survey comprehensively analyzes the security landscape of the IoBNT, identifies gaps in current research, and establishes a foundation for future investigations, with its key contributions summarized as follows:

1. Review the state-of-the-art in IoBNT overview, system architecture, system architecture components, communication paradigms, and communication models.
2. Identify the cybersecurity threats, attacks, and challenges in IoBNT.
3. Explain the security requirements in IoBNT.
4. Critically review the security protocols and threat mitigation strategies in IoBNT security.
5. Explore the integration of emerging technologies into IoBNT Security.
6. State the tools, testbeds, and simulation platforms for IoBNT Security.
7. Synthesize the performance metrics and evaluation frameworks in IoBNT Security.
8. Identify the open challenges and future research directions.

The survey proceeds as follows: Section 2 details the materials and methods used in this study, while Section 3 provides background on IoBNT, covering its overview, architecture, system components, communication paradigms, and models. Section 4 analyzes cybersecurity threats, attacks, and challenges specific to IoBNT, and Section 5 addresses security, including requirements, protocols, and threat mitigation strategies. Section 6 examines technological integrations, and Section 7 reviews tools, testbeds, and simulation platforms for modeling and evaluating IoBNT security. Section 8 presents performance metrics and evaluation frameworks for assessing security mechanisms; Section 9 discusses current challenges and technological and implementation gaps; and Section 10 outlines future research directions to enhance secure and resilient IoBNT deployments. Finally, Section 11 concludes the article, summarizing key findings and implications for researchers and practitioners.

2. MATERIALS AND METHODS

This survey employs a structured, multi-stage methodology to systematically collect, evaluate, synthesize, analyze, and organize the literature on the IoBNT's security landscape. The approach follows established best practices for systematic, technology-focused reviews while explicitly accounting for the interdisciplinary scope of IoBNT, which integrates molecular communications, bioengineering, nanotechnology, wireless networking, and cybersecurity.
The survey is organized around a set of core research questions (RQs) that define its structure and analytical focus.

1. RQ1: What is the overview, architecture, system architecture components, communication paradigms, and communication models of IoBNT systems, and how do they influence security requirements?
2. RQ2: What types of cybersecurity threats, attacks, and challenges arise in IoBNT systems?

3. RQ3: Which security protocols and threat mitigation strategies have been proposed to secure IoBNT?
4. RQ4: What technological integrations enhance IoBNT security?
5. RQ5: What tools, datasets, simulation environments, and performance metrics are commonly used to evaluate IoBNT security solutions?
6. RQ6: What open challenges and limitations, and future research directions emerge from the existing literature?

These RQs guided the selection criteria, informed the categorization of contributions, and directed the evaluation of security approaches.

The researchers developed a comprehensive search protocol to capture relevant literature across engineering and life sciences, examining peer-reviewed articles, conference papers, and book chapters from Frontiers, ACM Digital Library, Wiley Online Library, Nature, Springer Nature, ScienceDirect, MDPI, IEEE Xplore Digital Library, and Google Scholar. Using Boolean operators, the researchers combined keyword groups to cover IoBNT, nanonetworks, and molecular communication security, with representative queries such as “Internet of Bio-Nano Things” AND “security,” OR “molecular communication” AND (“threats” OR “attacks”), OR “bio-cyber interface” AND “authentication,” OR “nanonetworks” AND “intrusion detection,” OR “bio-nano devices” AND “cryptography,” OR “biological nano-machines” AND “trust management,” and “IoBNT” AND (“blockchain” OR “machine learning”). The researchers iteratively refined and tailored these search strings to each database’s indexing and search capabilities, ensuring comprehensive coverage while retaining only the most relevant studies on IoBNT security.

To ensure methodological rigor and thematic relevance, the researchers applied explicit inclusion and exclusion criteria during literature selection to identify studies that make substantive contributions to IoBNT security challenges, mitigation strategies, protocols, architectures, and evaluation frameworks. The inclusion criteria covered peer-reviewed articles, conference papers, and book chapters that explicitly addressed security, privacy, or trust in the IoBNT. Eligible studies analyzed or proposed security protocols, cryptographic mechanisms, authentication schemes, or access-control models tailored to bio-nano or molecular communication networks. We also included works that examined IoBNT-specific threat models, attack surfaces, and mitigation strategies, as well as studies integrating IoBNT security with enabling technologies such as nanotechnology, synthetic biology, molecular communications, blockchain, AI/machine learning (ML), and edge or fog computing. In addition, studies introducing, evaluating, or benchmarking tools, frameworks, or simulation environments for securing IoBNT systems were considered, provided they reported relevant quantitative or qualitative performance metrics (e.g., latency, energy efficiency, reliability, scalability, or security overhead). Only English-language publications with accessible full text, published between 1 January 2023 and 30 April 2026, were included to capture recent advances.

The exclusion criteria excluded studies that focused exclusively on general IoT, wireless sensor networks, or body area networks, or that lacked explicit relevance to bio-nano or molecular communication contexts. We excluded works centered on biomedical nanotechnology or bioengineering applications that lacked a security, privacy, or threat-mitigation perspective, as well as non-peer-reviewed materials such as editorials, opinion pieces, posters, abstract-only papers, blogs, or other non-academic sources. Studies were also excluded if they lacked sufficient methodological detail, experimental validation, or conceptual clarity regarding IoBNT security mechanisms; failed to discuss protocols, tools, threat-mitigation strategies, or performance evaluation; or offered no practical insights for securing IoBNT systems. Duplicate publications and extended versions were removed when a more comprehensive or updated version was available, and studies not written in English, without an accessible full text, or published before 1 January 2023 were excluded.

The study selection followed a rigorous multi-stage process to minimize bias and ensure methodological consistency. Three independent reviewers screened titles and abstracts to exclude irrelevant publications and identify studies addressing IoBNT security, including threats, attacks, challenges, mitigation protocols, technological integrations, tools, and performance metrics. The reviewers then conducted full-text assessments of eligible records to confirm inclusion, resolving disagreements through discussion or consultation with a third reviewer. They managed references in Mendeley and screened in Rayyan, removing duplicates before evaluation. At each stage, they documented reasons for exclusion and standardized retained studies to support accurate data extraction. To enhance reliability, the reviewers used a test–retest strategy, repeatedly reassessing randomly selected papers to ensure consistency and reduce selection bias.

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow diagram illustrates the identification, screening, eligibility, and inclusion stages of the review process. The researchers initially identified more than 5,765 publications from academic databases and search engines. After duplicate removal and abstract screening, they narrowed the pool to 2,623 studies, then assessed eligibility for 1,812 publications. From these, 153 studies met the inclusion criteria and were selected for systematic analysis. Figure 1 presents the PRISMA flow diagram summarizing this selection process.

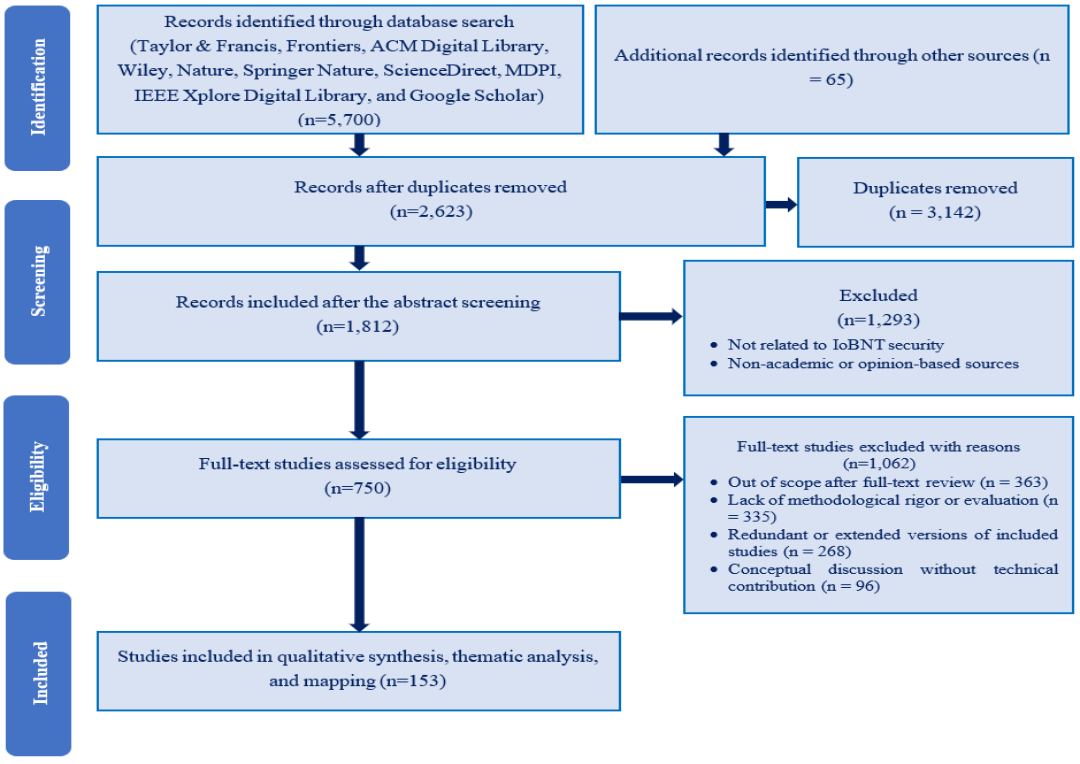


Fig. 1. The PRISMA flow diagram summarizes this selection process.

The final dataset comprised 153 studies sourced from multiple digital libraries. These included 2 from Frontiers, 4 from ACM Digital Library, 1 from Wiley Online Library, 23 from Nature, 6 from Springer Nature, 16 from ScienceDirect, 20 from MDPI, 48 from IEEE Xplore Digital Library, and 33 from Google Scholar, reflecting a broad and diverse coverage of the relevant literature. To contextualize this corpus, Figure 2 presents a structured overview of the research paper categories included in the survey.

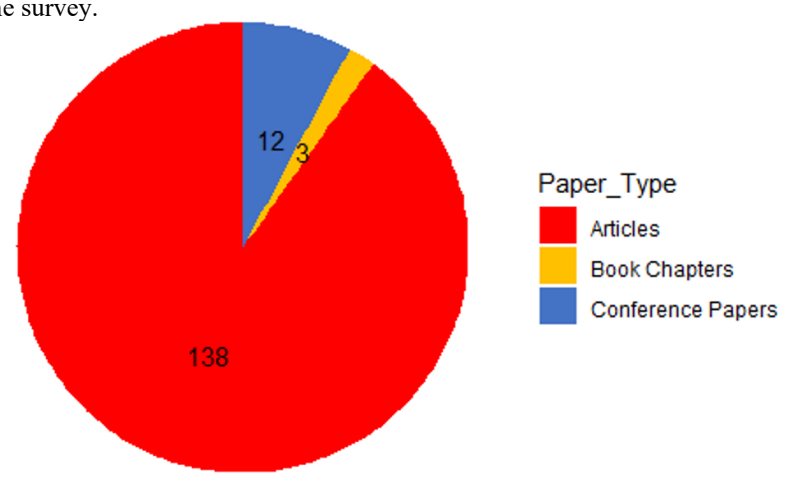


Fig. 2. Presents a structured overview of the research paper categories included in the survey.

Figure 3 illustrates the digital databases used by the researchers to retrieve the research papers included in this survey, providing a clear overview of the sources from which the relevant literature was systematically collected.

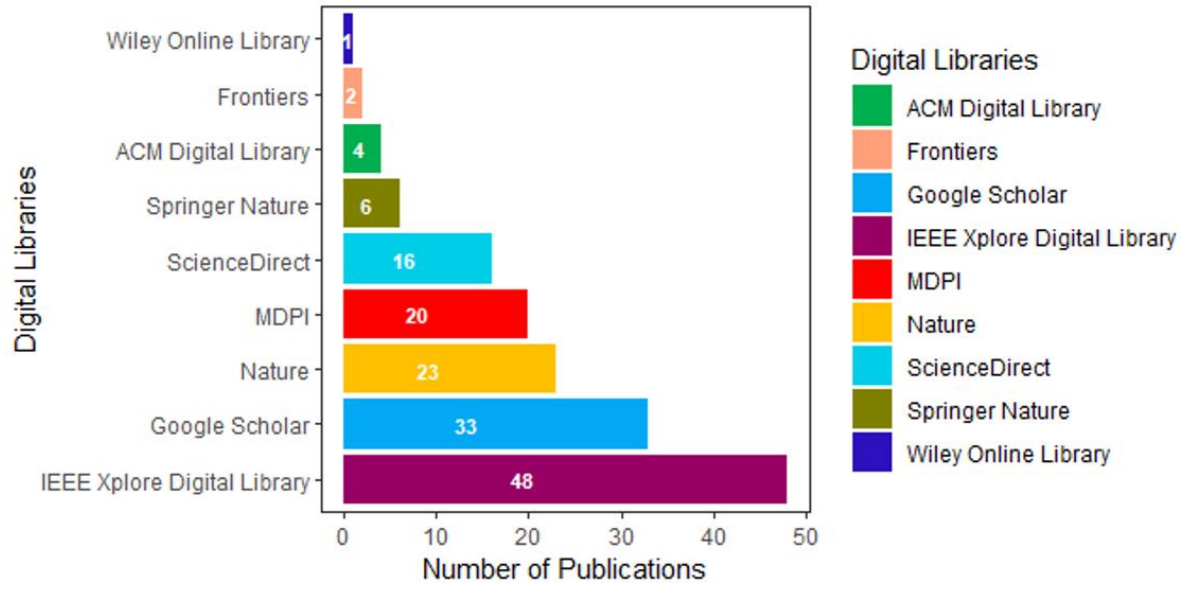


Fig. 3. Illustrates the digital databases used to retrieve the research papers.

Figure 4 illustrates the distribution of the selected research papers across major digital libraries, showing how the included studies are allocated among different repositories. This figure provides a clear overview of the relative contributions of each digital library to the final dataset, thereby clarifying the sources of the reviewed literature.

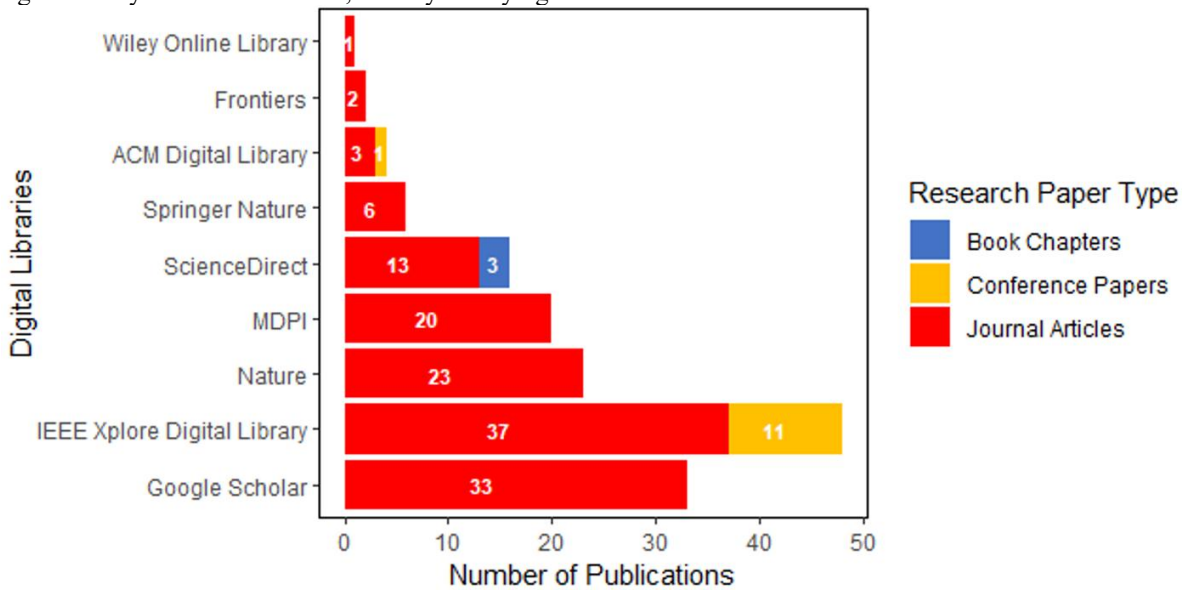


Fig. 4. Illustrates the distribution of the selected research papers across major digital libraries.

Figure 5 illustrates the distribution of selected papers across different digital libraries by publication year, highlighting temporal trends in the literature.

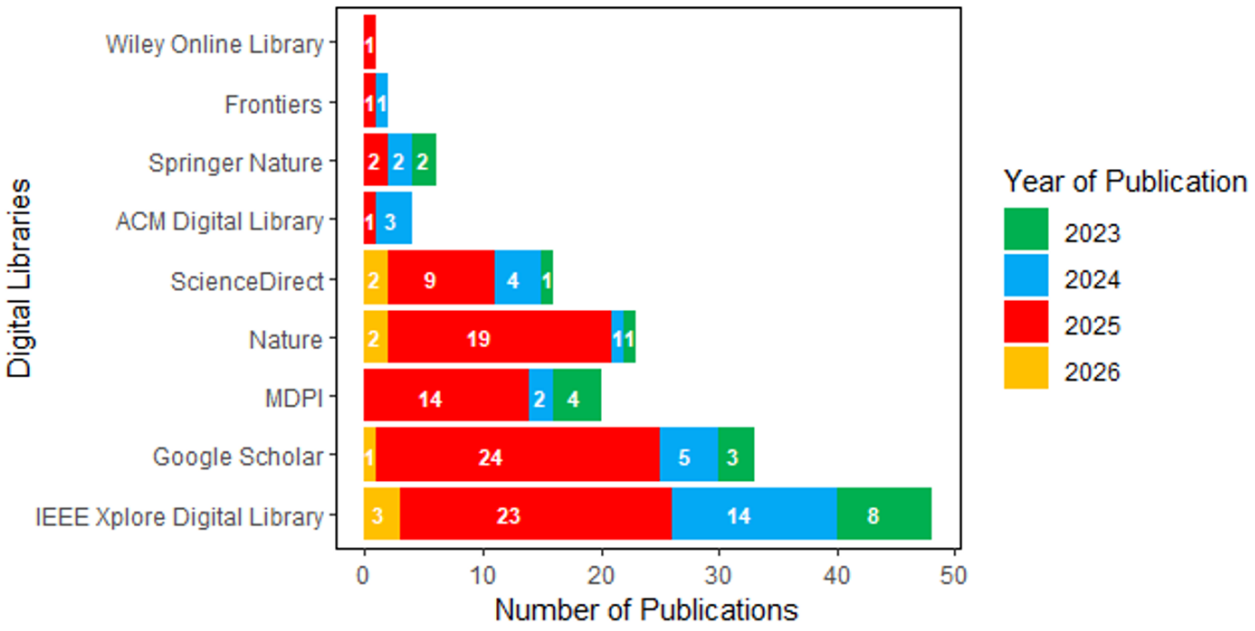


Fig. 5. Illustrates the distribution of selected papers across different digital libraries by publication year.

All retrieved publications underwent a structured three-stage screening process. First, titles and abstracts were reviewed to exclude studies outside the IoBNT or nanonetwork security domains. Second, the full texts of the remaining articles were assessed for relevance to communication protocols, security threats, mitigation strategies, tools, and performance metrics. Finally, data extraction was validated through cross-checking by three independent reviewers to minimize bias.

Each included study was systematically evaluated using multiple quality dimensions. These included technical rigor, assessed by the clarity of proposed protocols, mathematical modeling, and biological feasibility; security relevance, evaluated by the threat model definition, attack coverage, and mitigation completeness; and experimental support, assessed by simulations, testbed validation, or molecular modeling. The assessment also examined reproducibility, based on the availability of pseudocode, tools, datasets, or parameter specifications, and innovative contribution, reflecting novel insights into IoBNT architectures or security paradigms. From each study, the researchers extracted detailed information on IoBNT architectures, system components, communication paradigms, and models. They also documented and identified cybersecurity threats, attacks, and challenges, along with the corresponding security objectives. In addition, the review captured proposed security protocols and mitigation strategies, technological integrations, tools, datasets, simulation environments, performance metrics, and explicitly stated limitations and assumptions.

To ensure consistency and reliability, the researchers developed and piloted a standardized data-charting form. This form recorded bibliographic details (authors, year, and country), study type (empirical, simulation, conceptual, review, or policy/standards), IoBNT security focus, protocols, threat mitigation strategies, technological integrations, tools, performance metrics, key findings, contributions, reported limitations, and future research directions. Three reviewers independently extracted the data, followed by cross-verification to ensure accuracy.

Given the exploratory scope of the study, the researchers employed qualitative thematic synthesis to analyze the collected data in depth. They validated the findings through expert consultation, comparison with prior studies, and critical evaluation of robustness. Only high-quality studies were included, selected using a grading system that assessed methodological rigor, reliability, and relevance to IoBNT security. As the analysis relied solely on published literature, ethical approval was not required, and all sources were appropriately cited.

Despite the comprehensive methodology, several limitations warrant consideration. IoBNT research evolves rapidly, and although structured search strategies were employed, some recently published protocols, threat models, or experimental frameworks may not yet be indexed in major databases, leading to minor gaps in coverage of emerging security primitives or biological communication paradigms. In addition, terminological heterogeneity across bioengineering, nanotechnology, molecular communications, cybersecurity, and synthetic biology complicates consistent classification; while normalization procedures mitigate these issues, some conceptual discrepancies persist. Many studies further rely on simulation-based or theoretical evaluations, as large-scale experimental datasets and real-world validations remain constrained by current technological capabilities, which limit the generalizability of reported performance metrics. Comparative analysis is also

challenged by heterogeneous threat models and attack assumptions, including idealized adversarial capabilities or narrowly defined attack surfaces; mapping studies to a unified threat taxonomy improves consistency but cannot fully resolve these methodological differences. Finally, while necessary for rigor, the inclusion and exclusion criteria may introduce selection bias by omitting non-English publications, non-peer-reviewed sources, or emerging contributions. Collectively, these limitations underscore the need for cautious interpretation of the findings and highlight directions for future surveys and experimental research in IoBNT security.

3. BACKGROUND

3.1 Conceptual Overview of IoBNT

The IoBNT is an emerging interdisciplinary paradigm that integrates nanotechnology, biotechnology, and information and communication technologies to enable networks of nano-scale biological and artificial devices, known as BNTs. Unlike conventional IoT systems, IoBNT operates within or at the boundaries of living systems, allowing continuous biochemical sensing, in situ diagnostics, targeted therapy, and closed-loop feedback through bio-cyber interfaces [11]. These capabilities position IoBNT as a transformative framework for interacting directly with biological environments.

IoBNT networks consist of engineered cells, nano-sensors, nanorobots, synthetic biological constructs, and other nano-scale devices that can sense, process, and communicate within complex biological environments. Operating at the micro- and nano-scale, these devices detect molecular or physiological signals, transmit information, and execute localized actions, such as drug delivery, biochemical actuation, and intracellular monitoring [31]. This integration of sensing, computation, and actuation enables precise and context-aware interventions.

Communication in IoBNT relies on nano-scale mechanisms, including molecular signaling, terahertz electromagnetic waves, nanomechanical interactions, and natural cell-to-cell communication pathways. Bio-Nano Things (BNTs) exchange information both among themselves and with surrounding biological structures and external cyber systems through hierarchical network architectures. Bio-cyber gateways, such as wearable devices, implantable systems, and biochemical-to-electronic interfaces, translate molecular signals into digital data, enabling multi-hop communication from nano-scale devices to external networks. This architecture supports real-time monitoring, adaptive decision-making, and precision interventions [32][33].

To ensure sustained functionality, IoBNT systems emphasize biocompatibility, ultra-low energy consumption, and high spatial resolution. Many devices harvest energy from local biological sources, such as metabolic processes or chemical gradients, reducing dependence on conventional power supplies. These features make IoBNT particularly suitable for applications in personalized medicine, environmental monitoring, precision agriculture, and biothreat detection.

Operationally, IoBNT interconnects bio-nanomachines into coordinated communication networks that follow a layered workflow adapted from traditional networking principles. These bio-nanomachines, including engineered cells, nanoparticles, and synthetic nano-devices, perform sensing, processing, and actuation by detecting biochemical signals (e.g., pH, glucose, toxins, or pathogens), interpreting inputs through genetic circuits or embedded logic, and triggering responses such as drug release or molecular signaling. For example, an engineered bacterium can detect a disease biomarker and activate a genetic pathway to produce a therapeutic agent. Communication among bio-nanomachines primarily occurs through molecular mechanisms rather than conventional electromagnetic waves. Information is encoded in molecules such as ions, proteins, or Deoxyribonucleic Acid (DNA) strands and transmitted through biological media like blood, interstitial fluid, or air. Diffusion-based communication is the most common method, in which molecules propagate from the transmitter to the receiver. However, flow-based transport, catalytic signaling, quorum sensing, and ligand–receptor interactions also contribute to signal exchange. At the receiver, specialized receptors decode these molecular signals into actionable information, enabling coordinated nano-scale interactions and system-wide functionality. Figure 6 illustrates the IoBNT in humans.

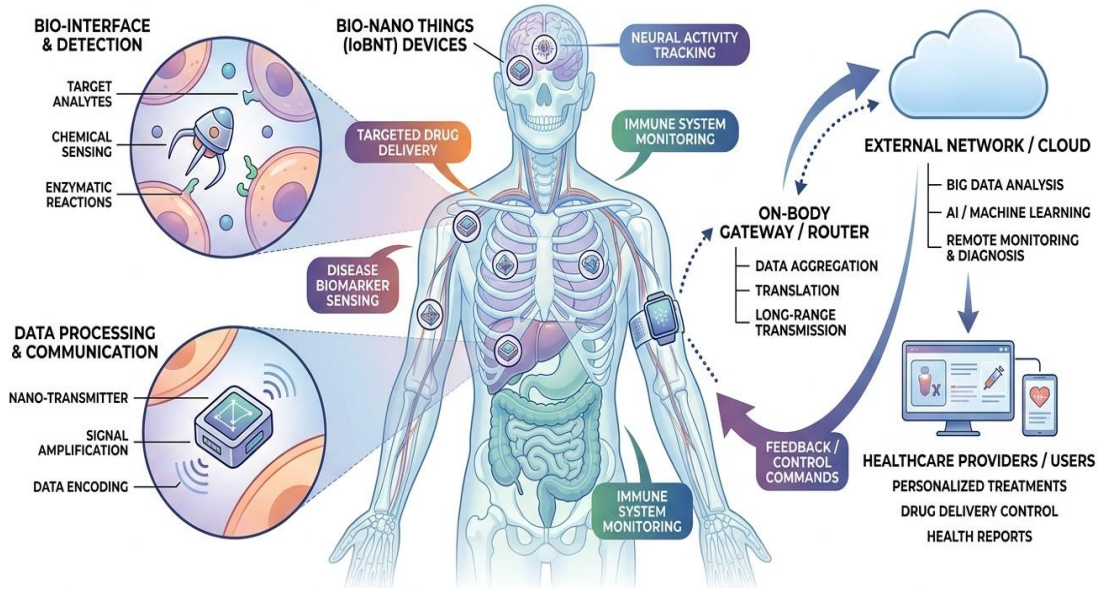


Fig. 6. Illustrates the conceptual drawing of a continuous health monitoring application of IoBNT in humans.

The evolution of IoBNT reflects the convergence of biotechnology, nanotechnology, molecular communication, synthetic biology, and advanced networking, progressing through distinct phases shaped by key scientific breakthroughs. Early foundations (pre-2000s to early 2000s) integrated advances in molecular biology and nanomaterials to enable bio-nano devices capable of sensing, actuation, and molecular signaling, with communication mechanisms inspired by biological processes such as neurotransmission [11]. This groundwork led to the conceptualization of bio-nano networks (mid-2000s to early 2010s), during which researchers formalized diffusion-, flow-, and catalytic-based communication models and developed programmable gene circuits alongside early nano-devices. Building on these theoretical advances, the period between 2012 and 2018 emphasized experimental validation, integrating engineered cells and artificial nano-devices into functional systems such as bionanosensors and biological transceivers. From 2018 to 2023, the field matured toward structured IoBNT architectures and protocols, incorporating multilayer designs, bio-cyber interfaces, energy harvesting, and security mechanisms, while expanding applications in healthcare and environmental monitoring [11]. Since 2023, convergence with AI, biocomputing, and advanced synthetic biology has driven the development of intelligent, adaptive bio-nano systems and hybrid communication models, enabling applications such as personalized medicine and real-time diagnostics [11]. Looking ahead, IoBNT aims to achieve fully autonomous, self-organizing bio-nano ecosystems with robust interoperability, scalable biomanufacturing, and safe deployment, while addressing persistent challenges in communication reliability, energy efficiency, and regulation [31][34].

IoBNT applications span healthcare, environmental monitoring, agriculture, and industrial systems, unified by continuous nano-scale sensing, intelligent communication, and adaptive actuation. In healthcare, IoBNT enables continuous in-body disease monitoring through biocompatible nano-sensor networks that track biomarkers, such as cytokines, hormones, metabolites, and enzymatic activity, and transmit real-time data via molecular or hybrid channels for AI-driven analysis and early detection of chronic diseases, cancer, neurodegeneration, and metabolic disorders [4][31][35]. Building on this capability, bio-nano machines support targeted, adaptive drug delivery by identifying disease-specific molecular signatures and releasing therapeutics locally with AI-guided dosing, thereby improving efficacy and minimizing off-target effects [20][36]. This functionality extends to precision cancer theranostics, in which nanorobots and smart nanocarriers integrate diagnosis and treatment, with continuous feedback for adaptive intervention [37][38]. IoBNT also advances smart prosthetics and neural interfaces by enabling high-bandwidth communication between nanosensors and neural pathways, thereby supporting closed-loop control and neurorehabilitation [39]. Additional applications include infection detection, immune modulation, wound healing, tissue regeneration, and personalized metabolic regulation through precise nano-scale monitoring and response [3][35]. Beyond medicine, IoBNT enables real-time detection and autonomous response systems for environmental pollution monitoring, smart water treatment, and precision agriculture [31].

In parallel, IoBNT enhances food safety and supply chains by embedding nano-sensors that detect pathogens and spoilage, improving transparency and traceability. In industrial contexts, it supports bioprocess optimization and smart biomanufacturing by integrating AI-driven nano-sensing with digital twins for predictive control and scalable production

[3], while also strengthening biosecurity through rapid, high-sensitivity pathogen detection [40]. Emerging directions, including precision fertility monitoring, in-body communication for assistive nanorobots, and bio-cyber interfaces, further connect biological signals with external computational platforms to enable personalized interventions [4]. Collectively, advanced paradigms such as digital twins, autonomous nanorobotics, and biocompatible cellular networks position IoBNT as a transformative framework for predictive healthcare and intelligent interaction with biological and environmental systems [8][31].

IoBNT delivers transformative benefits by enabling real-time monitoring and intervention at the cellular and molecular levels. It advances precision healthcare and personalized medicine by tailoring treatments to individual biological profiles, thereby improving efficacy and reducing side effects [31]. Through highly sensitive nano-sensors, it supports early disease detection and continuous health monitoring by identifying subtle biochemical changes and enabling proactive, data-driven clinical decisions [4][14][19]. Additionally, IoBNT enhances targeted drug delivery, advances neuroscience and brain-computer interfaces, and contributes to regenerative medicine by precisely monitoring and modulating biological processes [20]. Beyond clinical applications, IoBNT strengthens infection control, environmental monitoring, and public health surveillance by enabling real-time detection of pathogens and hazards and facilitating coordinated responses [40]. Its integration with AI supports predictive analytics, accelerates drug development, and enables continuous remote care, reducing hospitalizations and improving access [18]. Ultimately, IoBNT fosters cyber-physical symbiosis by linking biological systems with digital networks, enabling adaptive, closed-loop interventions and real-time lifestyle optimization based on continuous physiological feedback [13].

3.2 Architecture of IoBNT

IoBNT architecture consists of multiple layers, each performing distinct functions that collectively ensure seamless bio-nano communication and interaction with cyber-infrastructures. Below are the brief descriptions of these layers.

3.2.1. Nano-scale device layer

The nanoscale device layer forms the foundation of the IoBNT architecture, comprising bio-nano devices such as nano-sensors, nano-machines, and nanorobots that operate at the molecular level. These devices, whether synthetic, natural, or hybrid, perform molecular sensing (e.g., glucose, pH, temperature), localized actuation (e.g., targeted drug delivery or cell manipulation), basic onboard processing, and nano-scale communication using molecular or electromagnetic signals [32]. Molecular sensors and actuators detect biochemical changes and respond locally, while nanorobots and bio-hybrid systems execute more complex in-body functions. Additionally, nano-scale communication units enable inter-device signaling within biological environments. IoBNT envisions biocompatible nanonodes, such as engineered bacteria, human cells, and nano-biosensors, forming intra-body nanonetworks through molecular communication (MC), with capabilities for basic computation and embedded smart processing [18].

3.2.2. Nano-network layer

Building on nanoscale devices, the nanonetwork layer enables communication among these entities using mechanisms suited to biological environments. Since conventional electromagnetic communication is often impractical at this scale, the layer relies on molecular communication via chemical signaling and nano-electromagnetic communication using terahertz (THz) frequencies for short-range, high-bandwidth transmission. Relay and gateway nodes play a critical role by aggregating nano-scale signals and translating them for integration with higher-level networks. This layer defines communication protocols, addressing schemes, and network topologies while accounting for challenges such as diffusion delays, stochastic noise, and limited processing capacity. Core functions include routing, signal modulation, error detection, and collaborative data aggregation. These capabilities support applications such as real-time in-body diagnostics, smart drug delivery, and early disease detection [3][31]. Emerging approaches, including DNA-based molecular communication and advanced routing strategies, further enhance reliability, reduce latency, and mitigate congestion in IoBNT nanonetworks [4][8].

3.2.3. Bio-cyber interface layer

The bio-cyber interface layer bridges the gap between nano-scale biological systems and conventional digital infrastructure. It converts molecular or nanonetwork signals into digital data, aggregates and preprocesses inputs from multiple nano-scale sources, and translates high-level computational commands into nano-scale actuation instructions. This layer also ensures secure, authenticated data exchange between the biological and cyber domains. Signal conversion mechanisms may include bio-luminescent, protein-based, or AI-driven techniques that translate molecular interactions into electronic formats [20][41][42]. As a result, the layer enables seamless integration of intra-body nanonetworks with external communication

systems through electrical, electromagnetic, acoustic, or terahertz signals [13][18]. Neural-network-based interfaces further enhance interoperability and coherence between biological and digital systems [31].

3.2.4. Middleware layer

Above the interface layer, middleware abstracts the complexity of lower-level operations and provides standardized services for application development. It collects raw nano-scale and molecular data, processes it into actionable information, and translates it into conventional Internet-compatible formats. Middleware also enforces security and privacy through authentication, encryption, and access control tailored to sensitive biological data. By leveraging AI and ML, it supports advanced functions such as pattern recognition, anomaly detection, and predictive analytics. Additionally, it manages heterogeneous nano-scale devices, ensures interoperability, orchestrates system operations, and simplifies the deployment of IoBNT applications [31][41].

3.2.5. Edge layer

The edge layer connects bio-nano devices to the broader IoBNT infrastructure by operating close to the data source within biological or environmental contexts. It includes nano-sensors, actuators, and microscale bio-nano communication devices that capture biochemical, physiological, or environmental signals at the molecular or cellular level. This layer performs initial preprocessing steps, including filtering, noise reduction, aggregation, and normalization. It also supports local decision-making for time-critical actions, including triggering drug delivery or detecting pathogens. Designed for ultra-low-power operation, the edge layer relies on energy-harvesting mechanisms to enable autonomous, real-time functionality before transmitting data to higher layers [3][31][43-45].

3.2.6. Fog layer

Extending the capabilities of the edge layer, the fog layer provides distributed computing, storage, and networking closer to the data source. It aggregates and fuses data from multiple edge nodes, performs preliminary analytics to reduce latency and bandwidth usage, and temporarily stores relevant information. This layer supports real-time, context-aware processing and ML inference, enabling rapid decision-making in applications such as early disease detection. It also manages connectivity and routing between edge devices and the cloud while enforcing lightweight security mechanisms. By enhancing distributed intelligence and resource efficiency, fog computing plays a vital role in latency-sensitive IoBNT applications [31][43-45].

3.2.7. Cloud layer

At the top of the computational hierarchy, the cloud layer provides centralized, high-capacity resources for large-scale data processing and storage. It performs advanced analytics, including data mining and ML, to identify patterns, trends, and anomalies across aggregated bio-nano datasets. These capabilities support predictive modeling for disease progression, drug interactions, and environmental impacts. The cloud also enables system-wide orchestration, integration with healthcare and environmental platforms, and long-term data archiving for regulatory compliance and longitudinal studies. Additionally, cloud and off-chain databases support data synchronization, analytics, and secure access mechanisms in IoHT/IoT ecosystems [3][26][31][43-45].

3.2.8. Data storage layer

Complementing the cloud, the data storage layer ensures efficient management and retrieval of heterogeneous bio-nano data. It provides persistent storage for molecular signals, sensor readings, and biologically relevant information, enabling longitudinal analysis and cross-node data consolidation. The layer supports interoperability, allowing higher-level systems to access and interpret data regardless of format or origin. Security and privacy are maintained through encryption and anonymization techniques. IoBNT storage systems integrate conventional digital databases with emerging molecular storage technologies, such as DNA-based storage, protein memory, and nano-memory cells, enabling ultra-dense, long-term, and hierarchical data management [31].

3.2.9. Control and decision-making layer

The control and decision-making layer serves as the cognitive core of IoBNT, integrating sensing, analytics, and actuation into a unified intelligent framework. It interprets complex biological and environmental data, predicts system behavior, and coordinates responses across devices and applications. Using techniques such as ML, fuzzy logic, probabilistic modeling, and rule-based reasoning, the layer transforms raw data into actionable insights for real-time, adaptive decision-making. It

prioritizes tasks, triggers localized or distributed actions, and ensures safe, minimally invasive operations. Additionally, it enforces security, privacy, and regulatory compliance across the system [31].

3.2.10. Energy management systems layer

Supporting all operational layers, the energy management systems (EMS) layer ensures efficient and reliable power utilization in IoBNT environments. Given the constraints of nanoscale devices, EMS enables energy harvesting from biological sources, such as glucose, chemical gradients, or adenosine triphosphate, often via enzymatic biofuel cells. It also supports supplementary wireless energy transfer via electromagnetic induction or ultrasonic methods. By combining harvesting and transfer techniques, EMS maintains continuous operation while optimizing energy consumption through strategies such as duty cycling and energy-aware communication protocols. This layer is essential for sustaining long-term functionality and safe interaction with biological systems [42].

3.2.11. Application layer

At the top of the service stack, the application layer delivers user-facing services and decision-support systems by integrating IoBNT data into broader IoT ecosystems. It enables applications in healthcare, such as biomarker monitoring, early disease detection, targeted drug delivery, and remote patient management. Environmental monitoring applications benefit from molecular-level detection of toxins, pathogens, and pollutants, while industrial biotechnology applications support process monitoring in bioreactors. The layer also contributes to security and defense by detecting biological threats. By interfacing with users and AI systems, it provides real-time insights for advanced applications, including smart therapeutics and digital twins [3][31].

3.2.12. Management and control layer

Finally, the management and control layer oversees the entire IoBNT architecture, ensuring reliable, secure, and efficient system operation. It monitors network performance, optimizes energy usage, detects and mitigates faults, and enforces end-to-end security measures, including authentication, encryption, and access control. By coordinating network orchestration, lifecycle management, and compliance across all layers, it maintains system resilience and integrity. This cross-layer functionality is critical for ensuring safe and scalable deployment of IoBNT systems [41][46]. Figure 7 summarizes the layers of the IoBNT architecture.

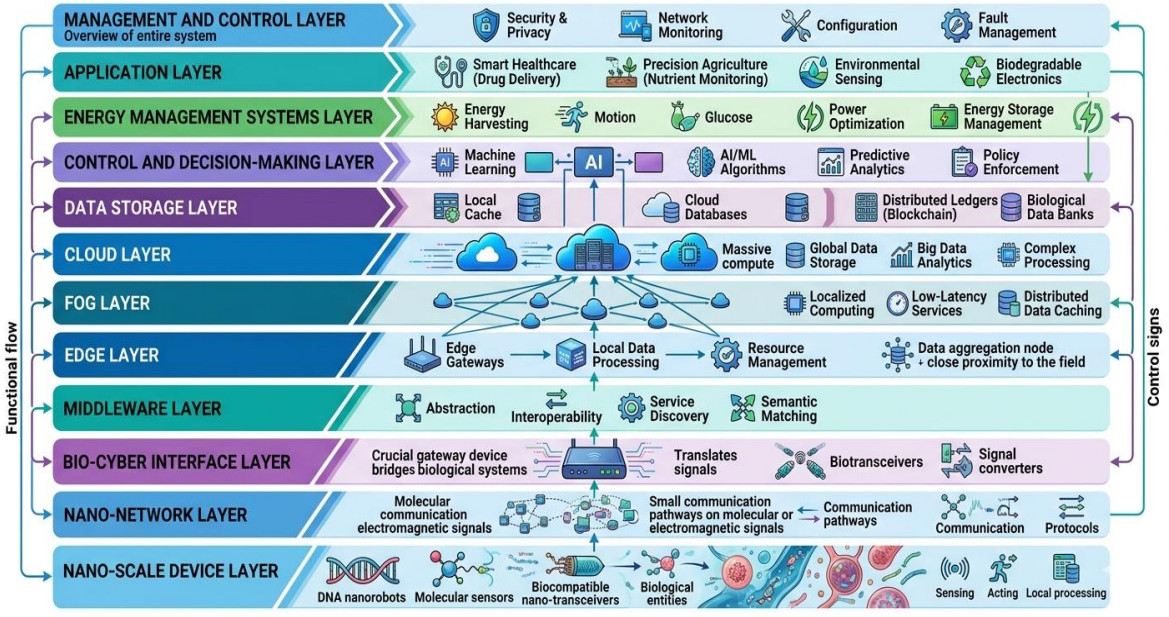


Fig. 7. Summarizes the layers of the IoBNT architecture.

3.3 IoBNT System Architecture Components

The IoBNT architecture consists of multiple interdependent layers and components that collectively ensure the system's functionality, each serving a distinct role in data collection, processing, communication, and system management. Below are the brief descriptions of these core components.

3.3.1. Bio-nano sensors

Bio-nano sensors serve as the primary data acquisition units in the IoBNT, operating at molecular, cellular, or nano-scale levels to detect biochemical, physical, and environmental signals. They convert these stimuli into measurable outputs, enabling real-time, in vivo monitoring of physiological parameters, disease biomarkers, and environmental toxins [11][31]. These sensors employ diverse transduction mechanisms, including electrochemical, optical, mechanical, and magnetic approaches. To achieve high sensitivity and selectivity, they incorporate advanced nanomaterials, such as graphene, carbon nanotubes, quantum dots, biocompatible polymers, and metallic nanoparticles, that are functionalized with bioreceptors such as antibodies, enzymes, and aptamers. When integrated into nano-scale networks, they support continuous monitoring and energy-efficient operation through molecular communication, electromagnetic nanonetworks, and bio-harvesting or ultra-low-power electronics.

3.3.2. Bio-nano actuators

Complementing bio-nano sensors, bio-nano actuators serve as effectors within the IoBNT, converting sensed signals into precise physical, chemical, or biological actions at the nano- or microscale. They enable autonomous or semi-autonomous interaction with biological systems, supporting applications such as targeted drug delivery, cellular modulation, and microenvironmental manipulation [5][31]. These actuators operate through mechanisms including chemical responsiveness to pH or enzymes, electrically or electrochemically induced motion, optical triggering for structural changes or cargo release, and magnetic or mechanical guidance. When integrated with sensing, communication, and control components, they translate real-time data into coordinated responses, advancing precision medicine, smart implants, regenerative therapies, and synthetic biology.

3.3.3. Nanonetwork (Intra-body/Inter-BNT)

Bio-nano devices operate within nanonetworks that enable coordinated sensing, communication, and actuation. These networks primarily rely on molecular communication, in which information is encoded in molecular type, concentration, or release timing and propagates via diffusion, advection, or transport processes, with reception mediated by ligand–receptor interactions [5][11]. In addition, hybrid approaches, such as graphene-based nano-electromagnetic antennas operating at THz frequencies, provide short-range, high-bandwidth communication. Intra-body nanonetworks function within a single organism to support real-time monitoring, targeted therapies, and cellular tracking. In contrast, inter-BNT networks connect multiple nanonetworks or external gateways, enabling multi-hop communication for coordinated tissue monitoring and remote diagnostics [9].

3.3.4. Nano micro/bio cyber interface

The nano–micro/bio–cyber interface connects nano-scale bio-devices with macroscale cyber systems by translating biochemical signals into electrical, optical, or electromagnetic forms and vice versa [9][16]. This interface incorporates technologies such as bioelectronic transducers (bioFETs), implantable chips, electronic tattoos, graphene-based sensors, and bioluminescent systems, often enhanced with ML for nonlinear signal processing. It aggregates and preprocesses data from nanonetwork nodes, enables protocol translation, and converts cyber-level commands into nano-scale actuation. By integrating transducers, gateways, edge computing, and lightweight security modules, it facilitates bidirectional, low-latency communication and supports applications in personalized medicine, environmental monitoring, and industrial bioengineering.

3.3.5. Gateways and controllers

Gateways and controllers form the communication and control backbone of the IoBNT, linking bio-nano devices with higher-level computational systems. Gateways translate biochemical or molecular signals into digital, electrical, or optical formats, while also aggregating data, reducing noise, performing protocol conversion (e.g., TCP/IP or MQTT), and enforcing local security measures such as encryption and access control [47]. Controllers manage network topology, allocate resources, coordinate device operations, and issue actuation commands, including targeted drug release. By

leveraging AI and ML for data analysis, controllers enable real-time decision-making, enhance communication reliability, and enforce system-wide security [9].

3.3.6. Nano-network interfaces

Nano-network interfaces facilitate efficient communication among bio-nano devices and across nano-, micro-, and macro-scale systems. They support multiple communication modalities, including molecular, electromagnetic, acoustic, and hybrid approaches, while addressing challenges such as limited energy, signal attenuation, interference, latency, and reliability [48]. These interfaces convert biochemical signals into digital or electromagnetic forms, adapt communication protocols for heterogeneous environments, and enable bidirectional interaction through embedded sensors and actuators [16]. Their energy-efficient designs, combined with routing, data aggregation, and lightweight security mechanisms, support applications such as in vivo monitoring, targeted drug delivery, and real-time environmental sensing.

3.3.7. Cloud and edge integration

Cloud and edge computing provide the computational and storage foundation for the IoBNT, enabling scalable, intelligent data processing across different system layers. Edge nodes, positioned close to bio-nano devices, handle real-time preprocessing, noise reduction, and low-latency decision-making, all of which are essential for time-sensitive applications such as medical interventions and environmental hazard detection. In contrast, cloud platforms offer high-performance computing, large-scale analytics, ML capabilities, long-term data storage, and integration with external systems such as electronic health records [10][31]. Through hierarchical communication and hybrid computation, the system distributes lightweight tasks to the edge while reserving intensive processing for the cloud, transforming raw biochemical data into actionable insights for both immediate response and long-term analysis. Figure 8 illustrates the components of the IoBNT architecture.

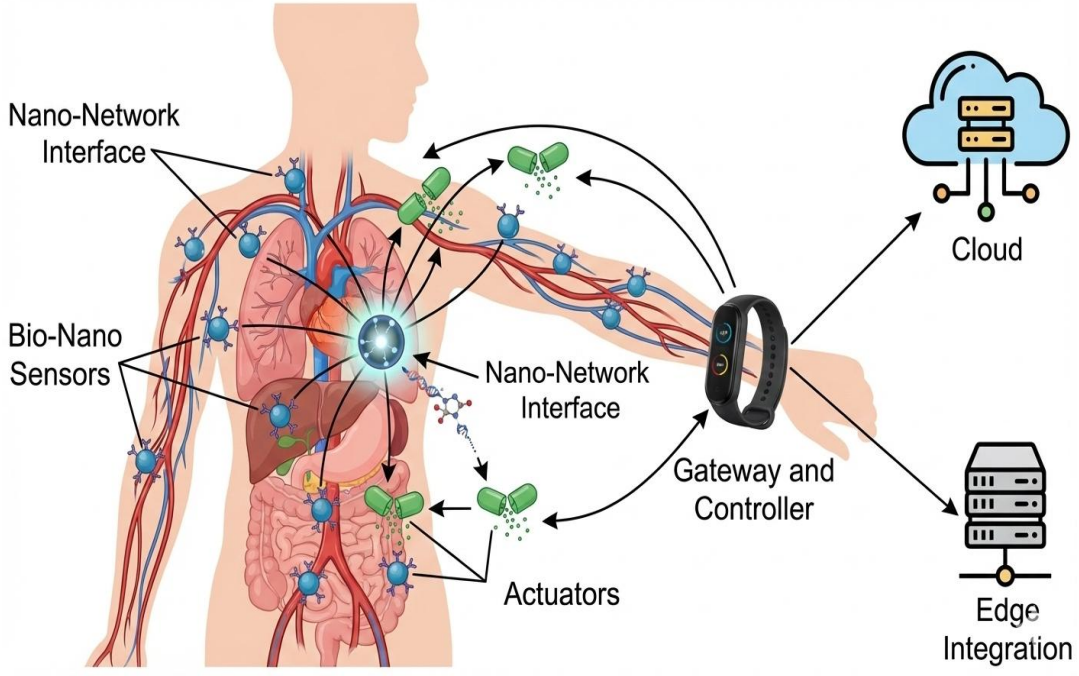


Fig. 8. Illustrates the components of the IoBNT architecture.

3.4. Communication Paradigms in IoBNT

IoBNT communication integrates molecular and non-molecular physical layers with hybrid bio–cyber gateways that translate nano-scale biological signals into formats compatible with conventional networks. Within this framework, IoBNT primarily relies on communication paradigms, each of which enables information exchange across different spatial scales and biological–cyber interfaces while supporting seamless interoperability between nano-bio systems and external digital infrastructures. Below are brief descriptions of principal communication paradigms used in IoBNT.

3.4.1. Molecular communication

Molecular communication enables bio-nanodevices in IoBNT to exchange information through the release, propagation, and detection of chemical signals. Transmitters encode data into molecules, such as ions, proteins, DNA, or synthetic compounds, by modulating their type, concentration, timing, or spatial distribution. These molecules propagate via diffusion, drift (e.g., blood flow), or a combination of both, mirroring natural biological signaling processes. Receivers equipped with biochemical receptors or nanosensors detect these signals and convert them into measurable outputs, making this paradigm suitable for nano-scale environments where electromagnetic communication is ineffective or unsafe [34]. Within IoBNT, molecular communication can be categorized by its physical mechanisms. Diffusion-based communication relies on random motion and concentration gradients, offering energy efficiency for short-range signaling but introducing latency, stochastic variability, and security risks, including eavesdropping and tampering [49]. In contrast, active transport mechanisms use energy-driven carriers, such as motor proteins, bacteria, or engineered nanovehicles, to improve directionality and reliability. However, they remain vulnerable to interception and pathway disruption [18]. Biochemical signaling further enhances this paradigm through ligand–receptor interactions, gene regulation, and synthetic biological circuits, enabling high specificity and programmability while facing challenges such as off-target effects, molecular mimicry, and susceptibility to mutation or interference [30][33].

3.4.2. Electromagnetic (EM)-based terahertz communication

Electromagnetic terahertz (THz) communication operates in the 0.1–10 THz band and enables high-speed, short-range data exchange among nano-machines and external systems [50]. Graphene-based and plasmonic nano-antennas support compact, low-power implementations suitable for nano-scale environments. However, tissue absorption, scattering, and severe path loss significantly constrain performance. To mitigate these limitations, multi-hop routing and cooperative communication protocols enhance link reliability. This paradigm provides high bandwidth and precise synchronization but faces challenges related to attenuation, limited power budgets, and biocompatibility. Security mechanisms such as frequency hopping, waveform shaping, device fingerprinting, and hierarchical architectures help reduce vulnerabilities [51].

3.4.3. Bio-electrical and ionic communication

Bio-electrical and ionic communication leverages endogenous biological processes to transmit information through ion fluxes and membrane potentials, including action potentials, graded potentials, and ionic currents [52]. Synthetic platforms, such as synaptic transistors and ionic-junction fibers, enable low-voltage and tissue-compatible operation for neuromodulation, sensing, and hybrid bioelectronic systems. In this paradigm, information is encoded in ion gradients, temporal dynamics, or ion species, closely mimicking natural signaling such as Ca^{2+} dynamics. While these approaches provide high temporal precision and low-latency actuation, they are limited by short communication ranges, potential interference with native physiology, and device complexity. Security strategies, therefore, emphasize biochemically grounded authentication, adaptive filtering, and context-aware anomaly detection [11][33].

3.4.4. FRET and optical nano-scale signaling

At the molecular scale, FRET enables non-radiative energy transfer between donor and acceptor fluorophores over distances of approximately 1–10 nm. Its efficiency is governed by:

$$E = \frac{1}{1 + \left(\frac{r}{R_0}\right)^6}$$

where R_0 depend on spectral overlap, quantum yield, dipole orientation, and refractive index [53]. This mechanism supports ultrafast signaling in the picosecond–nanosecond range, making it well-suited for localized sensing and diagnostics. Integration with plasmonic nanostructures, nanoparticles, and photonic waveguides extends communication range and improves directionality and efficiency [54][55]. However, performance is constrained by fluorophore lifetime, photobleaching, scattering, autofluorescence, and refractive index variability. Security concerns include optical eavesdropping, spectral interference, and detector cloning, although fluorophore-based encoding can support authentication strategies [46][48].

3.4.5. Neural/spike-based biochannels

Neural or spike-based biochannels transmit information via action potentials and synaptic plasticity, with memristors and artificial synapses that replicate biological learning and memory processes [56]. Mechanisms such as spike-timing-dependent plasticity improve communication efficiency and mutual information transfer. These channels underpin

neuromorphic systems and brain-inspired computing, enabling integration of neural tissue into IoBNT frameworks [12][57]. Despite their advantages, they introduce significant security and privacy risks, including exposure of cognitive data, malicious stimulation, malware injection, and DoS attacks. Mitigation strategies focus on local preprocessing, encryption, authenticated stimulation, anomaly detection, and hardware-level protections.

3.4.6. Hybrid architectures and bio–cyber gateways

Hybrid architectures integrate molecular, electrical, electromagnetic, and optical communication paradigms to connect biological nanonetworks with cyber-physical systems [58]. Bio–cyber gateways translate nano-scale biological signals into digital formats, enabling advanced healthcare and diagnostic applications. Within this framework, spike-based biochannels contribute high temporal precision, rapid signaling, and efficient information encoding. However, these gateways also concentrate security vulnerabilities, as protocol translation can expose sensitive physiological data and expand attack surfaces. Ensuring integrity, authenticity, and non-repudiation remains challenging due to biological variability and device heterogeneity, which complicate the application of conventional cybersecurity approaches. Figure 9 illustrates the principal communication paradigms used in IoBNT.

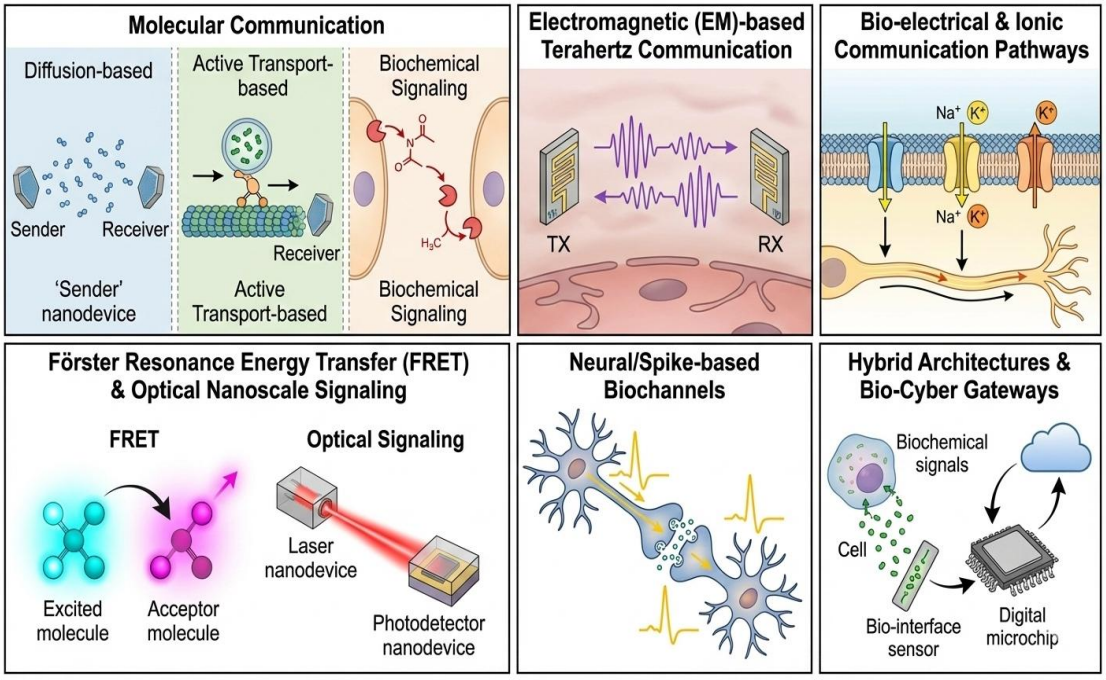


Fig. 9. Illustrates the principal communication paradigms used in IoBNT.

3.5 IoBNT Communication Models

Recent research identifies several foundational communication models in the IoBNT, each employing distinct mechanisms to facilitate information exchange among biological and artificial nano-scale devices. Below are the communication models in IoBNT.

3.5.1. Molecular communication

Molecular communication is a core paradigm in the IoBNT, enabling bio-nanomachines to encode, transmit, and receive information via chemical or biochemical signals. This approach offers strong biocompatibility, low energy consumption, and natural integration with living systems [4][8][15][40]. Information transmission occurs via diffusion, advection, active transport, or carrier-mediated mechanisms, with transmitters encoding data through the controlled release, synthesis, or activation of signaling molecules, and receivers decoding it via receptors or catalytic interactions. Diffusion-based channels are simple but suffer from stochastic delays and intersymbol interference. To address these limitations, alternative approaches, such as flow-assisted, motor-driven, and bacteria-mediated transport, enhance directionality and range. Encoding schemes include concentration-shift keying, molecule-shift keying, timing-based modulation, and reaction-based methods, often aligning with natural biological processes such as hormone signaling and quorum sensing. Recent advances,

including MIMO techniques, DNA-based transport, and ML-assisted detection, improve reliability and enable complex network topologies, though inherent low data rates and delays motivate complementary high-speed communication strategies.

3.5.2. Electromagnetic nano-scale communication

Electromagnetic nanoscale communication enables nanoscale and microscale devices to exchange information via electromagnetic signals, offering higher data rates, lower latency, and improved integration with external cyber systems compared to molecular approaches [42]. These systems typically operate in the THz band and rely on advanced materials such as graphene and carbon nanotubes to implement miniaturized antennas and plasmonic structures. Nano-transmitters and receivers use components including plasmonic oscillators, quantum-dot emitters, nano-rectennas, and photodetectors, while energy-efficient techniques such as duty cycling and hybrid modulation address power constraints. However, signal propagation in biological environments is limited by absorption, scattering, and short transmission ranges. Despite these challenges, THz communication can achieve gigabit-per-second data rates and sub-millisecond latency, supporting real-time sensing, rapid coordination, and hybrid networking [59]. Applications span in-body diagnostics, smart drug delivery, and neural interfaces, with energy supplied through biochemical harvesting or wireless transfer. While electromagnetic communication excels in speed and bandwidth, it complements rather than replaces biologically native chemical signaling.

3.5.3. Chemical signaling

Chemical signaling encodes information using biochemical molecules, including ions, hormones, peptides, neurotransmitters, and synthetic compounds [16]. In this paradigm, nano-machines modulate properties such as concentration, molecular type, structure, and release timing to convey information. At the same time, receptors decode signals via selective binding, ion channels, or chemical-sensing mechanisms. Signal propagation occurs via diffusion, fluid flow, or active transport, often introducing stochastic delays and noise. Despite these constraints, chemical signaling provides high biocompatibility, low energy requirements, and seamless integration with biological pathways, enabling direct interaction with cellular processes. It supports multiple encoding strategies, including concentration-, type-, temporal-, and gradient-based schemes, and underpins applications such as targeted drug delivery, distributed biosensing, and engineered cellular networks. However, challenges related to low data rates, interference, complex modeling, and biochemical security risks persist [42], reinforcing the need for complementary communication modalities.

3.5.4. Multi-modal communication frameworks

Multi-modal communication frameworks combine molecular, electromagnetic, acoustic, electrical, or thermal signaling mechanisms to enable adaptive and context-aware communication in bio-nano networks [11][18]. By leveraging the complementary strengths of each modality, these systems use molecular communication for energy-efficient in-body signaling and high-speed channels such as THz or acoustic links for rapid data exchange. Modular transceivers and cross-domain gateways facilitate signal conversion, fusion, synchronization, and error correction across heterogeneous channels. Bio-nano devices can dynamically switch between modalities based on environmental conditions, energy availability, and application requirements, while cross-layer integration enhances signal detection, classification, and prioritization. Hybrid combinations, such as molecular–electromagnetic or molecular–acoustic systems, enhance reliability, data rates, and localization capabilities. Despite these advantages, challenges remain in modeling cross-modal interactions, optimizing energy use and miniaturization, ensuring security, and designing stable coordination protocols [11][17].

4. CYBERSECURITY THREATS, ATTACKS, AND CHALLENGES IN IOBNT

IoBNT enables seamless interaction among bio-nano devices and external networks, creating new capabilities for real-time diagnostics, targeted therapies, and intelligent biomedical applications. However, it also exposes bio-nano infrastructures to novel cybersecurity threats and attack vectors. Table 1 briefly describes the cybersecurity threats, attacks, and challenges in IoBNT.

TABLE I. BRIEF DESCRIPTIONS OF THE CYBERSECURITY THREATS, ATTACKS, AND CHALLENGES IN IOBNT.

S/No	Cybersecurity threats, attacks, and challenges	Brief descriptions	References
1	Data breaches and privacy violations	IoBNT data breaches occur when attackers exploit weak communication channels, compromised nano-devices, or insecure cloud storage, exposing sensitive biological information. Breaches can reveal health records, genomic data, and biochemical readings, creating severe privacy risks.	[60-62]
2	Unauthorized actuation and physiological manipulation	Attackers can remotely trigger bio-nano devices via weak authentication or insecure channels, causing harmful actions like incorrect drug release. Physiological manipulation, such as the injection of false biosignals, can disrupt hormonal, neurological, or cardiovascular systems.	[61-63]
3	Privilege escalation	Exploiting device vulnerabilities allows attackers to gain unauthorized control, manipulate data, and disrupt medical treatments. Resource-limited devices, unpatched firmware, and heterogeneous networks amplify the risk of such attacks.	[61-63]
4	Authentication and authorization attack	Weak authentication enables device impersonation, credential theft, and access-control bypass, potentially leading to incorrect diagnoses or harmful interventions. Extreme resource constraints and dynamic biological environments complicate mitigation in IoBNT systems.	[64][65]
5	Chemical impersonation	Attackers can inject counterfeit chemical signals to spoof molecular communication, mislead devices, or alter biological responses. Noisy channels and limited molecular-level authentication make mitigation challenging.	[18][66]
6	Molecular eavesdropping	Unauthorized interception of biochemical signals allows attackers to infer sensitive information, inject false signals, or disrupt networks. Open molecular channels and limited device capabilities heighten the privacy risk.	[18][66]
7	Molecular jamming	Attackers distort molecular communications by injecting interfering molecules, lowering signal-to-noise ratios, and corrupting messages. Timing-based attacks can desynchronize transmission, compromising critical medical functions.	[18][66]
8	Denial-of-service (DoS) and distributed DoS (DDoS) attacks	Flooding bio-nano devices or channels exhausts energy and bandwidth, delaying or blocking biomarker data and control messages. Lightweight protocols and botnet coordination further amplify risks across heterogeneous IoBNT architectures.	[60-62]
9	Molecular replay attacks	Attackers capture and reintroduce legitimate molecular signals, causing devices to misinterpret outdated information. Replay attacks can trigger incorrect drug release or false physiological readings, thereby challenging molecular-level authentication.	[66]
10	Man-in-the-Middle (MitM) attacks	Interception or injection of molecular or THz signals enables attackers to manipulate sensitive data or control devices. Limited computational power and subtle molecular communications hinder detection.	[66]
11	Molecular signal tampering	Deliberate alteration of molecular signals compromises device operations and data integrity. Detection is difficult due to stochastic behavior and resource-constrained bio-nano devices.	[18][12]
12	Nano-device cloning and impersonation	Cloned or impersonated devices gain unauthorized network access, manipulate physiological data, or hijack drug-delivery nanobots. Device heterogeneity and limited authentication capabilities make mitigation challenging.	[67]
13	Nano-malware injection and propagation	Nano-malware exploits wireless channels or compromised sensors to manipulate device functionality and propagate across bio-integrated systems. Resource constraints and stealthy operation make detection and mitigation extremely difficult.	[12][18]
14	Nano-scale physical tampering	Physical manipulation at the molecular or cellular level compromises device integrity and patient safety. Detecting tampering is difficult due to device size, biological integration, and limited computational capacity.	[12]
15	Node capture attacks	Attackers can physically or remotely capture nodes, extract sensitive data, or manipulate functions. Compromised nodes facilitate broader network attacks, highlighting the risks of limited secure key storage.	[12]
16	Biological hijacking and behavioral manipulation	Hijacking bio-nano devices enables attackers to manipulate physiology or behavior via neural, hormonal, or cellular pathways. Such attacks pose direct safety risks and create hybrid cyber-biological threats.	[68]
17	Identity spoofing attack	Attackers spoof device identities to access data or issue false commands, exploiting limited processing power and dynamic network topologies. Spoofing threatens patient safety and system integrity.	[18][66]
18	Side-channel attacks	Unintended emissions from nano-devices reveal sensitive information without breaking algorithms. Timing, power, electromagnetic, or chemical signals allow attackers to infer health data or therapeutic schedules.	[18][69]
19	Signal tampering	Manipulating molecular or electromagnetic signals can cause false readings or unintended device activation. Weak nano-scale signals and biocompatibility requirements complicate detection and defense.	[70]
20	Molecular spoofing	Introducing counterfeit molecules tricks devices into producing false readings or triggering false actions, disrupting drug delivery or immune responses. Molecular spoofing evades conventional cybersecurity and threatens molecular communication channels.	[11][18]

21	Black hole attack	Malicious nodes attract and drop all data packets, preventing them from reaching their destinations. Limited resources and dynamic topologies make detection and mitigation challenging, threatening patient safety.	[18]
22	Sinkhole attack	Attackers falsely advertise optimal routes, attracting traffic to drop, alter, or delay data. These attacks disrupt medical nano-devices and environmental bio-networks, compromising confidentiality and availability.	[70]
23	Wormhole attack	Packets are captured at one point in the network and replayed elsewhere, creating false proximity illusions. Wormholes disrupt routing, intercept data, and compromise therapeutic commands.	[18]
24	Zero-day attack	Unknown device or protocol vulnerabilities allow attackers to compromise IoBNT systems before patches are applied. Heterogeneous architectures and complex biological interactions increase susceptibility.	[18]
25	Sybil attack	Malicious nodes create multiple fake identities to manipulate data or dominate networks. Limited authentication and indistinguishable chemical signals amplify risks in IoBNT systems.	[47]
26	Data poisoning attack	Attackers manipulate operational or training data to corrupt machine-learning models. False biochemical signals can cause incorrect drug delivery, misdiagnoses, or compromised federated learning (FL) models.	[71]
27	Fake node insertion	Unauthorized nodes masquerade as legitimate devices, intercepting or manipulating molecular signals. Fake nodes disrupt communication, data integrity, and network reliability, serving as precursors to other attacks.	[9][47]
28	Collusion attacks	Multiple compromised devices coordinate to manipulate network behavior, interfere with sensing, or produce false consensus. Collusion threatens medical, environmental, and FL applications.	[71]
29	Selective forwarding attack	Compromised nodes forward some packets while dropping others, subtly disrupting communication. Multi-hop molecular networks and resource constraints make detection difficult, compromising medical safety and data integrity.	[9][47]
30	Malicious code injection attack	Unauthorized code injected into bio-nano devices or molecular channels alters device behavior and biochemical processes. Consequences include misdiagnosis, tissue damage, and manipulated drug release.	[47]
31	Multi-scale coordinated attacks	Attackers exploit vulnerabilities across nano, micro, network, and cloud layers simultaneously. Layered attacks distort biological functions, drug delivery, or diagnostics while remaining hard to detect.	[9][71]
32	Cross-domain cyber-bio attacks	Attackers manipulate bio-digital feedback loops to falsify data, embed malware, or alter device behavior. These attacks threaten health, cause cascading effects, and challenge detection across cyber-bio interfaces.	[16][72]
33	Location tracking	Adversaries infer health conditions or device positions by analyzing molecular, electromagnetic, or chemical signals. Predictable biological environments and immature molecular security increase exposure risks.	[12][18]
34	On-off attack	Malicious nodes alternate between normal and malicious behavior to evade detection. Intermittent false readings or packet drops strain detection systems in energy-constrained networks.	[9][73]
35	Profile inference attack	Analyzing molecular or physiological signals allows attackers to reconstruct sensitive individual profiles. Continuous nano-sensing and heterogeneous channels enable detailed profiling without direct identifiers.	[12]
36	Artificial immune evasion	Attackers mimic or obfuscate biochemical cues to bypass artificial immune mechanisms. Stealthy behavior enables attacks on drug-delivery nanobots, surveillance systems, and synthetic immune controllers.	[68]
37	Bad-mouthing	Compromised nodes spread false reports about other nodes, undermining trust and disrupting coordination. False or biased reporting can isolate healthy nodes and bias biological or clinical decisions.	[9][73]
38	Ballot stuffing	Attackers inject fake or duplicate bio-nano signals to mislead majority-based aggregation, which can trigger premature drug release, false diagnostics, or undue influence on network decisions.	[9]
39	Environmental manipulation attacks	Attackers alter chemical, pH, temperature, or electromagnetic conditions to disrupt sensing, communication, or actuation. Such manipulations mimic natural variability, threatening patient safety and system integrity.	[12][18]
40	Hybrid cyber-bio interfaces	Bidirectional cyber-bio interfaces create attack surfaces in which digital intrusions manipulate biology and biological signals compromise cyber systems. Limited resources and non-deterministic biology complicate detection and defense.	[73]
41	Service degradation attack	Subtle attacks reduce communication performance without fully disabling devices. Energy constraints, signal interference, or protocol flaws delay or distort biological data transmission.	[12][18]
42	Biochemical channel degradation	Attackers disrupt molecular communication via enzymatic cleavage, chemical noise, or environmental manipulation. Such degradation can induce DoS attacks, spoofing, or erroneous signal interpretation.	[12][18]

43	Biocompatibility exploitation	Adversaries exploit biocompatibility by triggering immune responses, hijacking communication, or embedding Trojan nano-devices. These threats compromise safety, data integrity, and therapeutic efficacy.	[9][68]
44	Cascading bio-nano system failures	Faults in one device can propagate across interconnected systems, causing escalating clinical or physiological harm. Nonlinear biological feedback and rapid response requirements amplify these cascading failures.	[9[12][18]
45	Toxic nano-agents	Malicious nano-agents manipulate payloads, poison communication channels, or impersonate devices to induce cellular or organ damage. Detection is difficult, while regulatory frameworks remain inadequate.	[9][68]
46	Unpredictable biological environment challenges	Dynamic physiological conditions, such as fluctuations in pH or blood flow, can alter device behavior and enable attacks. Environmental perturbations and biomolecular interactions threaten the stability and reliability of IoBNT.	[9][18]
47	Manipulation of biochemical patterns	Attackers alter hormones, proteins, or metabolites to trigger unintended biological responses or disrupt device functions. Detection is challenging due to biological complexity and device limitations.	[68]
48	Resource exhaustion and energy depletion	Flooding, computation-intensive requests, or environmental interference deplete the energy and memory of nano-devices. Resource exhaustion can shut down devices, compromise patient safety, and enable DoS attacks.	[9][12][18]

5. SECURITY IN IOBNT

Security in IoBNT is a rapidly evolving field that addresses unique threats at the intersection of nanotechnology, biology, and cyber-physical systems.

5.1.Security Requirements in IoBNT

Traditional cybersecurity mechanisms for classical IoT fail to fully protect IoBNT because nano-devices face severe constraints in computation, energy, and memory when interacting with biological systems. This bio-integration amplifies risks to data confidentiality, integrity, authenticity, and patient safety, requiring security frameworks tailored to bio-nano environments that address biocompatibility, non-invasiveness, and resilience to biological variability [47]. Securing IoBNT, therefore, demands security frameworks that extend beyond conventional cybersecurity principles to address bio-nano–specific requirements, including biocompatibility, non-invasiveness, and resilience to biological variability. Rigorous, context-aware security models are essential for safe and ethical IoBNT deployment. Below are detailed descriptions of key security requirements in IoBNT.

- *Privacy*: IoBNT privacy safeguards sensitive biological, medical, and genetic data from unauthorized access or misuse. Techniques such as strong encryption, access control, anonymization, and blockchain ensure data remains confidential while supporting secure processing and sharing [74].
- *Confidentiality*: Ensures that only authorized entities access bio-nano data, including DNA sequences, biomarkers, and neural signals. Lightweight cryptography, secure aggregation, end-to-end encryption, and authentication protect against interception and unauthorized disclosure [74].
- *Integrity*: Maintains accurate, consistent, and unaltered bio-nano data for safe medical operations. Mechanisms such as cryptographic hashes, digital signatures, and blockchain technologies detect tampering and correct errors, ensuring reliable therapeutic actions [74].
- *Availability*: Guarantees continuous access to IoBNT devices and data for timely health monitoring and interventions. Redundancy, fault-tolerant designs, and energy-efficient protocols sustain operations under attacks and adverse conditions [74].
- *Authentication*: Verifies the identities of devices and entities, preventing impersonation and malicious control. Methods include biometrics, molecular tagging, and lightweight cryptography, securing targeted drug delivery and neural interfaces [74][75].
- *Authorization*: Enforces which actions authenticated users or devices can perform, preventing unauthorized manipulation of bio-nano devices. Role-based, context-aware access control and smart contracts manage dynamic permissions while complying with regulations like HIPAA and GDPR [47].
- *Trustworthiness*: Ensures devices, data, and communication channels operate reliably and securely. Blockchain, anomaly detection, and secure attestation enhance patient safety and ethical compliance, fostering confidence in IoBNT systems [76].
- *Scalability*: Supports secure operation as the number and heterogeneity of devices grow. Lightweight cryptography, edge computing, and blockchain-based authentication maintain security across large, dynamic IoBNT networks [74][75].

- *Accountability*: Traces user or device actions to their origins, deterring misuse. Secure identity management, tamper-proof logging, and behavioral monitoring help detect malfunctions or unauthorized access in critical biomedical applications [9][77].
- *Auditability*: Allows systematic review and verification of IoBNT operations and data. Tamper-proof logs, timestamps, regulatory checks, and anomaly detection enable transparency, compliance, and anomaly identification [78].
- *Interoperability*: Enables diverse bio-nano devices and systems to communicate securely across platforms. Standardized protocols preserve privacy, integrity, and coordinated functionality despite device heterogeneity [9][77][79].
- *Non-repudiation*: Provides verifiable proof of message origin and actions. Digital signatures, secure audit logs, and blockchain prevent denial of medical interventions or data operations, maintaining trust in IoBNT systems [78].
- *Access control*: Regulates interactions with sensitive bio-nano resources. Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and capability-based models enforce authentication, authorization, and accountability in dynamic, resource-limited environments [64].
- *Anonymity*: Conceals device and user identities, protecting personal physiological data. Techniques like pseudonymization, multi-hop routing, differential privacy, and privacy-preserving authentication mitigate targeted attacks while enabling secure data use [78].
- *Resiliency*: Enables IoBNT systems to maintain secure operations under failures, attacks, or disruptions. Redundancy, adaptive recovery, and self-healing mechanisms ensure continuity of drug delivery and health monitoring [77][80].
- *Reliability*: Ensures consistent, accurate bio-nano network performance and secure data transmission. Error correction, fault-tolerant protocols, and timely communication uphold reliability in critical biomedical applications [77][80].
- *Fault tolerance*: Enables correct operation despite device or system failures. Redundancy, self-healing networks, error detection, and distributed consensus prevent single points of failure in critical healthcare applications [9].
- *Robustness*: Ensures devices and protocols function reliably despite disturbances, uncertainties, or attacks. Redundant designs, error-tolerant encoding, and deep-learning anomaly detection maintain trustworthy operation under dynamic biological conditions [9][81].
- *Freshness*: Guarantees that data and cryptographic exchanges are recent and not replayed. Timestamps, sequence numbers, and ephemeral biochemical markers prevent harmful responses to stale or replayed messages [81-83].
- *Forward secrecy*: Ensures past session data remains secure even if long-term keys are compromised. Ephemeral session keys and lightweight key-exchange protocols protect ongoing IoBNT communications [81-83].
- *Backward secrecy* protects historical data even when new or compromised nodes join the network. Frequent key updates and session-based cryptography prevent access to past communications, preserving confidentiality [81-83].

Revocation: Removes compromised or unauthorized devices promptly. Mechanisms include key disabling, biochemical self-deactivation, and consensus-based isolation, ensuring safe and secure network operation [81][83].

5.2. Security Protocols for IoBNT

Security protocols in the IoBNT protect communication, control, and data integrity across bio-engineered nano-devices, micro-interfaces, and conventional cyber systems. These protocols ensure confidentiality by preventing unauthorized access to sensitive biological data, preserve integrity by protecting molecular and biochemical signals from tampering, and authenticate bio-nano devices before communication. They also maintain availability despite environmental noise, biological interference, or malicious attacks, while remaining lightweight and biocompatible to avoid disrupting living tissues. Below are the descriptions of the security protocols in IoBNT.

5.2.1. Lightweight cryptographic protocols

Lightweight cryptographic protocols are essential for securing IoBNT systems under strict constraints on computation, energy, and memory. They prioritize low complexity, small key sizes, and reduced latency to support nano- and molecular-scale communication. To achieve efficiency, they rely mainly on symmetric encryption, physically unclonable functions (PUFs), and biologically inspired primitives rather than heavy public-key cryptography. Resource-intensive operations such as ECC are typically offloaded to edge or gateway devices to reduce the burden on nano-devices. Efficient algorithms like PRESENT, SIMON, SPECK, RECTANGLE, TinyAES, and ChaCha20 use simple operations such as XOR and

rotations to ensure confidentiality and authentication, while lightweight MACs and hash functions (e.g., SPONGENT, PHOTON, QUARK) maintain integrity and authenticity. These approaches reduce energy consumption by approximately 30–58% compared to AES/ECC while maintaining secure communication and authentication [29][84][85].

5.2.2. Authentication and access control

Authentication and access control in IoBNT ensure that only authorized entities can interact with bio-nano devices while maintaining lightweight operation and biological compatibility. Authentication is achieved through symmetric cryptography, PUF-based challenge–response mechanisms, and biochemical signatures. Access control enforces the principle of least privilege using RBAC, ABAC, and context-aware policies tailored to physiological and environmental conditions. Recent frameworks integrate ECC-based methods with multi-factor authentication, combining biometrics, passwords, smart cards, and PKI to reduce latency and overhead in medical and sensor systems [74]. Emerging molecular approaches enhance security through DNA, peptides, and polymers used as nano-scale molecular tags verified by nanosensors and programmable DNA systems [37]. Additionally, biochemical identifiers and nanoscale challenge–response systems that use enzymatic or optical reactions strengthen resistance to replay and spoofing attacks.

5.2.3. Secure molecular communication protocols

Secure molecular communication protocols protect IoBNT data transmission by ensuring confidentiality, integrity, and authenticity in noisy, biologically complex environments. These protocols integrate molecular encryption, authentication tags, error detection, and access control while operating under strict energy constraints. However, diffusion-based communication remains vulnerable to attacks such as jamming, eavesdropping, spoofing, and MitM attacks, depending on the propagation mechanisms [66]. Information-theoretic models and wiretap-based approaches establish secure transmission limits for molecular channels [86]. DNA-based encryption techniques introduce programmable molecular locks and modular codebooks to improve robustness [87]. To further enhance reliability, noise-resilient encoding and error-correction techniques such as Self-Orthogonal Convolution Codes (SOCC), Low-Density Parity Check (LDPC), and Hamming codes reduce diffusion-related errors and improve communication stability [88].

5.2.4. Trust management in nano-networks

Trust management in nano-networks enhances cooperation among bio-nano devices by evaluating behavioral evidence rather than relying solely on cryptography. It dynamically adjusts trust scores based on interaction reliability, communication success, and contextual factors. This approach improves resilience against data falsification, replay, and message-dropping attacks in IoBNT environments. Blockchain-based models provide decentralized trust, access control, and reputation management while reducing single points of failure [24][74]. Zero-trust frameworks further integrate blockchain with encryption methods to enable context-aware authorization and reduce latency. In addition, AI-driven and agent-based models compute real-time trust scores, supporting adaptive decision-making and improving intrusion detection and service selection [89][90].

5.2.5. Privacy-preserving techniques

Privacy-preserving techniques in IoBNT protect sensitive biological and physiological data by ensuring confidentiality, anonymity, and minimal exposure during processing and sharing. These methods integrate cryptographic mechanisms, trust management, and data minimization strategies. Certificateless lattice-based ring signatures provide anonymity and post-quantum security without relying on traditional certificate systems [91]. Differential privacy introduces controlled noise to preserve data utility while limiting data leakage, and is often combined with k-anonymity to achieve a better balance [92][93]. Data sharing is further secured using FL, homomorphic encryption, and secure multi-party computation in decentralized environments ([114]). Additionally, IDS based on Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) models enhances real-time protection with high accuracy and low latency [5].

5.2.6. Quantum and physical-layer security protocols

Quantum and physical-layer security protocols enhance IoBNT protection by leveraging quantum properties and molecular channel characteristics. The Quantum Bacterial Nanonetworks (QBaN) protocol uses quantum entanglement and entropy-based detection to identify eavesdropping while maintaining energy efficiency [94]. Physical-layer security techniques exploit channel randomness and molecular properties to provide information-theoretic secrecy and keyless encryption [46]. These methods are supported by biomolecular encoding and experimental prototypes that demonstrate secure molecular transmission [95]. To address emerging threats, quantum-resistant approaches, such as lattice-based cryptography, ensure post-quantum security in resource-constrained environments [91][92]. However, secure integration of molecular systems with external networks remains an open research challenge [16][18].

5.2.7. Cryptographic and authentication protocols

Recent cryptographic and authentication protocols for IoBNT emphasize lightweight and hybrid security mechanisms to balance efficiency and protection. Hybrid schemes combining ECC, hash functions, and XOR operations provide secure yet resource-efficient authentication [81]. Smart contract–based authentication enhances security in emerging 6G-enabled IoNMT systems while reducing latency and energy use [83]. Bio-molecular cryptography further strengthens security by encoding information using DNA and protein structures for molecular communication systems [96]. DNA-based schemes integrate ECC-derived keys to ensure confidentiality and integrity under strict constraints [22]. Additionally, multi-factor and post-quantum authentication frameworks improve resistance against replay, MitM, and brute-force attacks in IoT and IoMT environments [65].

5.2.8. Bio-cyber interface and privacy schemes

Bio-cyber interface and privacy schemes ensure secure interaction between biological systems and computational networks in IoBNT. A privacy-preserving scheme using chaotic systems and BPSK modulation enhances patient data security while maintaining system performance [72]. Non-invasive capacitive sensing enables high-speed molecular signal recovery but currently lacks integrated security and access control mechanisms [16]. To address this gap, AI-edge frameworks combine CNNs, LSTMs, and trust-aware controllers to support dynamic access decisions [97]. Federated learning with differential privacy and homomorphic encryption further supports secure decentralized model training [89]. In addition, nanopore-based DL methods enhance secure molecular communication by enabling encrypted signal interpretation at the molecular level [98].

5.2.9. DL-based intrusion detection

DL–based IDS enhances IoBNT security by automatically identifying anomalies in molecular and bio-cyber environments. Hybrid CNN-LSTM models extract features and classify normal and malicious activities with high accuracy and low latency. These models achieve approximately 93.5% accuracy in bioluminescent interfaces and 92% in BioFET systems [41][99]. Their ability to operate in real time makes them suitable for constrained IoBNT environments. Additional ML and FL approaches further improve detection accuracy while maintaining energy efficiency. DL-based IDS solutions achieve 85–99% accuracy depending on architecture and deployment conditions [89][100].

5.2.10. Existing security protocols and mechanisms

Existing IoBNT security protocols adapt IoT frameworks to meet the unique constraints of molecular and nano-scale communication. They emphasize lightweight cryptography, authentication, key management, and secure communication with minimal overhead. AI-driven intrusion detection and blockchain-based architectures enhance adaptability, decentralization, and trust management [29][101]. PQC techniques and hybrid AI-blockchain frameworks provide resilience against emerging threats while maintaining low energy consumption [31][92]. Lightweight ECC and DNA-based cryptography further enable secure communication in constrained environments with improved efficiency [22]. Additionally, bio-inspired authentication and physical-layer security strengthen resistance against spoofing, impersonation, and routing attacks in complex IoBNT systems [41].

5.3. Threat Mitigation Strategies

The IoBNT presents unique security, privacy, and safety challenges due to its use of nano-scale devices, molecular communication, and direct interaction with biological systems. To address both cyber and biophysical attack vectors while accommodating the extreme resource constraints of bio-nano devices, researchers have proposed a range of tailored mitigation strategies, briefly described below.

5.3.1. Countermeasures for molecular-layer attacks

Molecular-layer attacks in IoBNT exploit biochemical processes that govern sensing, actuation, and communication, enabling threats such as spoofing, enzymatic manipulation, and pathway alteration. Diffusion-based molecular communication is particularly exposed to jamming, eavesdropping, MitM, and spoofing due to its physical-layer characteristics and modulation dynamics [66]. Despite extensive threat identification efforts, concrete defensive mechanisms remain underdeveloped compared with more mature quantum-layer protections. Effective countermeasures include chemical shielding with selective barriers, biological watermarking for traceability, and molecular authentication via aptamers or antibody–antigen binding [46]. Additional resilience is achieved through redundancy, enzymatic degradation of malicious compounds, and context-aware activation mechanisms [4]. Secure encoding, anomaly detection,

and adaptive self-healing biochemical responses further strengthen system integrity and enable sustained operation under attack.

5.3.2. Network-layer mitigation

At the network layer, IoBNT systems face vulnerabilities due to limited resources and reliance on untrusted intermediate nodes, exposing them to spoofing, Sybil, wormhole, and DoS attacks. Compromised repeaters can intercept or alter traffic, making strategies like entanglement-swapping and adaptive rerouting essential, though they introduce performance trade-offs [102]. Reliability declines sharply as the compromise probability increases, underscoring the need for redundant and grid-based topologies. Hybrid defenses combine classical techniques such as rate limiting and filtering with secure routing, encryption, and trust-based quality of service mechanisms. Nano-firewalls and biochemical filtering regulate molecular communication, while probabilistic multi-path routing and anomaly detection enhance reliability under diffusion uncertainty [103]. Self-healing networks, secure addressing, and ML-driven detection further improve resilience, scalability, and protection against routing and flooding attacks.

5.3.3. Physical and biological defenses

Physical and biological defenses protect IoBNT systems from tampering, environmental stress, and biological interference, while supporting system reliability and safety. Bio-inspired approaches, such as swarm intelligence and artificial immune systems, enhance detection efficiency and energy consumption but remain limited in scalability and real-world validation [104]. Core mechanisms include immune-mimicking security with “self” markers, bio-compatible coatings, and nano-encapsulation to resist chemical and mechanical damage [105]. Nano-robot swarms provide decentralized threat neutralization, while structural encapsulation and tamper-resistant designs prevent unauthorized access [11]. Environmental isolation and controlled deployment reduce exposure and signal leakage, improving system stability [42][46]. Adaptive strategies such as apoptosis-inspired regulation and biohybrid integration enable self-repair, fail-safe operation, and enhanced resilience in dynamic environments.

5.3.4. Behavior- and pattern-based detection

Behavior- and pattern-based detection enhances IoBNT security by identifying anomalies in device activity and biological signals that signature-based methods miss. Deep-learning IDS models analyze network traffic and physiological data to detect threats such as DDoS attacks, malware, and insider attacks with high accuracy [106][107]. Hybrid architectures such as CNN–LSTM–VAE capture spatial, temporal, and latent features, achieving strong performance with low latency on resource-constrained devices [97]. Federated IDS frameworks distribute models across nodes while preserving privacy through techniques like differential privacy and homomorphic encryption [89]. Complementary ML methods analyze biochemical dynamics and graph-based relationships to improve scalability and robustness. Continuous behavioral profiling and adaptive baseline updates enable detection of evolving and stealthy threats in dynamic bio-nano environments.

5.3.5. Device hardening

Device hardening reduces IoBNT attack surfaces by turning off unused ports, restricting boot processes, and filtering access, thereby limiting unauthorized interactions. Continuous monitoring of bio-cyber interface logs supports real-time anomaly detection and rapid incident response [5]. Advanced biochip security frameworks extend hardening to multiple layers, detecting microstructure attacks via deep learning and mitigating material-level threats using spectrometric watermarking [108]. DNA barcoding and PUFs provide traceability and hardware-level trust, embedding security into device design. Integrated implementations that combine LSTM-based detection with cryptographic protections demonstrate real-time secure monitoring on embedded hardware [109]. Zero-trust architectures further reinforce endpoint security by aligning AI-based defenses with resource constraints and enforcing continuous verification.

5.3.6. Cryptographic mechanisms

Cryptographic mechanisms ensure confidentiality and integrity in IoBNT communication through symmetric, asymmetric, and keyless approaches. Resource constraints often necessitate offloading cryptographic tasks to external devices, though this introduces additional risks if those devices are compromised [5]. Lightweight protocols such as Lightweight Elliptic Curve Cryptography–based Encryption Protocol with Authentication (LECCEP-A) enable secure, low-latency communication using elliptic-curve techniques and entropy-enhanced encryption [110]. Hybrid systems integrate encryption with AI-based anomaly detection to defend against brute-force and cryptanalytic attacks [109]. FL frameworks further enhance privacy using homomorphic encryption and secure aggregation while maintaining high detection accuracy

[111]. Lightweight cryptography, blockchain integration, and privacy-preserving techniques form a cohesive strategy for securing heterogeneous IoT environments [67][112].

5.3.7. Hardware-based solutions

Hardware-based solutions strengthen IoBNT security through tamper-resistant designs, secure enclosures, and dedicated protection modules. Interference-resistant packaging can detect and respond to attacks, including triggering self-destruction mechanisms when compromised [5]. PUFs provide unique device identities, preventing cloning and enabling verification of hardware integrity. AI–blockchain frameworks extend protection by recording activity on immutable ledgers and automating responses via smart contracts, improving detection accuracy and resilience [106]. Federated edge-trust systems combine encryption, privacy preservation, and dynamic access control to secure distributed environments [89]. Additional architectures integrating explainable AI, blockchain, and lightweight cryptography enhance transparency, reduce false positives, and support scalable, robust IoT security [67].

6. TECHNOLOGICAL INTEGRATIONS IN IOBNT

The IoBNT relies on tightly integrated technologies that enable autonomous operation, secure communication, and intelligent decision-making in complex biological environments. Recent research highlights the rapid evolution of technological integration in IoBNT security, including:

6.1. Artificial intelligence

AI is central to IoBNT, enabling intelligent sensing, secure communication, and adaptive control across bio-nano networks by processing heterogeneous biochemical and physiological data from nanosensors and molecular devices [7][18]. ML techniques, including supervised, unsupervised, and reinforcement learning, extract patterns, classify molecular signatures, detect anomalies, and optimize nano-device behavior. Neural networks support data-driven channel estimation, detection, decoding, and end-to-end learning where analytical models are infeasible [18]. DL architectures such as CNNs, RNNs, and LSTMs capture spatiotemporal biochemical dynamics for signal interpretation and communication optimization with high accuracy under constraints [7]. AI also enables real-time anomaly detection and bio-inspired security by identifying abnormal biochemical signaling [99]. Additionally, FL ensures privacy-preserving, distributed intelligence for applications such as biological digital twins and nano-scale optimization [3][7].

6.2. Blockchain and Distributed Ledgers

Blockchain and distributed ledger technologies (DLTs) provide decentralized, tamper-resistant mechanisms for managing sensitive IoBNT data. Replacing centralized servers enables trustless coordination among nanosensors and improves resilience against cyberattacks [113]. Multi-channel and consortium architectures support domain-specific isolation, while usage-control ledgers enforce embedded policies [114]. Immutable, hash-chained records ensure data integrity and authentication, even in resource-constrained environments [115]. Security is strengthened through smart contracts, cryptography, and lightweight consensus protocols tailored for nano-device participation [24]. Furthermore, privacy-preserving techniques and bio-ledgers, such as BioBlock, enable secure, traceable nanoscale operations, including drug delivery [114].

6.3. Post-quantum and bio-inspired security

IoBNT security requires hybrid approaches combining PQC with bio-inspired mechanisms. Lattice-based, hash-based, and multivariate schemes provide quantum resistance, with lightweight implementations such as Dilithium-5 supporting constrained devices [95][116]. Advanced frameworks integrate zero-knowledge proofs and hybrid cryptographic architectures for secure nano-network communication [117][118]. Quantum-enhanced systems such as QuantumShield-BC combine PQC, quantum key distribution, and secure consensus to enhance resilience against major cyberattacks [119]. Additionally, bio-molecular and physical-layer security exploit biochemical dynamics and environmental cues for keyless encryption [46][95]. Together, these approaches form adaptive, multi-layered, quantum-resilient IoBNT security systems.

6.4. Integration with 6G and terahertz communications

Integrating 6G networks with terahertz (THz) communication enables ultra-high-speed and low-latency IoBNT connectivity. Operating in the 0.1–10 THz band, 6G supports terabit-level data rates and massive connectivity among nano-devices. Gateways bridge nano-devices with external networks using THz transceivers, AI edge processing, and adaptive protocols. Graphene-based transceivers convert biochemical signals into electromagnetic formats for seamless integration

[120]. Security is enhanced through physical-layer methods, anomaly detection, and lightweight quantum key distribution. However, challenges such as path loss, interference, and DoS attacks require AI-driven optimization and hybrid molecular–THz communication frameworks [3][121].

6.5. Edge, fog, and cloud computing

IoBNT systems rely on integrated edge, fog, and cloud computing to manage heterogeneous nano-scale data. Edge computing enables local preprocessing, feature extraction, and real-time decision-making near data sources [43][122]. Fog computing aggregates and processes data at intermediate layers, supporting latency-sensitive and privacy-aware operations [123]. Cloud computing provides large-scale analytics, digital twin modeling, and long-term storage for population-level insights [3][43]. Together, these layers enable dynamic workload distribution, improving efficiency and scalability. This multi-tier architecture significantly reduces latency and energy consumption while supporting secure IoBNT applications.

6.6. Digital twins

Digital twins are real-time virtual replicas of physical systems that enable continuous monitoring and optimization of IoBNT environments [26]. In IoBNT, nanosensors and engineered cells act as data sources, feeding high-resolution biological information into AI-driven models. CNNs and FL enhance predictive accuracy while preserving privacy and reducing bandwidth usage [3]. Molecular signals are translated into digital streams via bio-cyber interfaces such as protein-based systems and graphene transceivers [42]. These systems support predictive simulation, adaptive control, and microbial or tissue-level monitoring [124]. Distributed digital twins further extend scalability across edge, fog, and cloud infrastructures for real-time applications.

6.7. Synthetic biology enhancements

Synthetic biology enables programmable bio-nano devices capable of sensing, computing, and actuating within biological environments. Engineered cells and synthetic gene circuits support molecular communication and bio-computational processing [7][18]. DNA-based systems enhance communication reliability through programmable encoding and optimized routing strategies [4][8]. Bio-cyber interfaces integrate biochemical and electronic domains using optogenetic and electrochemical mechanisms [41][42]. Synthetic biology also strengthens security through kill-switches, intrusion detection, and biological cryptographic primitives [41][46]. These capabilities enable autonomous IoBNT systems for applications such as targeted drug delivery and biosensing [18][31].

6.8. Advanced materials and sensing technologies

IoBNT relies on advanced nanomaterials to enable sensitive and biocompatible sensing and actuation. Carbon-based materials such as graphene and CNTs provide high conductivity and biocompatibility for nanosensors and communication interfaces. Metal nanoparticles support optical, catalytic, and plasmonic sensing for biomedical applications. Biodegradable polymers and hydrogels enable controlled drug release and adaptive interfaces, while 2D materials like MoS_2 enhance sensing selectivity. These materials support electrochemical, optical, and bio-FET-based sensing modalities for real-time biomarker detection. Integrated with capacitive and indirect sensing, they form a robust IoBNT interface for high-precision healthcare systems [31]. Figure 10 summarizes some of the technological integrations in the IoBNT.

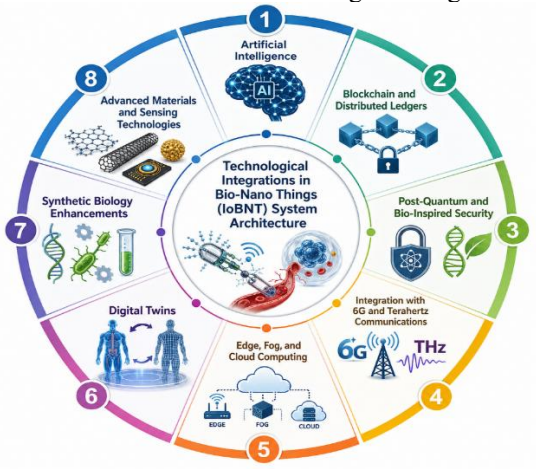


Fig. 10. Summary of the technological integrations in the IoBNT.

7. TOOLS, TESTBEDS, AND SIMULATION PLATFORMS

Because bio-nano devices operate under extreme resource constraints and rely on hybrid molecular and electromagnetic communication paradigms, researchers require specialized experimental environments to accurately capture interactions, threat models, and defensive strategies. Accordingly, the section surveys representative software tools, in vitro and in vivo testbeds, and multi-scale simulation platforms that support reproducible security analysis, performance benchmarking, and cross-layer validation of IoBNT security solutions under realistic biological and networking conditions.

7.1. Simulation tools for IoBNT security

Recent IoBNT research primarily relies on custom, ad hoc simulators to model molecular communication channels and evaluate security, as no dedicated, widely accepted IoBNT security simulator currently exists. Table 2 provides a comparative view of key IoBNT-related simulators and their security-relevant properties.

TABLE II. COMPARATIVE VIEW OF KEY IOBNT-RELATED SIMULATORS AND THEIR SECURITY-RELEVANT PROPERTIES.

Tool/Approach	Description	Scalability	Accuracy & Realism	Main Limitations	References
Custom bioluminescent IoBNT traffic simulator	A synthetic generator produces bioluminescent bio-cyber interface traffic to train DL–based anomaly and attack detection models for the IoBNT, focusing on time-series molecular and optical signals collected at the bio-cyber gateway.	The approach supports large-scale datasets by delegating feature extraction to a CNN–LSTM architecture, enabling efficient training on conventional hardware.	Uses parameter ranges derived from molecular communication and IoBNT literature, appropriately scaled to capture key channel characteristics and abnormal operating ranges, while excluding detailed biochemical dynamics and patient-specific anatomical variations.	It is not a complete network simulator and lacks explicit 3D spatial transport, multi-organ physiological modeling, and in-body adversary behavior; consequently, the realism of simulated attacks is constrained by the synthetic traffic model, and the framework provides no standard interface for interoperability with other IoBNT simulators.	[41]
OpenFOAM–MPPIC microfluidic MC simulator	Uses computational fluid dynamics (CFD) with the OpenFOAM MPPIC solver to simulate particle transport in microfluidic molecular communication channels for IoBNT transceivers and experimental testbeds.	CFD simulations are computationally intensive but effectively capture complex geometries, making them suitable for channel-level analysis rather than large-scale network-level simulations.	Validated against analytical models, particle-based simulators, and a millimeter-scale testbed, the CIR achieved an RMSE below 10% in flow-dominated regimes and converged to the analytical tail in expanding geometries.	Focuses exclusively on the physical layer, excluding higher-layer protocols, security considerations, and adversarial models, and it is limited to flow-dominated regimes and specific geometries, making scaling to whole-body IoBNT networks or large swarms impractical.	[125]
Neural network–based molecular communication/IoBNT simulation workflows	Researchers employ neural network surrogates and data-driven simulators to approximate complex molecular communication channels and nanonetworks,	Neural network surrogates, once trained, efficiently scale to numerous channel realizations and nodes, although their training can be computationally expensive.	Accuracy depends on the training datasets, and models can approximate highly nonlinear or stochastic channels where analytic models fail, but	Current research primarily emphasizes reliability and capacity rather than addressing explicit security attacks, often relying on	[18]

	enabling the exploration of clustering, channel estimation, and intelligent protocols for IoBNT.		extrapolating beyond the training regime remains risky.	synthetic, scenario-specific datasets and lacking standardized benchmarks or comprehensive end-to-end IoBNT security models.	
DNA-based IoBNT routing & track hopper molecular communication simulators (AoI OptiIoBNT, THMC)	Researchers use custom simulators for DNA-encoded packets, Markov decision process routing, age-of-information optimization, and DNA track-hopper transport to investigate reliability, delay, and congestion in DNA-based IoBNT.	Simulation enables studies of larger networks with many nodes and links, allowing higher node counts than CFD.	Capture DNA channel coding (e.g., Yin–Yang coding), retransmissions, and topology-dependent delays, while simplifying the physical layer compared with full biochemical CFD.	Focus on performance rather than attack models, without modeling explicit adversary behaviors such as eavesdropping, jamming, or DNA tampering; biochemical and immune system processes are abstracted, and the tools are released as study-specific code rather than general-purpose simulators.	[4][8]
Semi-autonomous in vivo nanoswimmer simulator	A computational framework that enables magnetically controlled nanoswimmer swarms to sense gradients and actively search for tumors, effectively performing semi-autonomous in vivo computation.	It supports large swarms through particle-based simulation, trading off runtime, and has been applied at the organ scale rather than the Internet scale.	The model simulates static and mobile obstacles as well as biological gradients, providing realistic representations of motion and deposition while offering only minimal abstractions for communication and cybersecurity.	Focused on locomotion and detection time, without modeling molecular communication or adversarial interference, conducting a security analysis would require additional layers.	[126]

7.2. Experimental testbeds and prototypes

Recent IoBNT literature presents complementary experimental and prototyping platforms and provides emerging security design guidance across the stack. Table 3 compares experimental testbeds, prototypes, and platforms in IoBNT.

TABLE III. CONTRASTING IOBNT MOLECULAR COMMUNICATION TESTBEDS AND CONCEPTUAL PLATFORMS.

Platform/approach	Description	Scalability	Accuracy & realism (in vitro/in vivo)	Main Limitations	References
Low-cost microfluidic molecular communication testbed (pH, hydrodynamic gating)	Tape-based microfluidics integrates screen-printed potentiometric sensors with programmable hydrodynamic gating to prototype end-to-end molecular communication signaling (4-ary CSK) for IoBNT healthcare applications.	The devices achieve very high scalability (~$1/unit, <1 h fabrication time) and enable easy geometry reconfiguration, making them ideal for exploring large design spaces and educational applications.	The microfluidic system provides high control realism for diffusion, flow, and symbol shaping, precisely mimicking microchannel environments in vitro while enabling accurate spatiotemporal signal control and repeatable results.	The experiments did not occur directly in vivo, failed to capture biochemical complexities such as immune responses and heterogeneous tissues, and limited security testing to physical-layer properties without addressing adversarial threats.	[27]

OpenFOAM microfluidic molecular communication simulation + mm-scale testbed	The CFD-based OpenFOAM MPPIC solver was used to simulate molecular communication in microfluidic channels, and its results were validated against an analytical model, particle-based simulations, and measurements from a millimeter-scale fluidic testbed.	The physical testbed operates at the millimeter scale and offers moderate scalability limited by lab hardware, while simulations achieve very high scalability across numerous geometries and conditions.	Analytical and particle-based models closely matched in flow-dominated regimes, achieving high accuracy in in vitro microfluidic channels with experimental RMSE below 10% compared to simulations.	Most studies focus on in vitro microfluidics, simplifying biological reactions, binding, and active transport, while modeling only channel behavior rather than security experiments.	[125]
Thermomolecular communication testbed (demo)	The first physical testbed for thermomolecular signaling demonstrates temperature-modulated molecular channels as a novel physical layer for the IoBNT–IoT interface.	The early-stage demonstration focuses on proof of concept, and although it is scalable in principle through replication, it currently remains at a low TRL.	It captures realistic physical and thermodynamic effects under controlled in vitro conditions, although no in vivo experiments have been conducted yet.	Reports limited functions and metrics, has not been integrated with bionanodevices or real tissues, and lacks a systematic security evaluation.	[127]
DNA-based track hopper molecular communication system (THMCs)	DNA track-hopping systems enable highly reliable, low-delay molecular communication in IoBNT, supporting applications such as health monitoring and disease detection (e.g., theoretical and simulation studies).	The network-level scalability, encompassing multiple links and nodes, has been demonstrated conceptually, though it has been validated only through simulations to date.	The model incorporates detailed link delay and reliability but lacks experimental (in vitro or in vivo) validation, and its biological realism relies on assumptions from DNA nanotechnology.	No prototype or testbed has been developed, and researchers have not yet tested biochemical noise, immune interactions, or deployment constraints, nor have they evaluated the security properties.	[4]
Nano-scale chemical computing unit	Compartmental diffusion-reaction architectures perform matrix multiplications for in-body computing in IoBNT.	It scales well in simulations and micro- and mesoscopic models, although its physical implementation remains conceptual.	Stochastic and dynamical models realistically capture temporal dynamics at the mesoscopic scale, although they have not yet been demonstrated in vitro or in vivo.	Challenges remain in fabricating and integrating BNTs, ensuring their robustness in real biological environments, and assessing their security against side-channel attacks and tampering.	[32]
Bottom-up synthetic cells as IoBNT nodes	Artificial “cells,” assembled from molecular components, actively exchange chemicals and participate in molecular communication networks, functioning as programmable bionano nodes.	Current lab systems are low in complexity and small in scale, with the potential to scale through parallel fabrication, though this has not yet been achieved.	High biochemical realism (wet lab, cell-like compartments) but low in complexity and small in scale, with the potential to scale through parallel fabrication, though this has not yet been achieved.	Experimental maturity lags behind theory, as controlling complex, stochastic molecular communication and its interaction with natural cells remains challenging, and these systems have not yet been employed in formal security experiments.	[128]

7.3. Benchmarking datasets and evaluation environments

Existing studies address individual components, such as synthetic molecular-level data, bio-cyber interfaces, IoMT/IoT datasets, digital twins/testbeds, and threat models, that can be integrated to form a provisional comparison. Table 4 maps existing datasets to the IoBNT benchmarking goals.

TABLE IV. EXISTING DATASETS ARE MAPPED ONTO THE IOBNT BENCHMARKING GOALS.

Category	What current work provides	Description	Scalability/Accuracy/ Realism	Key Limitations	References
Molecular communication synthetic datasets	Synthetic parameter-driven traces to optimize bioluminescent biocyber interfaces and BioFET sensors.	Researchers use these datasets to train deep models that classify anomalous bioluminescent or BioFET signals in IoBNT interfaces.	The model demonstrates high scalability due to its low generation cost, maintains accuracy consistent with the assumed equations, but offers limited realism because it does not account for biological noise or tissue effects.	Rely solely on analytical models, which fail to capture real wet-lab artifacts, cross-talk, or long-term drift.	[41][99]
Bio cyber interface (bioFET/biosensor) datasets	Synthesized features characterize BioFET and bioluminescent interface parameters, including binding rates, gain, and timing.	Benchmark DL–based anomaly detectors for interface-level attacks, including parameter tampering and abnormal signal statistics.	Demonstrates very high scalability and provides good accuracy for electronic and signal-level behavior, but it does not account for patient variability or biochemical degradation.	Datasets remain private, lack an agreed-upon schema or public corpus, and employ threat models that are mostly binary (normal vs. anomalous) rather than following standardized attack taxonomies.	[41][99]
IoMT/IoT network traffic adapted for IoBNT gateways	Modern IoT and IoMT intrusion detection relies on datasets such as CICIoT2023, CICIDS2017, ToN-IoT, and WUSTL EHMS 2020.	Train and evaluate IDS on edge gateways that aggregate IoBNT traffic by simulating standard network-layer attacks, including DoS/DDoS, brute-force attacks, port scans, and web-based attacks.	Demonstrates high scalability, handling millions of flows, and ensures accuracy through well-labeled attacks, making it suitable for machine learning benchmarking, while generating realistic IP-layer traffic despite lacking molecular semantics.	Map molecular events to IP flows before reusing them in IoBNT, without modeling intra-body molecular links or biological constraints.	[3][129][130]
Physiological/clinical datasets coupled to IoT/IoMT	IoMT datasets that combine biometric and traffic data, such as WUSTL EHMS 2020, support broader IoMT risk-assessment case studies.	Jointly evaluating attack detection and its impact on vital signs and alarms enables risk-based benchmarking of security controls.	Demonstrates moderate scalability, handling hundreds to thousands of subjects or records, achieves good accuracy for clinical signals, and generates realistic patient data without modeling nano-scale processes.	True IoBNT deployments have not collected these data due to organizational and ethical constraints that limit sharing, and no standardized method links them to molecular channel models.	[130][131]
Wet lab experiment logs for IoBNT	Researchers have conducted conceptual discussions on	It primarily motivates nanoscale threat models and	Scalability is low due to the high cost of experiments, while accuracy and realism are potentially the highest,	There are no publicly available, structured wet-	[95][128]

	bottom-up synthetic cells and molecular security experiments, yet they have not provided any open benchmark logs.	physical-layer countermeasures rather than serving as a machine-learning dataset.	though they are currently described only conceptually.	lab security datasets, and discussions of reproducibility and standard logging formats are lacking.	

7.4. Tool comparison and limitations

Table 5 compares simulation tools for IoBNT security, highlighting their scalability, accuracy, realism, and associated limitations.

TABLE V. SUMMARY OF THE COMPARISON OF THE SIMULATION TOOLS FOR IOBNT SECURITY, EMPHASIZING SCALABILITY, ACCURACY, AND REALISM, ALONG WITH THEIR LIMITATIONS.

Tool/family	Description	Scalability	Accuracy & realism for comms/security	Key limitations for IoBNT security	References
NS 3 (incl. QKDNetSim+, QKDNetSim)	QKDNetSim+ extends a widely used discrete event network simulator for Internet and IoT applications by incorporating more realistic quantum key management and channel models, enabling the study of DDoS attacks, malware propagation, QKD networks, and wireless video streaming.	It manages hundreds to thousands of nodes and is commonly used in large wireless and QKD networks.	QKDNetSim+ enhances realism in key buffers and cryptography compared to earlier NS-3 quantum modules by providing high-fidelity packet-level models and full protocol stacks, making it well-suited for evaluating traffic-level attacks and defenses, such as DDoS traceback.	IoBNT must be modeled as conventional links because it lacks native bio-nano channels or molecular communication. Quantum extensions address QKD rather than biochemical processes, and increasing the scenario detail in C++ simulations increases both complexity and runtime.	[132][133]
OMNeT++ (+ INET, Castalia, etc.)	A modular, GUI-driven simulator with rich frameworks such as INET, Veins, and Castalia supports the simulation of wired and wireless networks, IoT, and WSN security and intrusion detection. It is used to evaluate WSN performance, security, and TSN accuracy.	It demonstrates good scalability and achieves more stable throughput and latency than NS-3 for large WSNs, effectively scaling from small deployments to city-scale systems.	With carefully calibrated INET and hardware-aligned models, researchers can accurately approximate real TSN switch behavior, including clock synchronization, forwarding latency, and frame preemption, thereby enabling realistic malware and intrusion studies in wireless sensor networks (WSNs).	Requires substantial expertise in C++ and supporting frameworks, relies heavily on external modules, and offers limited built-in models for nano- and molecular-scale channels as well as cell-scale physics, which necessitates a highly abstracted representation of IoBNT.	[134][135]
Contiki/Cooja	Serves as an operating system and emulator/simulator for low-power IoT and 6LoWPAN networks, emulating real motes and RPL routing to	It is well-suited for detailed emulation involving tens to hundreds of nodes, but is less	Enables realistic firmware-level behavior and the execution of RPL-based attacks, including Hello Flood, Rank Decrease, and	Focus on low-power IP-based networks and assume simplified environments and channel models, excluding nano-scale transport	[136]

	support anomaly detection experiments.	appropriate for very large-scale network topologies.	Version Number Modification, while capturing network traffic for machine-learning-based anomaly detection.	mechanisms and biochemical processes; consequently, they provide limited support for massive bio-nano populations and do not adequately address intra-body communication media.	
IoTSecSim	A purpose-built simulator for IoT security models, flexible IoT topologies, emulates malware behaviors such as Mirai, integrates node- and network-level defense mechanisms, and computes relevant security metrics.	Designed to simulate thousands of devices and multiple attacker models using epidemic-like propagation, this approach explicitly improves upon prior SIoT simulators, which were limited to approximately 2,000 devices.	Represent realistic malware scanning, exploitation, and defense mechanisms, with sensitivity analysis yielding results consistent with related empirical studies.	Cyber attacks at the IP/TCP layers have been extensively studied. Still, malware models do not capture bio-nano interactions, and epidemic abstractions fail to capture molecular transport, diffusion, and receptor-level processes essential to IoBNT.	[137]
NetSim	The commercial network simulator with a graphical interface is used to assess IoT performance under botnet-based DDoS attacks by varying the number of attackers.	Handles moderate-to-large IoT topologies and studies network models with multiple malicious nodes.	Evaluates throughput and latency under UDP flooding, showing up to 67% throughput loss and over 350% latency increase, and demonstrates sufficient realism for IoT traffic-level security assessment.	Lacks inherent nano-scale channel, cell biology, or biochemical reaction models, and vendor lock-in due to closed-source restrictions hinders its extension to IoBNT physics.	[138]
MATLAB/Simulink (incl. quantum comms, MatPSST, CSMO)	General numerical and simulation environments support quantum secure direct communication (QSDC) protocol simulations, power system/ICS co-simulations using MatPSST, and smart grid cyber-physical co-simulations with OMNeT++.	It scales effectively for differential equations and control system models, and has demonstrated full co-simulation of large power grids and networks.	Enables high-precision modeling of physical layer processes, control loops, and quantum channels, including noisy QSDC with frequency coding, and co-simulates control and communication with OMNeT++, which is crucial for studying cyberattack resilience.	While it performs excellently for molecular, biophysical, and reaction-diffusion models, it lacks a built-in discrete nano-networking security stack, requiring manual implementation of IoBNT protocols and attacks, and its licensing cost remains a barrier.	[139]
Python/SimPy-based custom simulators	Implement wireless ad hoc and WSN algorithms using	Lightweight and suitable for algorithm-	Offer flexible timing, enable node sleep, and	No built-in channel, bio nano, or security models;	[140]

	discrete-event frameworks such as DAWN Sim with SimPy, which closely aligns with the concept of 'custom molecular comms scripts' in your list.	level studies, it is not designed for large, detailed networks.	support mobility, making it well-suited for prototyping distributed protocols and MAC algorithms.	all IoBNT physics and threat models must be coded from scratch. Validation and realism depend entirely on the developer.	
General-purpose molecular communication/multicellular platforms	An agent-based platform models multicellular molecular communication systems, such as cancer spheroids and vascular-like networks, simulating cell–cell forces, division, growth, death, and molecular exchange.	Designed to handle numerous interacting cells, it employs efficient algorithms to manage their interactions.	High realism in intra-tissue molecular dynamics and cell behavior makes it suitable for studying bionano communication mechanisms.	Currently, it focuses on communication and biology rather than on explicit cybersecurity, such as attacker models, cryptographic protocols, or adversarial nanonodes. It requires integration with security logic to function as an IoBNT security testbed.	[141]

8. PERFORMANCE METRICS AND EVALUATION FRAMEWORKS IN IOBNT SECURITY

Performance evaluation in IoBNT inherently spans multiple disciplines, including communication theory, nanotechnology, synthetic biology, and biomedical engineering. Below are the brief descriptions of the performance metrics and evaluation frameworks used in IoBNT security.

8.1. Molecular communication metrics

Molecular communication enables information exchange in IoBNT by encoding and transmitting data through molecules, a process that requires metrics tailored to stochastic and chemistry-driven dynamics. Recent studies replace Shannon rate with identification capacity in event-triggered secure MC over Poisson channels, enabling efficient detection with doubly exponential code growth and improved energy performance [86]. Core metrics include signal propagation delay, governed by diffusion and first-passage processes, and molecular concentration levels that determine detection reliability. Molecular noise, often modeled using Poisson, binomial, or Gaussian processes, captures diffusion variability, counting uncertainty, and interference [15][28]. Channel capacity and mutual information define the limits of communication, while Bit Error Rate (BER) and Symbol Error Rate (SER) quantify reliability in the presence of inter-symbol interference (ISI), noise, and adversarial effects. Additional measures, such as signal-to-noise ratio (SNR), signal-to-interference-plus-noise ratio (SINR) scalability, and throughput, capture channel quality, multi-user interference, and overall system efficiency, highlighting trade-offs among reliability, energy, and security.

8.2. Security evaluation metrics

Security evaluation in IoBNT must address extreme resource constraints, sensitive biomedical data, and complex biological environments, necessitating metrics beyond those of traditional IoT approaches. While no unified framework exists, prior work identifies key components, such as secure event-triggered MC, in which identification capacity reflects both secrecy and reliability [86]. Intrusion detection performance is commonly assessed using accuracy, F1-score, false positive rate (FPR), ROC-AUC, and Matthews Correlation Coefficient, with reported results exceeding 94–99% accuracy in healthcare systems [97][110]. Building on these, IoBNT security can be evaluated in terms of confidentiality, integrity, authentication, authorization, and availability. Additional metrics include attack detection rate, resilience, and energy-aware security performance. Biocompatibility overhead, chemical consumption, and scalability further extend evaluation to biological and operational constraints, forming a comprehensive basis for IoBNT-specific security assessment.

8.3. Network performance metrics

Network performance in IoBNT reflects the need for reliable, efficient communication in dynamic, biologically constrained environments. Unlike conventional systems, IoBNT integrates molecular and terahertz communication, requiring metrics such as throughput, latency, reliability, and energy efficiency. Throughput measures successful data delivery, while latency

captures delays dominated by diffusion and processing. Reliability is assessed using packet delivery ratio (PDR) and error metrics such as bit error rate (BER) and Packet Error Rate (PER) in the presence of biological noise and interference [29][110]. Energy efficiency and network lifetime quantify sustainability under limited nano-device resources, while scalability evaluates performance in dense deployments. Importantly, IoBNT introduces biocompatibility-aware performance, ensuring communication remains safe, non-toxic, and minimally invasive while maintaining system effectiveness.

8.4. Multi-objective optimization metrics

Multi-objective optimization (MOO) in IoBNT addresses trade-offs among competing goals such as security, energy, latency, and privacy by using Pareto-based approaches rather than single metrics. Recent work applies MOO in IoT-related systems, optimizing secrecy energy efficiency, key generation, and IDS performance using bio-inspired algorithms [142][143]. Evaluation relies on metrics such as generational distance, inverted generational distance, hypervolume, spacing, and runtime to assess solution quality and diversity [144][145]. Application-level metrics include accuracy, false-positive rate, secrecy rate, energy consumption, and latency [72]. In IoBNT, these metrics capture interactions between biological and cyber constraints, in which improvements in one dimension often degrade the other. MOO provides a structured framework for balancing these trade-offs and optimizing secure, efficient IoBNT systems.

9. CHALLENGES AND LIMITATIONS

The IoBNT offers immense potential but encounters critical challenges that hinder its widespread adoption and secure deployment. Below are the brief descriptions of several limitations and open challenges in securing IoBNT.

9.1. Resource constraints of bio-nano devices

Bio-nano devices operate under severe constraints in computation, memory, energy, and communication, making conventional cryptography and IDS impractical [18]. Limited processing power and storage capacity constrain the use of complex algorithms, while intermittent energy harvesting from chemical or thermal sources prevents continuous operation. Communication via molecular signaling or terahertz waves offers low data rates and high susceptibility to noise. These limitations hinder real-time monitoring and secure exchanges. Consequently, research prioritizes lightweight, energy-efficient, and cooperative security mechanisms.

9.2. Heterogeneity of IoBNT devices and networks

IoBNT systems integrate diverse components, including nanosensors, nanorobots, molecular nodes, and bio-cyber interfaces, operating across multiple scales and modalities [18][31]. This heterogeneity complicates the design of unified security protocols and interoperable frameworks. Differences in communication methods and resource capacities hinder standardization and consistent enforcement. Dynamic topologies and varying quality of service requirements further increase complexity. Addressing these challenges requires adaptive, cross-layer security solutions, though scalable heterogeneous networks remain an open issue [18].

9.3. Limited standardization and interoperability

IoBNT lacks widely accepted standards for communication, data formats, and security, limiting interoperability and scalability. Proprietary designs across devices and platforms complicate the implementation of addressing, routing, and authentication mechanisms. This fragmentation increases the risk of misconfiguration and weakens system reliability. Integration with IoT and biomedical systems further amplifies these challenges. Advancing standardization and unified frameworks is essential for secure and scalable IoBNT ecosystems [31][77].

9.4. Vulnerability to physical and molecular-level attacks

Bio-nano devices operate in biological environments, exposing them to molecular and cellular-level attacks such as chemical tampering and bio-interference. Traditional cybersecurity methods cannot address these biologically grounded threats. Attackers can manipulate molecules or biochemical pathways to disrupt device functionality. Detection is difficult due to limited observability and system complexity. Therefore, IoBNT security must incorporate multi-layer defenses, including physical-layer protection and molecular integrity checks [66].

9.5. Data privacy and sensitivity concerns

IoBNT systems handle highly sensitive biomedical data, including genetic and physiological information, raising serious privacy risks. Continuous in-body monitoring increases exposure compared to conventional IoT systems. Resource constraints limit the use of strong cryptographic protections. Heterogeneous architectures and vulnerable communication channels expand attack surfaces. Techniques such as FL improve privacy but do not fully resolve regulatory and ethical concerns [3][31].

9.6. Communication reliability and noise in molecular channels

Molecular communication is inherently slow, stochastic, and noise-prone, limiting reliability and throughput. Diffusion dynamics, inter-symbol interference, and environmental interactions degrade signal integrity. Channel conditions are highly nonlinear and difficult to model analytically. These challenges complicate error correction and channel estimation. As a result, IoBNT systems rely on adaptive and data-driven methods to maintain acceptable communication performance [18].

9.7. Scalability and network management

Scaling IoBNT networks poses major challenges due to the dense deployment of resource-limited devices. Nano-nodes cannot support complex routing, synchronization, or management protocols. Dynamic topologies and biological variability require adaptive and autonomous control mechanisms. High density increases interference and congestion, reducing reliability. Scalable architectures and decentralized strategies are needed but remain underdeveloped [18].

9.8. Integration with existing cyber-physical and IoT systems

Differences hinder ioBNT integration with IoT and cyber-physical systems due to differences in protocols, latency, and security requirements. Bio-nano devices generate heterogeneous data incompatible with conventional processing pipelines. Middleware such as BioFET interfaces enables translation but introduces synchronization challenges. Existing IoT security mechanisms are often too resource-intensive. Therefore, lightweight and adaptive security approaches are required for seamless integration [67].

9.9. Real-time monitoring and intrusion detection

Real-time intrusion detection in IoBNT is constrained by limited energy and computational resources, as well as heterogeneous communication models. Continuous monitoring rapidly depletes resources and is difficult to sustain. Propagation delays and biological noise hinder timely anomaly detection. Current solutions mainly rely on gateway-level analysis rather than in-body detection. Developing lightweight, real-time IDS tailored to IoBNT remains a significant research gap [67].

9.10. Emerging threats and evolving attack vectors

IoBNT faces a rapidly evolving threat landscape that combines cyber, biological, and nano-scale attacks. Traditional threats such as spoofing and jamming are adapted to molecular communication channels. Integration with AI and cloud systems expands attack surfaces and enables more sophisticated intrusions. Static defenses are insufficient in such dynamic environments. Adaptive and context-aware security frameworks are therefore essential [18].

9.11. Trade-offs between security and system efficiency

IoBNT security must balance protection with strict resource constraints. Strong security mechanisms increase energy consumption, latency, and communication overhead. Lightweight solutions reduce resource use but may weaken security guarantees. Heterogeneous device capabilities further complicate optimization. Designing adaptive security frameworks that balance efficiency and robustness remains a core challenge [97].

9.12. Adversarial ML and AI vulnerabilities

AI enhances IoBNT functionality but introduces vulnerabilities to adversarial attacks such as poisoning and evasion. These attacks can manipulate models and compromise decision-making. Biological noise and high data complexity make it difficult to detect adversarial inputs. Limited resources further constrain defensive mechanisms. Strengthening robustness and explainability of AI models is essential for safe IoBNT deployment [111][112].

9.13. Regulatory, ethical, and legal limitations

IoBNT deployment is constrained by ethical, legal, and regulatory challenges related to data privacy and device safety. Continuous biological monitoring raises concerns about consent, ownership, and surveillance. Regulatory frameworks remain fragmented and lag behind technological advances. Legal ambiguity complicates accountability and liability. Harmonized standards and transparent governance are required for responsible adoption [9][100][112].

9.14. Complexity of secure protocol design across multiple layers

IoBNT systems span multiple layers, each with distinct constraints and vulnerabilities. Designing secure protocols across these layers is challenging due to heterogeneity and dynamic conditions. Physical-layer security must address the unreliability of molecular channels, while higher layers ensure integrity and confidentiality. Cross-layer dependencies complicate optimization. Holistic and integrated security frameworks are needed but remain limited [62].

9.15. Biological and environmental unpredictability

Biological environments introduce inherent variability that affects IoBNT performance and security. Factors such as temperature, chemical reactions, and molecular concentrations alter communication behavior. These dynamics reduce reliability and complicate protocol design. Environmental unpredictability also impacts device stability and sensing accuracy. Adaptive and context-aware mechanisms are required to handle these uncertainties [15].

9.16. Difficulties in testing and validation

Testing IoBNT systems is difficult due to their multi-scale and dynamic nature. Simulations often rely on simplified assumptions that fail to capture the full complexity of biological systems. In vivo testing is limited by ethical and safety constraints. Lack of standardized benchmarks reduces reproducibility and comparability. Developing realistic testbeds and evaluation frameworks remains a critical need [31].

9.17. Multi-domain attack complexity

IoBNT systems are vulnerable to attacks spanning biological, nano, and cyber domains. A single compromised node can trigger cascading effects across multiple layers. Heterogeneity and cross-layer interactions complicate detection and attribution. Traditional single-domain defenses are insufficient. Comprehensive, multi-domain security models are required to address these complex threats [18][66].

9.18. Communication reliability and noise in molecular channels

Molecular communication suffers from severe noise, low data rates, and inter-symbol interference. Time-varying diffusion and biochemical interactions further degrade signal quality. Channel modeling is difficult due to the nonlinear and stochastic nature of channels. These factors increase error rates and reduce reliability. Advanced communication techniques are required to improve performance under these constraints [15].

9.19. Bio-nano device design, biocompatibility, and safety

IoBNT devices must be biocompatible, safe, and reliable within living systems. Material toxicity, immune responses, and device degradation pose significant risks. Extreme miniaturization limits functionality and security capabilities. Current fabrication technologies cannot fully support complex IoBNT designs. Ensuring safety and long-term stability remains a major challenge [31].

9.20. Molecular communication and bio-cyber interfacing

IoBNT relies on molecular communication and bio-cyber interfaces to connect biological and digital systems. Nonlinear dynamics and environmental noise complicate signal transmission and decoding. Interfaces such as BioFETs translate signals but remain sensitive to variability and attacks. Precise control of molecule release and device coordination is difficult. Robust and secure interfacing mechanisms are still under development [13][72].

9.21. Energy supply and sustainability at the nano-scale

Energy supply is a fundamental constraint in IoBNT systems. Nano-devices rely on limited energy-harvesting and storage mechanisms, thereby restricting functionality. Security operations directly compete with energy availability. Continuous and safe in vivo power generation remains unresolved. Efficient energy management and sustainable power solutions are essential for long-term deployment [18].

Collectively, these challenges underscore the need for multidisciplinary approaches, standardized metrics, and comprehensive security frameworks to ensure the safe, reliable, and effective deployment of IoBNT systems. By systematically addressing these gaps, future research can advance the development of secure, resilient, and trustworthy IoBNT architectures, enabling their successful integration into real-world applications.

10. FUTURE RESEARCH DIRECTIONS

To overcome these challenges, researchers must develop innovative solutions that enhance security, interoperability, and efficiency while addressing the unique constraints of bio-nano networks. Below are the brief descriptions of the key directions for future research.

10.1. Bio-cyber interface security and standardization

Securing bio-cyber interfaces is critical to prevent cyberattacks and bio-cyber terrorism in IoBNT systems. These interfaces, including graphene, optogenetic, electrochemical, and capacitive platforms, convert biochemical signals into digital data and require strong authentication, access control, and interference mitigation. Key threats include spoofing, unauthorized access, and side-channel leakage. Future research should define standardized protocols, threat models, and security-by-design frameworks to ensure data integrity, authenticity, and confidentiality. Efforts such as IEEE P1906.x and IoNT studies emphasize interoperable architectures, lightweight security, and unified evaluation platforms [16][77].

10.2. Lightweight cryptographic and authentication schemes for nano-scale devices

IoBNT devices operate under strict energy, memory, and computational constraints, making conventional cryptography impractical. Research should prioritize ultra-lightweight cryptographic primitives, including stream ciphers, ECC, hash-based methods, and PUF-based authentication. These schemes must address both classical threats (e.g., impersonation, MitM) and nanoscale-specific risks, such as molecular interference. Hybrid approaches combining symmetric encryption, challenge-response protocols, and energy-efficient key management are promising. Emerging work highlights DNA-based cryptography and ultra-lightweight protocols achieving high efficiency and resilience, while calling for standardized performance metrics and post-quantum readiness [22][146].

10.3. Secure and reliable molecular communication protocols

Molecular communication enables nano-scale data exchange via chemical signals but faces challenges such as noise, interference, and molecular degradation. These systems are also vulnerable to attacks like interception, spoofing, and tampering. Future protocols must integrate error correction, interference-resilient modulation, synchronization, and adaptive retransmission while maintaining biological compatibility. Cryptography-inspired mechanisms, including molecule-level encoding and enzyme-mediated key exchange, can enhance security. Research should also explore hybrid molecular–electromagnetic systems, cross-layer integration, and standardized simulation frameworks for reliable and secure communication [4].

10.4. Cross-layer security frameworks

IoBNT systems span the molecular, physical, network, and application layers, requiring integrated security that goes beyond traditional layer-specific approaches. Cross-layer frameworks enable coordination, such as using physical-layer signals to support network-layer intrusion detection. These frameworks should incorporate AI-driven threat detection, blockchain-based trust, and FL for scalability and privacy. Standardized metrics for latency, energy, and resilience are essential for benchmarking. Current studies emphasize the need for unified, end-to-end architectures that co-design communication, cryptography, and safety mechanisms across layers [77][96].

10.5. AI-driven threat detection and adaptive defenses

AI and ML enhance IoBNT security by enabling real-time detection of complex and stealthy attacks. Techniques such as CNN–LSTM models, unsupervised anomaly detection, and reinforcement learning improve threat classification and adaptive response. Deployment at the edge or bio-cyber gateways supports privacy-preserving, low-latency defenses. FL and blockchain further ensure data integrity and trust. While high detection accuracy has been demonstrated, challenges remain regarding scalability, resource constraints, and the handling of non-IID data in distributed environments [18][67].

10.6. Privacy preservation in IoBNT data flows.

IoBNT systems process highly sensitive biological data, requiring advanced privacy-preserving mechanisms beyond traditional IoT models. Lightweight cryptography, homomorphic encryption, and secure multi-party computation enable secure data handling under resource constraints. FL, differential privacy, and blockchain-based auditability support decentralized and privacy-aware analytics. Future work should address inference attacks, privacy in multi-hop nano-networks, and secure frameworks for biological digital twins. Existing studies highlight the need for scalable, privacy-preserving architectures with strong guarantees to protect biomedical data [3][111].

10.7. Interoperability and policy harmonization across domains

IoBNT applications span healthcare, environmental monitoring, and bioengineering, requiring interoperable systems and harmonized security policies. Unified protocols, middleware, and architectures are essential for seamless data exchange while maintaining performance and security. Policy-aware access control and automated compliance mechanisms can support regulatory requirements. Current research emphasizes the need for coordinated global frameworks addressing privacy, ethics, and data governance. IoNT and healthcare studies identify interoperability and regulatory alignment as key barriers to large-scale deployment [77][147].

10.8. Bio-aware attack modeling and simulation tools

IoBNT introduces complex interactions across biochemical and cyber domains, requiring advanced bio-aware attack modeling tools. These tools simulate threats across molecular, physiological, and network layers, incorporating factors such as immune responses and stochastic channel behavior. Hybrid simulation environments that combine nanonetwork and biochemical platforms enable comprehensive risk assessment and system validation. Current research highlights the lack of standardized simulators and testbeds for nano-scale security evaluation. Future work should focus on realistic attack scenarios, benchmarking datasets, and cross-domain simulation frameworks [16][67][77].

10.9. Ethical, regulatory, and human safety considerations

IoBNT systems operate within biological environments, raising critical ethical, safety, and regulatory concerns. These include privacy, consent, toxicity, immune response, and fail-safe operation of implanted or embedded devices. Research should integrate explainable AI, dynamic consent models, and lifecycle risk assessment into system design. Current regulations remain insufficient for nano-bio convergence, necessitating harmonized standards and certification frameworks. Studies emphasize the need for interdisciplinary governance to ensure the safe, ethical, and clinically viable deployment of IoBNT [147].

10.10. Advanced testbeds and digital twin models

Realistic IoBNT experimentation requires advanced testbeds that capture multi-scale biological and network dynamics. These platforms integrate molecular, cellular, and communication components, with real-time monitoring and fault-injection capabilities. Digital twins complement testbeds by simulating biological states, enabling predictive analysis and attack testing. Challenges include modeling fidelity, synchronization, and data management. Current research highlights the need for scalable, hybrid virtual–physical platforms to support secure IoBNT validation and optimization [3][16].

10.11. Cross-disciplinary collaboration

IoBNT security requires collaboration across biology, nanotechnology, communications, AI, medicine, and ethics. Interdisciplinary efforts enable the design of biologically compatible and technically robust security mechanisms. Clinicians, engineers, and data scientists must jointly address privacy, safety, and performance challenges. Studies emphasize hybrid approaches combining AI, cryptography, and domain expertise to address evolving threats. Cross-disciplinary collaboration remains essential for developing secure, scalable, and ethically sound IoBNT systems [18][77].

10.12. Hybrid security models

Hybrid security architectures integrate cryptography, physical-layer techniques, and AI-based detection to meet the constraints of IoBNT. Lightweight cryptography secures communication, while physical-layer features enable device authentication without heavy key management. AI models such as CNN–LSTM improve anomaly detection and adaptive response. Digital twins and FL enhance privacy and scalability. Current research highlights the effectiveness of multi-layer hybrid frameworks in improving resilience and energy efficiency against complex attacks [3][97].

10.13. Biocompatible cryptography

Biocompatible cryptography adapts security mechanisms to biological environments using non-toxic, ultra-lightweight approaches. These methods exploit biochemical properties such as pH, temperature, and molecular interactions for key generation and authentication. DNA-based keys, enzyme-mediated protocols, and molecular randomness provide secure and efficient alternatives to conventional cryptography. Physical channel characteristics can also serve as intrinsic fingerprints for device identification. Research highlights the need for biologically compatible, energy-efficient cryptographic solutions integrated with IoBNT systems [18][67].

10.14. Autonomous and adaptive bio-nano security mechanisms

IoBNT systems require autonomous, adaptive security that can operate under extreme resource constraints. These mechanisms monitor environmental and molecular signals to detect and respond to threats in real time. Techniques include lightweight ML, reinforcement learning, and bio-inspired algorithms for dynamic defense. Self-healing systems can isolate compromised nodes and reconfigure network behavior. Studies demonstrate the effectiveness of immune-inspired and FL-based approaches in improving detection accuracy and energy efficiency [148][149].

10.15. Secure and trustworthy key management

Efficient key management is essential for securing IoBNT systems with limited resources and dynamic topologies. Lightweight cryptographic primitives and channel-based key generation provide viable alternatives to traditional PKI. Context-aware key distribution supports mobility and physiological variability. Blockchain enables decentralized trust and secure authentication, while FL enhances privacy. Future research should address post-quantum resilience, energy efficiency, and secure key lifecycle management [150].

10.16. PQC for IoBNT

Quantum computing poses a threat to conventional cryptographic schemes, necessitating post-quantum solutions for IoBNT. Promising approaches include lattice-based, code-based, multivariate, and hash-based cryptography. However, their implementation is challenging due to constraints in nano-devices. Research should focus on lightweight, hardware-aware, and energy-efficient post-quantum designs. Hybrid frameworks combining classical and quantum-resistant methods, with offloading to gateways, can support practical deployment and interoperability [151].

10.17. Distributed ledger and blockchain-based identity & trust

Blockchain enables decentralized identity and trust management in IoBNT systems without relying on central authorities. It supports secure device registration, authentication, and data integrity through smart contracts and immutable ledgers. Lightweight and scalable designs, including DAG-based and hybrid consensus mechanisms, address the constraints of nano-devices. Integration with edge computing improves efficiency and interoperability. Research highlights the role of blockchain in ensuring trust, traceability, and secure data sharing in IoBNT environments [116].

10.18. Immune-aware security solutions

Immune-inspired security mechanisms provide adaptive and self-organizing protection for IoBNT systems. Artificial immune systems detect anomalies, classify threats, and adapt over time. These systems support collaborative defense, enabling nodes to alert others and mitigate attacks. Self-healing capabilities allow networks to isolate compromised components and maintain functionality. Integration with AI, cryptography, and blockchain enhances resilience and scalability in dynamic environments [152].

10.19. Energy-efficient security mechanisms

Energy efficiency is a critical constraint in IoBNT due to limited power sources. Security mechanisms must minimize computational and communication overhead while maintaining protection. Techniques include lightweight cryptography, adaptive protocols, and energy-aware key management. Offloading tasks to gateways and synchronizing operations with energy availability improves efficiency. Research emphasizes cross-layer designs and adaptive strategies to balance security, performance, and device longevity [153].

10.20. AI-accelerated adaptive security policies

AI enables dynamic and context-aware security policies in IoBNT systems. Reinforcement learning optimizes access control, while DL models detect anomalies and predict vulnerabilities. These systems adapt in real time based on network

conditions and threat patterns. FL preserves privacy while enabling collaborative intelligence. Current research demonstrates high detection accuracy and highlights AI-driven orchestration as a key direction for scalable and efficient IoBNT security [3][92].

10.21. Large-scale deployment and big data security

Scaling IoBNT systems requires managing large numbers of heterogeneous devices while ensuring secure and efficient data handling. Hierarchical and cluster-based architectures support reliability, synchronization, and load balancing. Security mechanisms include lightweight encryption, FL, and privacy-preserving data aggregation. Integration with cloud and big data platforms necessitates secure storage, access control, and regulatory compliance. Current research highlights the importance of scalable, privacy-aware frameworks for managing high-volume biological data [3].

Pursuing these research directions will collectively enable the development of secure, resilient, and trustworthy IoBNT systems, thereby supporting their practical deployment and safe, effective integration into real-world applications.

11. CONCLUSION

The IoBNT represents a transformative paradigm that connects biological systems with digital networks, enabling advances in precision medicine, environmental monitoring, and bio-hybrid computing. As IoBNT architectures evolve, security has become a fundamental requirement. This survey provides a comprehensive and up-to-date overview of the IoBNT security landscape by examining communication protocols, threat models, mitigation strategies, technological integrations, analytical tools, and performance metrics. It aims to present a cohesive framework for designing, evaluating, and optimizing security across the IoBNT ecosystem.

IoBNT security challenges extend beyond those of conventional wireless and IoT networks due to the unique properties of bio-nano communication. Molecular signaling, nanomaterial interfaces, intra-body channels, and wet-lab constraints introduce novel attack vectors and complex cyber-biological risks. Although existing mitigation strategies show promise, they remain fragmented and often lack rigorous experimental validation. In addition, the absence of standardized security benchmarks and interoperable protocol stacks limits consistent implementation across diverse application domains.

Emerging technological integrations offer significant opportunities to enhance IoBNT security and resilience. Approaches such as AI-driven anomaly detection, blockchain-based trust management, PQC, nanosensor fusion, and synthetic biology safeguards can strengthen security frameworks. However, practical deployment remains challenging due to extreme nano-scale resource constraints, complex biological environments, and unresolved safety and ethical concerns. Furthermore, while simulation platforms and analytical tools provide useful insights, many rely on oversimplified biological models and lack comprehensive support for cross-layer security evaluation.

Performance evaluation in IoBNT security is evolving alongside these technological developments. Traditional metrics, such as latency, reliability, energy consumption, and throughput, remain important, but bio-specific criteria are increasingly critical. These include biocompatibility, tolerance to biochemical noise, robustness of molecular propagation, and minimal invasiveness. Establishing a comprehensive set of tailored performance metrics is therefore essential to enable fair comparisons and guide effective protocol design.

Addressing IoBNT security requires a multidisciplinary approach that integrates nanoengineering, synthetic biology, wireless communication, cybersecurity, and computational intelligence. By consolidating current knowledge and identifying critical gaps, this survey supports researchers and practitioners in developing secure and trustworthy IoBNT systems. As the field advances from conceptual models to real-world applications, robust, holistic security architectures will be essential to ensuring safe and impactful societal integration.

Conflicts of Interest

The authors should pledge that they don’t have any conflict of interest in regards of their research. If there are no conflict of interest then authors can declare the following "The authors declare no conflicts of interest".

Funding

The funding section of your journal paper template should provide a concise and transparent declaration of the financial support received to carry out the research presented in your paper.

Acknowledgment

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks ...”. Instead, try “R. B. G. thanks...”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

References

[1] A. Yadav, A. Kumar, E. Shitiri, S. Kumar, and H. Cho, "Non-Data-Aided SNR Estimation for Molecular Communication Systems in Internet of Bio-Nano Things," *IEEE Internet Things J.*, vol. 12, pp. 595–604, 2025, doi: 10.1109/JIOT.2024.3465495.

[2] D. Jing, L. Lin, and A. W. Eckford, "Optimal Energy Allocation for Cooperative Molecular Communication With Imperfect Transmitters in Internet of Bio-Nano Things," *IEEE Internet Things J.*, vol. 12, no. 22, pp. 48351–48361, 2025, doi: 10.1109/JIOT.2025.3605211.

[3] M. B. Jamshidi, D. T. Hoang, D. N. Nguyen, D. Niyato, and M. E. Warkiani, "Revolutionizing Biological Digital Twins: Integrating Internet of Bio-Nano Things, Convolutional Neural Networks, and Federated Learning," *Comput. Biol. Med.*, vol. 189, Art. no. 109970, 2025, doi: 10.1016/j.compbiomed.2025.109970.

[4] Y. Sun, W. Cheng, Q. Wang, K. Yang, and Y. Chen, "Advancing the Internet of Bio-Nano Things: A Novel DNA-Based Track-Hopper System for Enhanced Efficiency and Reliability," *IEEE Internet Things J.*, vol. 12, pp. 4144–4157, 2025, doi: 10.1109/JIOT.2024.3482722.

[5] L. Yadav and V. Sharma, "Journey Toward Internet of Bio-Nano Things: Evolution, Trends, and Future Challenges," in *Future of Internet of Bio-Nano Things in Personalized Healthcare*. Amsterdam, The Netherlands: Elsevier, 2025, pp. 1–22, doi: 10.1016/B978-0-443-27604-0.00014-7.

[6] R. Khanzadeh *et al*., "Explainable Asymmetric Auto-Encoder for End-to-End Learning of IoBNT Communications," in *Proc. IEEE Int. Conf. Mach. Learn. Commun. Netw. (ICMLCN)*, Stockholm, Sweden, May 2024, pp. 412–418, doi: 10.1109/ICMLCN59089.2024.10624774.

[7] M. Jamshidi, D. Hoang, and D. Nguyen, "CNN-FL for Biotechnology Industry Empowered by Internet-of-BioNano Things and Digital Twins," *IEEE Internet Things Mag.*, vol. 7, pp. 54–63, 2024, doi: 10.1109/IOTM.001.2400081.

[8] W. Cheng, J. Fu, Q. Wang, K. Yang, Y. Chen, and Y. Sun, "AoI-OptiIoBNT: Age of Information-Driven DNA-Based Internet of Bio-Nano Things Optimization," *IEEE Internet Things J.*, vol. 12, pp. 28214–28228, 2025, doi: 10.1109/JIOT.2025.3566219.

[9] P. K. Bulasara, S. Sahoo, N. Gupta, Z. Han, and N. Kumar, "The Internet of Bio-Nano Things With Insulin-Glucose, Security and Research Challenges: A Survey," *ACM Comput. Surv.*, vol. 57, no. 5, pp. 1–42, 2024, doi: 10.1145/3703448.

[10] B. Thiyagaraj, "Edge AI and Internet of Bio-Nano Things (IoBNT): Revolutionizing Smart Healthcare and Bioengineering Applications," *Int. J. Mod. Sci. Discov.*, vol. 1, no. 1, pp. 9–15, 2025, doi: 10.64137/31079377/IJMSD-V1I1P102.

[11] P. Srivastava *et al*., "Exploring the Internet of Bio-Nano Things: Technologies, Applications, and Challenges," *J. Inf. Syst. Eng. Manage.*, vol. 9, no. 4s, pp. 81–118, 2024, doi: 10.52783/JISEM.V9I4S.11014.

[12] N. Sathish, V. Yokesh, A. Prasanth, and P. C. Thang, "Security and Privacy Aspects of Internet of Bio-Nano Things (Confidentiality, Integrity, Availability, Authentication)," in *Future of Internet of Bio-Nano Things in Personalized Healthcare*. Amsterdam, The Netherlands: Elsevier, 2026, pp. 139–154, doi: 10.1016/B978-0-443-27604-0.00003-2.

[13] S. Bhattacharjee *et al*., "Exhaled Breath Analysis Through the Lens of Molecular Communication: A Survey," *IEEE Commun. Surveys Tuts.*, vol. 28, pp. 412–445, 2026, doi: 10.1109/COMST.2025.3605748.

[14] Y. Tang, Q. Wang, Z. Hao, Z. Ma, W. Gao, and L. Yang, "Molecular Code Index Modulation: Signaling, Detection, and Performance Analysis," *IEEE Trans. Mol. Biol. Multi-Scale Commun.*, vol. 12, pp. 208–217, 2026, doi: 10.1109/TMBMC.2025.3605778.

[15] H. Cai and O. B. Akan, "Semantic Learning for Molecular Communication in Internet of Bio-Nano Things," *arXiv*, Feb. 2025, doi: 10.48550/arXiv.2502.08426.

[16] X. Huang, J. Liu, L. Lin, M. Wen, W. Gan, and Y. Huang, "Capacitive Sensing in High-Speed Molecular Communication System: A Noninvasive Interface for Internet of Bio-Nano Things," *IEEE Internet Things J.*, vol. 12, pp. 16711–16719, 2025, doi: 10.1109/JIOT.2025.3534166.

[17] M. Ramachandran, T. Prathiba, S. Jayachitra, and A. Prasanth, "Next-Generation Terahertz Communication Protocols for Internet of Bio-Nano Things and Future Networking Paradigms," in *Future of Internet of Bio-Nano Things in*

Personalized Healthcare. Amsterdam, The Netherlands: Elsevier, 2026, pp. 59–74, doi: 10.1016/B978-0-443-27604-0.00008-1.

[18] J. T. Gómez *et al*., "Communicating Smartly in Molecular Communication Environments: Neural Networks in the Internet of Bio-Nano Things," *arXiv*, Jun. 2025, doi: 10.48550/arXiv.2506.20589.

[19] Z. Jin, H. Luo, B. Jiang, Y. Chen, and L. Lin, "An Engineered Neural Communication System Based on CDM Scheme for the Internet of Bio-Nano Things," *IEEE Trans. Mol. Biol. Multi-Scale Commun.*, vol. 12, pp. 1–10, 2026, doi: 10.1109/TMBMC.2025.3606625.

[20] I. Kamal, S. El-Atty, S. El-Zoghdy, and R. Soliman, "Intelligent Deep Learning Model for Targeted Cancer Drug Delivery," *Sci. Rep.*, vol. 15, pp. 1–17, 2025, doi: 10.1038/S41598-025-96149-6.

[21] Z. Jia, L. Ma, J. Zhu, and X. Jiang, "Secrecy Capacity in Two-Hop Diffusive Molecular Communication Systems," *Comput. Netw.*, vol. 272, Art. no. 111659, 2025, doi: 10.1016/j.comnet.2025.111659.

[22] S. Aqeel, A. Khan, I. Abbasi, F. Algarni, and D. Grzonka, "Enhancing IoT Security With a DNA-Based Lightweight Cryptography System," *Sci. Rep.*, vol. 15, 2025, doi: 10.1038/S41598-025-96292-0.

[23] A. El-Sayed, A. Toony, F. Alqahtani, Y. Alginahi, and W. Said, "CO-STOP: A Robust P4-Powered Adaptive Framework for Comprehensive Detection and Mitigation of Coordinated and Multi-Faceted Attacks in SD-IoT Networks," *Comput. Secur.*, vol. 151, Art. no. 104349, 2025, doi: 10.1016/j.cose.2025.104349.

[24] H. Fang, L. Xu, G. Nan, D. Zheng, H. Zhao, and X. Wang, "Accountable Distributed Access Control With Privacy Preservation for Blockchain-Enabled Internet of Things Systems: A Zero-Trust Security Scheme," *IEEE Internet Things J.*, vol. 12, pp. 17936–17947, 2025, doi: 10.1109/JIOT.2025.3540868.

[25] Z. Guo, "Blockchain-Enhanced Smart Contracts for Formal Verification of IoT Access Control Mechanisms," *Alexandria Eng. J.*, vol. 118, pp. 315–324, 2025, doi: 10.1016/j.aej.2024.12.109.

[26] D. Ionescu, A. Filipescu, G. Simion, and A. Filipescu, "Internet of Things-Cloud Control of a Robotic Cell Based on Inverse Kinematics, Hardware-in-the-Loop, Digital Twin, and Industry 4.0/5.0," *Sensors*, vol. 25, no. 6, Art. no. 1821, 2025, doi: 10.3390/S25061821.

[27] M. Albay, E. Akyol, F. Mirlou, L. Beker, and M. Kuscu, "Low-Cost Microfluidic Testbed for Molecular Communications With Integrated Hydrodynamic Gating and Screen-Printed Sensors," *arXiv*, Jan. 2025, doi: 10.48550/arXiv.2501.19341.

[28] N. Briantceva, L. Chouhan, M. Parsani, and M. Alouini, "On Error Rate Reduction in Sub-Diffusion-Based Mobile Molecular Communication," *IEEE Trans. Mol. Biol. Multi-Scale Commun.*, vol. 11, pp. 107–115, 2025, doi: 10.1109/TMBMC.2024.3522010.

[29] R. Mustafa, N. I. Sarkar, M. Mohaghegh, S. Pervez, and R. Morados, "A Secure and Energy-Efficient Cross-Layer Network Architecture for the Internet of Things," *Sensors*, vol. 25, no. 11, Art. no. 3457, 2025, doi: 10.3390/S25113457.

[30] L. F. Borges, M. T. Barros, and M. Nogueira, "Cell Signaling Error Control for Reliable Molecular Communications," *Front. Commun. Netw.*, vol. 5, pp. 1–16, 2024, doi: 10.3389/FRCMN.2024.1332379.

[31] M. Pasupuleti, "Internet of Bio-Nano Things: A Foundational Framework for Next-Generation Biomedical Networks," *Int. J. Acad. Ind. Res. Innov.*, vol. 5, no. 7, pp. 1–16, 2025, doi: 10.62311/NESX/RPJ1.

[32] S. Angerbauer, F. Enzenhofer, T. Pankratz, M. Hamidović, A. Springer, and W. Haselmayr, "Novel Nano-Scale Computing Unit for the IoBNT: Concept and Practical Considerations," *IEEE Trans. Mol. Biol. Multi-Scale Commun.*, vol. 10, pp. 549–565, 2024, doi: 10.1109/TMBMC.2024.3397050.

[33] S. M. A. El-Atty, P. Vijayakumar, O. Alfarraj, M. Karuppiah, and F. Shawki, "Bioinspired Molecular Communications System for Targeted Drug Delivery With IoBNT-Based Sustainable Biocyber Interface," *Comput. Electr. Eng.*, vol. 118, Art. no. 109452, 2024, doi: 10.1016/j.compeleceng.2024.109452.

[34] D. Jing, L. Lin, and A. Eckford, "Energy Allocation for Multiuser Cooperative Molecular Communication Systems in Internet of Bio-Nano Things," *IEEE Internet Things J.*, vol. 11, pp. 16303–16313, 2024, doi: 10.1109/JIOT.2024.3353329.

[35] Y. Liu and B. Wang, "Advanced Applications in Chronic Disease Monitoring Using IoT Mobile Sensing Device Data, Machine Learning Algorithms and Frame Theory: A Systematic Review," *Front. Public Health*, vol. 13, 2025, doi: 10.3389/FPUBH.2025.1510456.

[36] H. Bae *et al*., "Artificial Intelligence-Driven Nanoarchitectonics for Smart Targeted Drug Delivery," *Adv. Mater.*, Art. no. e10239, 2025, doi: 10.1002/ADMA.202510239.

[37] K. Wang, S. Jiang, W. Wang, W. Chen, and T. Kai, "Dual-miRNA Guided In-Vivo Imaging and Multimodal Nanomedicine Approaches for Precise Hepatocellular Carcinoma Differentiation and Synergistic Cancer Theranostics Using DNA Hairpins and Dual-Ligand Functionalized Zirconium-MOF Nanohybrids," *Biomaterials*, vol. 321, Art. no. 123330, 2025, doi: 10.1016/j.biomaterials.2025.123330.

[38] N. Parthasarathy *et al*., "Biomolecule-Based Engineered Nanoparticles for Cancer Theranostics," *Coord. Chem. Rev.*, vol. 530, Art. no. 216489, 2025, doi: 10.1016/j.ccr.2025.216489.

[39] S. Fischer, "The Internet of Bio-Nano Things—Smart Computing in the Human Body," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Osaka, Japan, Jun.–Jul. 2024, p. 2, doi: 10.1109/SMARTCOMP61445.2024.00019.

[40] X. Chen, Y. Huang, M. Wen, S. Mumtaz, F. Gulec, A. Al-Dulaimi, and A. Eckford, "Empowering Nanoscale Connectivity Through Molecular Communication: A Case Study of Virus Infection," *IEEE Commun. Mag.*, vol. 63, pp. 182–188, 2025, doi: 10.1109/MCOM.005.2400029.

[41] T. Bakhshi and S. Zafar, "Hybrid Deep Learning Techniques for Securing Bioluminescent Interfaces in Internet of Bio Nano Things," *Sensors*, vol. 23, no. 21, Art. no. 8972, 2023, doi: 10.3390/S23218972.

[42] M. Civas, M. Kuscu, O. Cetinkaya, B. E. Ortlek, and O. B. Akan, "Graphene and Related Materials for the Internet of Bio-Nano Things," *APL Mater.*, vol. 11, no. 8, pp. 1–24, 2023, doi: 10.1063/5.0153423.

[43] D. Rajagopal and P. Subramanian, "AI-Augmented Edge and Fog Computing for Internet of Health Things (IoHT)," *PeerJ Comput. Sci.*, vol. 11, 2025, doi: 10.7717/peerj-cs.2431.

[44] N. Fernando, S. Shrestha, S. W. Loke, and K. Lee, "On Edge-Fog-Cloud Collaboration and Reaping Its Benefits: A Heterogeneous Multi-Tier Edge Computing Architecture," *Future Internet*, vol. 17, no. 1, Art. no. 22, 2025, doi: 10.3390/FI17010022.

[45] H. Kuchuk, Y. Husieva, S. Novoselov, D. Lysytsia, and H. Krykhovetskyi, "Load Balancing of the Layers IoT Fog-Cloud Support Network," *Adv. Inf. Syst.*, vol. 9, no. 1, pp. 91–98, 2025, doi: 10.20998/2522-9052.2025.1.11.

[46] S. Qiu, Z. Wei, Y. Huang, M. Abbaszadeh, J. Charmet, B. Li, and W. Guo, "Review of Physical Layer Security in Molecular Internet of Nano-Things," *IEEE Trans. Nanobiosci.*, vol. 23, no. 1, pp. 91–100, 2023, doi: 10.1109/TNB.2023.3285973.

[47] A. Alabdulatif, N. N. Thilakarathne, Z. K. Lawal, K. E. Fahim, and R. Y. Zakari, "Internet of Nano-Things (IoNT): A Comprehensive Review From Architecture to Security and Privacy Challenges," *Sensors*, vol. 23, no. 5, Art. no. 2807, 2023, doi: 10.3390/S23052807.

[48] S. M. A. El-Atty, K. A. Lizos, O. Alfarraj, and F. Shawki, "Internet of Bio Nano Things-Based FRET Nanocommunications for eHealth," *Math. Biosci. Eng.*, vol. 20, no. 5, pp. 9246–9267, 2023, doi: 10.3934/MBE.2023405.

[49] M. Rezaei *et al*., "Spheroidal Molecular Communication via Diffusion: Signaling Between Homogeneous Cell Aggregates," *IEEE Trans. Mol. Biol. Multi-Scale Commun.*, vol. 10, pp. 197–210, 2024, doi: 10.1109/TMBMC.2024.3366420.

[50] S. Parveez and S. Gupta, "Analyzing Effect of Spreading and Absorption Losses on Performance of Nano-Network Operating at Terahertz Frequency Band," *Int. J. Syst. Assur. Eng. Manage.*, vol. 15, pp. 2529–2540, 2024, doi: 10.1007/S13198-024-02274-2.

[51] W. Jiang *et al*., "Terahertz Communications and Sensing for 6G and Beyond: A Comprehensive Review," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 4, pp. 2326–2381, 2024, doi: 10.1109/COMST.2024.3385908.

[52] Y. Xing *et al*., "Integrated Opposite Charge Grafting Induced Ionic-Junction Fiber," *Nat. Commun.*, vol. 14, 2023, doi: 10.1038/S41467-023-37884-0.

[53] A. Hamza, A. Al-Dulaimi, J. Bouillard, and A. Adawi, "Long-Range and High-Efficiency Plasmon-Assisted Förster Resonance Energy Transfer," *J. Phys. Chem. C*, vol. 127, pp. 21611–21616, 2023, doi: 10.1021/ACS.JPCC.3C04281.

[54] I. Khalin *et al*., "Nanocarrier Drug Release and Blood-Brain Barrier Penetration at Post-Stroke Microthrombi Monitored by Real-Time Förster Resonance Energy Transfer," *ACS Nano*, vol. 19, pp. 14780–14794, 2025, doi: 10.1021/ACSNANO.4C17011.

[55] L. Petrosyan, M. Noginov, and T. Shahbazyan, "Förster Resonance Energy Transfer in Inhomogeneous and Absorptive Environments," *J. Chem. Phys.*, vol. 163, no. 5, 2025, doi: 10.1063/5.0276433.

[56] L. Lin, W. Chen, Y. Huang, and J. Xu, "Mutual Information for Neural Communication With Spike-Time Dependent Plasticity and Consolidation Effect," *IEEE Access*, vol. 12, pp. 129648–129659, 2024, doi: 10.1109/ACCESS.2024.3453400.

[57] J. Li and X. Yang, "Advances in Bioelectronics for Neural Interfacing," *MRS Commun.*, pp. 1–14, 2025, doi: 10.1557/S43579-025-00822-W.

[58] L. Chouhan and M. Alouini, "Interfacing of Molecular Communication System With Various Communication Systems Over Internet of Every Nano Things," *IEEE Internet Things J.*, vol. 10, pp. 14552–14568, 2023, doi: 10.1109/JIOT.2023.3273030.

[59] B. A. Asi, F. E. Mahmood, and N. I. Najim, "Breaking Barriers In-Vivo THZ Communication Analysis for Nano Networks in Human Tissues," *Period. Polytech. Electr. Eng. Comput. Sci.*, vol. 69, no. 1, pp. 26–32, 2025, doi: 10.3311/PPEE.37844.

[60] L. Dzamesi and N. Elsayed, "A Review on the Security Vulnerabilities of the IoMT Against Malware Attacks and DDoS," in *Proc. IEEE 4th Int. Conf. Comput. Mach. Intell. (ICMI)*, MI, USA, Apr. 2025, pp. 1–8, doi: 10.1109/ICMI65310.2025.11141098.

[61] A. Hlybovets, S. Shcherbyna, and O. Kyriienko, "Security Vulnerabilities and Protection Solutions in Internet of Things Systems," *NaUKMA Res. Pap. Comput. Sci.*, vol. 7, pp. 89–97, 2025, doi: 10.18523/2617-3808.2024.7.89-97.

[62] S. Szymoniak, J. Piątkowski, and M. Kurkowski, "Defense and Security Mechanisms in the Internet of Things: A Review," *Appl. Sci.*, vol. 15, no. 2, Art. no. 499, 2025, doi: 10.3390/APP15020499.

[63] L. Vidyashree and R. S. Anusha, "The Emergence of the Internet of Things: Analyze and Address Research Questions Concerning the Recognition and Mitigation Against IoT-Based Security Attacks," *Int. J. Environ. Sci.*, vol. 11, no. 23s, pp. 1–15, 2025.

[64] M. Anjum, N. Kraiem, H. Min, A. Dutta, Y. Daradkeh, and S. Shahab, "Opportunistic Access Control Scheme for Enhancing IoT-Enabled Healthcare Security Using Blockchain and Machine Learning," *Sci. Rep.*, vol. 15, pp. 1–28, 2025, doi: 10.1038/S41598-025-90908-1.

[65] M. Asif *et al*., "Intelligent Two-Phase Dual Authentication Framework for Internet of Medical Things," *Sci. Rep.*, vol. 15, no. 1, Art. no. 1760, 2025, doi: 10.1038/S41598-024-84713-5.

[66] G. Borghini, S. Caputo, S. Jayousi, M. Magarini, M. Pierobon, and L. Mucchi, "Security Threats in Diffusion-Based Molecular Communication Systems," in *Proc. 19th Int. Symp. Med. Inf. Commun. Technol. (ISMICT)*, Florence, Italy, May 2025, pp. 1–6, doi: 10.1109/ISMICT64722.2025.11059392.

[67] T. Zhukabayeva, Z. Ahmad, A. Adamova, N. Karabayev, and A. Abdildayeva, "An Edge-Computing-Based Integrated Framework for Network Traffic Analysis and Intrusion Detection to Enhance Cyber-Physical System Security in Industrial IoT," *Sensors*, vol. 25, no. 8, Art. no. 2395, 2025, doi: 10.3390/S25082395.

[68] E. Ince and M. Kuscu, "Hijacking Living Cells With Surface Engineering for the Internet of Bio-Nano Things," *arXiv*, 2025, doi: 10.48550/arXiv.2509.17227.

[69] S. Bommana, S. Veeramachaneni, S. Ershad, and M. Srinivas, "Mitigating Side Channel Attacks on FPGA Through Deep Learning and Dynamic Partial Reconfiguration," *Sci. Rep.*, vol. 15, pp. 1–10, 2025, doi: 10.1038/S41598-025-98473-3.

[70] I. R. Kamal, S. M. A. El-Atty, S. F. El-Zoghdy, and R. F. Soliman, "Explainable AI for Gastrointestinal Lesion Surveillance and Precision Targeted Drug Delivery," *Sci. Rep.*, vol. 16, no. 1, pp. 1–25, 2026, doi: 10.1038/S41598-026-40882-Z.

[71] M. Ferrag *et al*., "Edge Learning for 6G-Enabled Internet of Things: A Comprehensive Survey of Vulnerabilities, Datasets, and Defenses," *IEEE Commun. Surveys Tuts.*, vol. 25, pp. 2654–2713, 2023, doi: 10.1109/COMST.2023.3317242.

[72] I. R. Kamal, S. M. A. El-Atty, S. F. El-Zoghdy, and R. F. Soliman, "Internet of Bio-NanoThings Privacy: Securing a Multi-Compartmental Targeted Cancer Drug Delivery Scheme," *Multimed. Tools Appl.*, vol. 83, no. 33, pp. 79235–79258, 2024, doi: 10.1007/S11042-024-18423-5.

[73] S. Deb *et al*., "Securing the Internet of Medical Things (IoMT): Real-World Attack Taxonomy and Practical Security Measures," *arXiv*, Jul. 2025, doi: 10.48550/arXiv.2507.19609.

[74] A. Khan *et al*., "A Lightweight Scalable Hybrid Authentication Framework for Internet of Medical Things (IoMT) Using Blockchain Hyperledger Consortium Network With Edge Computing," *Sci. Rep.*, vol. 15, pp. 1–20, 2025, doi: 10.1038/S41598-025-05130-W.

[75] A. Alshehri *et al*., "IoT Authentication Protocols: Challenges and Comparative Analysis," *ACM Comput. Surv.*, vol. 57, pp. 1–43, 2024, doi: 10.1145/3703444.

[76] S. Asaithambi *et al*., "A Secure and Trustworthy Blockchain-Assisted Edge Computing Architecture for Industrial Internet of Things," *Sci. Rep.*, vol. 15, pp. 1–17, 2025, doi: 10.1038/S41598-025-00337-3.

[77] A. Rana, D. Gautam, P. Kumar, and A. Das, "Architectures, Benefits, Security, and Privacy Issues of Internet of Nano Things: A Comprehensive Survey, Opportunities, and Research Challenges," *IEEE Commun. Surveys Tuts.*, vol. 27, pp. 1152–1190, 2025, doi: 10.1109/COMST.2024.3423477.

[78] M. Aleisa, "Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments," *IEEE Access*, vol. 13, pp. 18660–18676, 2025, doi: 10.1109/ACCESS.2025.3529309.

[79] M. Jarwar, J. Watson, and S. Ali, "Modeling Industrial IoT Security Using Ontologies: A Systematic Review," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 2792–2821, 2025, doi: 10.1109/OJCOMS.2025.3532224.

[80] M. Khatun, S. Memon, C. Eising, and L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," *IEEE Access*, vol. 11, pp. 145869–145896, 2023, doi: 10.1109/ACCESS.2023.3346320.

[81] A. Rana, S. Prajapat, P. Kumar, and C. Chen, "Designing a Security Framework Based on Hybrid Communication in Internet of Nano Things," *IEEE Internet Things J.*, vol. 11, pp. 7265–7284, 2024, doi: 10.1109/JIOT.2023.3315712.

[82] S. Prajapat, A. Rana, P. Kumar, and A. Das, "Quantum Safe Lightweight Encryption Scheme for Secure Data Sharing in Internet of Nano Things," *Comput. Electr. Eng.*, vol. 117, Art. no. 109253, 2024, doi: 10.1016/j.compeleceng.2024.109253.

[83] N. Kumar and R. Ali, "A Smart Contract-Based 6G-Enabled Authentication Scheme for Securing Internet of Nano Medical Things Network," *Ad Hoc Netw.*, vol. 163, Art. no. 103606, 2024, doi: 10.1016/j.adhoc.2024.103606.

[84] G. Thakur, P. Chouksey, M. Chopra, and P. Sadotra, "Edge-Optimized Lightweight Cryptographic Protocol (ELCP) for Secure IoT Communications in Resource-Constrained Environments," *J. Inf. Syst. Eng. Manage.*, vol. 10, no. 45s, pp. 1199–1211, 2025, doi: 10.52783/JISEM.V10I45S.9146.

[85] H. Y. Naser, A. K. Mattar, M. A. Saare, M. A. Almaiah, and R. Shehab, "A Comparison of Lightweight Cryptographic Protocols for Energy-Efficient and Sustainable IoMT Authentication," *Eng. Technol. Appl. Sci. Res.*, vol. 15, no. 4, pp. 25746–25756, 2025, doi: 10.48084/ETASR.12204.

[86] W. Labidi, V. Gholamian, Y. Zhao, C. Deppe, and H. Boche, "Secure Event-Triggered Molecular Communication—Information Theoretic Perspective and Optimal Performance," *IEEE Trans. Mol. Biol. Multi-Scale Commun.*, vol. 12, pp. 265–278, 2025, doi: 10.1109/TMBMC.2025.3647208.

[87] Y. Yao, X. Zhang, X. Liu, X. Zhang, B. Wang, and Q. Zhang, "Programmable DNA Hairpin Locker: Dual-Layer Encrypted Carrier Communication," *ACS Nano*, vol. 19, no. 27, pp. 24763–24772, 2025, doi: 10.1021/ACSNANO.5C01802.

[88] S. Singh, R. Rai, S. Awasthi, D. Singh, and M. Lakshmanan, "VLSI Implementation of Error Correction Codes for Molecular Communication," *Wireless Pers. Commun.*, vol. 130, pp. 2697–2713, 2023, doi: 10.1007/S11277-023-10399-Z.

[89] V. Padmavathi and R. Saminathan, "A Federated Edge Intelligence Framework With Trust-Based Access Control for Secure and Privacy-Preserving IoT Systems," *Sci. Rep.*, vol. 15, no. 1, Art. no. 35832, 2025, doi: 10.1038/S41598-025-19712-1.

[90] Z. Lygizou and D. Kalles, "A Biologically Inspired Trust Model for Open Multi-Agent Systems That Is Resilient to Rapid Performance Fluctuations," *arXiv*, Apr. 2025, doi: 10.48550/arXiv.2504.15301.
[91] Y. Zhang, P. Duan, C. Li, H. Zhang, and H. Ahmad, "Preserving Privacy of Internet of Things Network With Certificateless Ring Signature," *Sensors*, vol. 25, no. 5, Art. no. 1321, 2025, doi: 10.3390/S25051321.
[92] M. Elkhodr, "An AI-Driven Framework for Integrated Security and Privacy in Internet of Things Using Quantum-Resistant Blockchain," *Future Internet*, vol. 17, no. 6, Art. no. 246, 2025, doi: 10.3390/FI17060246.
[93] B. Kara, C. Eyupoglu, and O. Karakuş, "(r, k, ε)-Anonymization: Privacy-Preserving Data Publishing Algorithm Based on Multi-Dimensional Outlier Detection, k-Anonymity, and ε-Differential Privacy," *IEEE Access*, vol. 13, pp. 70422–70435, 2025, doi: 10.1109/ACCESS.2025.3559410.
[94] N. Islam, S. Pal, and S. Misra, "QBaN: Quantum Bacterial Nanonetworks for Secure Molecular Communication," *IEEE Trans. Mol. Biol. Multi-Scale Commun.*, vol. 10, pp. 633–641, 2024, doi: 10.1109/TMBMC.2024.3476192.
[95] Y. Huang, M. Wen, L. Lin, B. Li, Z. Wei, D. Tang, J. Li, W. Duan, and W. Guo, "Physical-Layer Counterattack Strategies for the Internet of Bio-Nano Things With Molecular Communication," *IEEE Internet Things Mag.*, vol. 6, pp. 82–87, 2023, doi: 10.1109/IOTM.001.2300029.
[96] A. Rizzardi, G. Piro, S. Sicari, L. Grieco, and A. Coen-Porisini, "Bio-Molecular Cryptography for Protecting Nano-Network Transmissions in Healthcare Applications," in *Proc. 13th Wireless Days (WD)*, Niterói, Brazil, Dec. 2025, pp. 1–9, doi: 10.1109/WD67713.2025.11302720.
[97] N. Naik *et al*., "Hybrid Deep Learning-Enabled Framework for Enhancing Security, Data Integrity, and Operational Performance in Healthcare Internet of Things (H-IoT) Environments," *Sci. Rep.*, vol. 15, no. 1, Art. no. 31039, 2025, doi: 10.1038/S41598-025-15292-2.
[98] Q. Fan *et al*., "De Novo Non-Canonical Nanopore Basecalling Enables Private Communication Using Heavily-Modified DNA Data at Single-Molecule Level," *Nat. Commun.*, vol. 16, 2025, doi: 10.1038/S41467-025-59357-2.
[99] T. Bakhshi and F. Yousaf, "Securing Bio-FET Interfaces in IoBNT Systems Using Deep Learning Techniques," in *Proc. 17th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Lahore, Pakistan, Dec. 2023, pp. 1–6, doi: 10.1109/ICOSST60641.2023.10414198.
[100] 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," *Artif. Intell. Rev.*, vol. 58, no. 2, pp. 123–189, 2025, doi: 10.1007/S10462-025-01234-6.
[101] D. Ajinkya, K. Balu, P. Ramesh, and P. Nandu, "End-to-End Security Architecture for Internet of Things Systems," *Int. J. Multidiscip. Res.*, vol. 8, no. 1, pp. 1–10, 2026, doi: 10.36948/IJFMR.2026.V08I01.66664.
[102] X. Yang, Z. Wang, S. Yu, D. Li, and S. Chan, "A Knowledge Distillation-Based Lightweight Intrusion Detection Method for the Internet of Things," *Cluster Comput.*, vol. 28, no. 15, pp. 1–14, 2025, doi: 10.1007/S10586-025-05597-2.
[103] J. Srinivasan, "Innovative Cross-Layer Defense Mechanisms for Blackhole and Wormhole Attacks in Wireless Ad Hoc Networks," *Sci. Rep.*, vol. 15, 2025, doi: 10.1038/S41598-025-97094-0.
[104] K. Saleem, "A Comprehensive Analysis of Bio-Inspired Intelligent Mechanisms for Data Communication Security in Cyber-Physical Systems," in *Proc. Int. Conf. Commun., Comput., Netw., Control Cyber-Phys. Syst. (CCNCPS)*, Dubai, United Arab Emirates, Jun. 2025, pp. 367–374, doi: 10.1109/CCNCPS66785.2025.11135692.
[105] U. Kumarasinghe *et al*., "Temporary Silk Nanocoatings Preserve Immune Cell Functions and Protection Against Biochemical and Mechanical Stressors," *Biomaterials*, vol. 325, Art. no. 123605, 2025, doi: 10.1016/j.biomaterials.2025.123605.
[106] S. A. Sathyabama and J. Katiravan, "Enhancing Anomaly Detection and Prevention in Internet of Things Using Deep Neural Networks and Blockchain-Based Cyber Security," *Sci. Rep.*, vol. 15, no. 1, Art. no. 22369, 2025, doi: 10.1038/S41598-025-04164-4.
[107] A. S. Ahanger, S. M. Khan, F. Masoodi, and A. O. Salau, "Advanced Intrusion Detection in Internet of Things Using Graph Attention Networks," *Sci. Rep.*, vol. 15, no. 1, Art. no. 9831, 2025, doi: 10.1038/S41598-025-94624-8.
[108] N. Baban, S. Bhattacharjee, Y.-A. Song, K. Chakrabarty, and R. Karri, "Cyber-Physical Security of Biochips: A Perspective," *Biomicrofluidics*, vol. 19, no. 3, Art. no. 031301, 2025, doi: 10.1063/5.0212607.

[109] A. Pallakonda *et al*., "AI-Driven Attack Detection and Cryptographic Privacy Protection for Cyber-Resilient Industrial Control Systems," *IoT*, vol. 4, no. 3, pp. 456–480, 2025, doi: 10.3390/IOT4030025.

[110] P. K. Samant, V. Pathak, W. Ahmad, and A. Alabdultif, "A Lightweight Trusted Framework for Secure Data Exchange and Threat Mitigation in IoT-Enabled Healthcare Environments," *Sci. Rep.*, vol. 15, no. 1, Art. no. 39248, 2025, doi: 10.1038/S41598-025-22797-3.

[111] M. Rahmati and A. Pagano, "Federated Learning-Driven Cybersecurity Framework for IoT Networks With Privacy-Preserving and Real-Time Threat Detection Capabilities," *Informatics*, vol. 12, no. 3, Art. no. 62, 2025, doi: 10.3390/INFORMATICS12030062.

[112] A. Alfahaid, E. Alalwany, A. M. Almars, F. Alharbi, E. Atlam, and I. Mahgoub, "Machine Learning-Based Security Solutions for IoT Networks: A Comprehensive Survey," *Sensors*, vol. 25, no. 11, Art. no. 3341, 2025, doi: 10.3390/S25113341.

[113] H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review," *Sensors*, vol. 23, no. 2, Art. no. 788, 2023, doi: 10.3390/S23020788.

[114] J. Wu, Z. Bian, H. Gao, and Y. Wang, "A Blockchain-Based Secure Data Transaction and Privacy Preservation Scheme in IoT System," *Sensors*, vol. 25, no. 15, Art. no. 4854, 2025, doi: 10.3390/S25154854.

[115] L. García, C. Cancimance, R. Asorey-Cacheda, C. Zúñiga-Cañón, A. García-Sánchez, and J. García-Haro, "Lightweight Blockchain for Data Integrity and Traceability in IoT Networks," *IEEE Access*, vol. 13, pp. 81105–81117, 2025, doi: 10.1109/ACCESS.2025.3567773.

[116] A. Castiglione, J. G. Esposito, V. Loia, M. Nappi, C. Pero, and M. Polsinelli, "Integrating Post-Quantum Cryptography and Blockchain to Secure Low-Cost IoT Devices," *IEEE Trans. Ind. Informat.*, vol. 21, no. 2, pp. 1674–1683, 2024, doi: 10.1109/TII.2024.3485796.

[117] B. B. Sezer, S. Akleylek, and U. Nuriyev, "PP-PQB: Privacy-Preserving in Post-Quantum Blockchain-Based Systems: A Systematization of Knowledge," *IEEE Access*, vol. 13, pp. 41382–41405, 2025, doi: 10.1109/ACCESS.2025.3545943.

[118] M. T. Ramzan and S. Cimato, "Blockchain in the Quantum Era: Surveying Security Challenges and Post-Quantum Cryptography," in *Proc. IEEE 49th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Toronto, ON, Canada, Jul. 2025, pp. 2218–2223, doi: 10.1109/COMPSAC65507.2025.00311.

[119] N. R. Reddy, S. Suryadevara, K. G. R. Reddy, R. Umamaheswari, R. Guttula, and R. Kotoju, "Quantum Secured Blockchain Framework for Enhancing Post-Quantum Data Security," *Sci. Rep.*, vol. 15, no. 1, Art. no. 31048, 2025, doi: 10.1038/S41598-025-16315-8.

[120] R. Chataut, M. Nankya, and R. Akl, "6G Networks and the AI Revolution—Exploring Technologies, Applications, and Emerging Challenges," *Sensors*, vol. 24, no. 6, Art. no. 1888, 2024, doi: 10.3390/S24061888.

[121] N. Kaur and L. Gupta, "Securing the 6G–IoT Environment: A Framework for Enhancing Transparency in Artificial Intelligence Decision-Making Through Explainable Artificial Intelligence," *Sensors*, vol. 25, no. 3, Art. no. 854, 2025, doi: 10.3390/s25030854.

[122] H. Kuchuk and E. Malokhvii, "Integration of IoT With Cloud, Fog, and Edge Computing: A Review," *Adv. Inf. Syst.*, vol. 8, no. 2, pp. 65–78, 2024, doi: 10.20998/2522-9052.2024.2.08.

[123] G. Walia, M. Kumar, and S. Gill, "AI-Empowered Fog/Edge Resource Management for IoT Applications: A Comprehensive Review, Research Challenges, and Future Perspectives," *IEEE Commun. Surveys Tuts.*, vol. 26, pp. 619–669, 2024, doi: 10.1109/COMST.2023.3338015.

[124] S. Zayed, G. Attiya, A. El-Sayed, and E. Hemdan, "A Review Study on Digital Twins With Artificial Intelligence and Internet of Things: Concepts, Opportunities, Challenges, Tools and Future Scope," *Multimed. Tools Appl.*, pp. 1–27, 2023, doi: 10.1007/s11042-023-15611-7.

[125] P. Hofmann, P. Zhou, C. Lee, M. Reisslein, F. Fitzek, and C. Chae, "OpenFOAM Simulation of Microfluidic Molecular Communications: Method and Experimental Validation," *IEEE Access*, vol. 12, pp. 109494–109512, 2024, doi: 10.1109/ACCESS.2024.3438243.

[126] M. Ali, Y. Chen, and M. Cree, "Semi-Autonomous *In Vivo* Computation in Internet of Bio-Nano Things," *IEEE Internet Things J.*, vol. 10, pp. 16845–16855, 2023, doi: 10.1109/JIOT.2023.3272213.
[127] M. Gattringer, S. Angerbauer, A. Springer, and W. Haselmayr, "Demo: A Testbed for Thermomolecular Communication in the IoBNT," in *Proc. 11th ACM Int. Conf. Nanoscale Comput. Commun. (NANOCOM)*, Milan, Italy, Oct. 2024, pp. 136–137, doi: 10.1145/3686015.3689425.
[128] P. Stano, P. L. Gentili, L. Damiano, and M. Magarini, "A Role for Bottom-Up Synthetic Cells in the Internet of Bio-Nano Things?," *Molecules*, vol. 28, no. 14, Art. no. 5564, 2023, doi: 10.3390/molecules28145564.
[129] M. Antonijevic *et al*., "Intrusion Detection in Metaverse Environment Internet of Things Systems by Metaheuristics Tuned Two-Level Framework," *Sci. Rep.*, vol. 15, 2025, doi: 10.1038/s41598-025-88135-9.
[130] Y. Hosain and M. Çakmak, "XAI-XGBoost: An Innovative Explainable Intrusion Detection Approach for Securing Internet of Medical Things Systems," *Sci. Rep.*, vol. 15, 2025, doi: 10.1038/s41598-025-07790-0.
[131] K. Svandova and Z. Smutný, "Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review," *J. Multidiscip. Healthc.*, vol. 17, pp. 2281–2301, 2024, doi: 10.2147/JMDH.S459987.
[132] D. Soler, I. Cillero, C. Dafonte, M. Fernández-Veiga, A. Vilas, and F. Nóvoa, "QKDNetSim+: Improvement of the Quantum Network Simulator for NS-3," *SoftwareX*, vol. 26, Art. no. 101685, 2024, doi: 10.1016/j.softx.2024.101685.
[133] J. Meka, A. Jain, and N. Kumar, "A Holistic Approach to DDoS Mitigation: Leveraging NS-3 Simulation and Traceback for Enhanced Network Resilience," in *Proc. Int. Conf. Innov. Comput. Eng. (ICE)*, Greater Noida, India, Feb.–Mar. 2025, pp. 1–6, doi: 10.1109/ICE63309.2025.10983918.
[134] J. Abdullah, "Simulation of Wireless Sensor Networks (WSN) Using NS-3 and OMNeT++," *Int. J. Electron. Devices Netw.*, vol. 6, no. 1, pp. 24–30, 2025, doi: 10.22271/27084477.2025.v6.i1a.73.
[135] M. Shaik and S. W. Kim, "Security in Wireless Sensor Networks Using OMNeT++: Literature Review," *Sensors*, vol. 25, no. 10, Art. no. 2972, 2025, doi: 10.3390/s25102972.
[136] S. P. C. Sergio, G. P. Fernando, and O. A. D. Torres, "Security in IoT Networks: Simulation, Capture, and Traffic Analysis Using Contiki Cooja Software and RPL Protocols for Anomaly Detection," in *Proc. IEEE VII Congr. Int. Intell. Ambient., Softw. Eng. Health Electron. Mobile (AmITIC)*, David, Panama, Sep. 2024, pp. 1–7, doi: 10.1109/AmITIC62658.2024.10747625.
[137] K. Chee, M. Ge, G. Bai, and D. Kim, "IoTSecSim: A Framework for Modelling and Simulation of Security in Internet of Things," *Comput. Secur.*, vol. 136, Art. no. 103534, 2023, doi: 10.1016/j.cose.2023.103534.
[138] A. C. Frâncu, G. Predusca, L. D. Circiumarescu, N. Angelescu, and D. C. Puchianu, "Evaluation of IoT Network Security Against Botnet Attacks Through Simulation in NetSim," in *Proc. 17th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, Targoviste, Romania, Jun. 2025, pp. 1–6, doi: 10.1109/ECAI65401.2025.11095494.
[139] M. Aslam, W. Li, W. Liu, Y. Qi, U. Saleem, and S. Riaz, "Integrated Modeling and Simulation of Control and Communication System in Smart Grid Using CSMO (Co-Simulation of MATLAB and OMNeT++)," *Comput. Electr. Eng.*, vol. 122, Art. no. 109989, 2025, doi: 10.1016/j.compeleceng.2024.109989.
[140] M. Tosun, U. C. Cabuk, O. Dagdeviren, and Y. Ozturk, "DAWN-Sim: A Distributed Algorithm Simulator for Wireless Ad-Hoc Networks in Python," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Honolulu, HI, USA, Feb. 2023, pp. 635–639, doi: 10.1109/ICNC57223.2023.10074218.
[141] T. Saiki, S. Imanaka, S. Kobayashi, and T. Nakano, "A General-Purpose Simulation Platform for Multicellular Molecular Communication Systems," *IEEE Trans. Mol. Biol. Multi-Scale Commun.*, vol. 11, pp. 152–165, 2025, doi: 10.1109/TMBMC.2025.3544141.
[142] A. Vaziri, P. Moghaddam, M. Shoeibi, and M. Kaveh, "Energy-Efficient Secure Cell-Free Massive MIMO for Internet of Things: A Hybrid CNN-LSTM-Based Deep-Learning Approach," *Future Internet*, vol. 17, Art. no. 169, 2025, doi: 10.3390/FI17040169.
[143] G. Murugan and M. Chinnadurai, "ESHA-256_GBGO: A High-Performance and Optimized Security Framework for Internet of Medical Thing," *Sci. Rep.*, vol. 15, 2025, doi: 10.1038/s41598-025-94345-y.

[144] K. Kalita, J. Ramesh, L. Čepová, S. Pandya, P. Jangir, and L. Abualigah, "Multi-Objective Exponential Distribution Optimizer (MOEDO): A Novel Math-Inspired Multi-Objective Algorithm for Global Optimization and Real-World Engineering Design Problems," *Sci. Rep.*, vol. 14, 2024, doi: 10.1038/s41598-024-52083-7.

[145] N. Khodadadi *et al*., "Multi-Objective Generalized Normal Distribution Optimization: A Novel Algorithm for Multi-Objective Problems," *Cluster Comput.*, vol. 27, pp. 10589–10631, 2024, doi: 10.1007/s10586-024-04467-7.

[146] B. M. Radhi, A. F. Ataalla, H. M. Alsayednoor, M. A. Al-Shareeda, M. A. Almaayah, and M. Obeidat, "A Lightweight Identity Authentication Protocol for Nano-Scale IoT Devices," *Eng. Technol. Appl. Sci. Res.*, vol. 15, no. 5, pp. 27938–27946, 2025, doi: 10.48084/ETASR.13449.

[147] A. U. Rehman *et al*., "Internet of Things in Healthcare Research: Trends, Innovations, Security Considerations, Challenges and Future Strategy," *Int. J. Intell. Syst.*, vol. 2025, no. 1, pp. 1–53, 2025, doi: 10.1155/int/8546245.

[148] A. K. Jonnalagadda and C. Bura, "Immune-Inspired AI: Adaptive Defense Models for Intelligent Edge Environments," *ICCK Trans. Emerg. Top. Artif. Intell.*, vol. 2, no. 3, pp. 1–18, 2025, doi: 10.62762/TETAI.2025.270695.

[149] Y. Li, H. Wang, and G. Xu, "Federated Reinforcement Learning-Driven Multi-Task Optimization for Robust and Ethical Edge Internet of Things Security," *Sci. Rep.*, vol. 16, no. 1, Art. no. 5278, 2026, doi: 10.1038/s41598-025-34879-3.

[150] P. Nimse, P. Ubale, and P. Gore, "Challenges of Nanotechnology, Nanoscience, Nanobiosensors, and Internet of Nano Things With Its Applications," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 3, pp. 290–295, 2024, doi: 10.48175/IJARSCT-22843.

[151] R. Mustafa, N. I. Sarkar, M. Mohaghegh, and S. Pervez, "A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey," *Sensors*, vol. 24, no. 22, Art. no. 7209, 2024, doi: 10.3390/s24227209.

[152] A. Uprety, D. Rawat, and B. Sadler, "Human Immune System Inspired Security for Federated Learning-Empowered Internet of Things," *ACM Trans. Internet Things*, vol. 6, pp. 1–18, 2025, doi: 10.1145/3722562.

[153] S. Singh, G. Kumar, U. Ahirwar, S. Selvarajan, and F. Khan, "Multi-Objective Quantum Hybrid Evolutionary Algorithms for Enhancing Quality-of-Service in Internet of Things," *Sci. Rep.*, vol. 15, 2025, doi: 10.1038/s41598-025-99429-3.