ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/353037619

# A Systematic Review of Bio-Cyber Interface Technologies and Security Issues for Internet of Bio-Nano Things

**Article** *in* IEEE Access · June 2021

DOI: 10.1109/ACCESS.2021.3093442

CITATIONS
36

READS
4,111

**8 authors**, including:

Sidra Zafar
Lahore College for Women University
**6** PUBLICATIONS **89** CITATIONS
SEE PROFILE

Mohsin Nazir
Lahore College for Women University
**22** PUBLICATIONS **175** CITATIONS
SEE PROFILE

Taimur Bakhshi
CIMACS
**44** PUBLICATIONS **685** CITATIONS
SEE PROFILE

Hasan Ali Khattak
National University of Sciences and Technology
**127** PUBLICATIONS **2,812** CITATIONS
SEE PROFILE

All content following this page was uploaded by Muhammad Bilal on 08 July 2021.

The user has requested enhancement of the downloaded file.

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 26, 2021, accepted June 21, 2021, date of publication June 29, 2021, date of current version July 7, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3093442*

# A Systematic Review of Bio-Cyber Interface Technologies and Security Issues for Internet of Bio-Nano Things

**SIDRA ZAFAR[1], MOHSIN NAZIR[1], TAIMUR BAKHSHI[2], HASAN ALI KHATTAK[3], (Senior Member, IEEE), SARMADULLAH KHAN[4], MUHAMMAD BILAL[5], (Senior Member, IEEE), KIM-KWANG RAYMOND CHOO[6], (Senior Member, IEEE), KYUNG-SUP KWAK[7], (Life Senior Member, IEEE), AND ANEEQA SABAH[8]**

[1]Department of Computer Science, Lahore College for Women University, Lahore 54000, Pakistan
[2]Center for Information Management and Cyber Security, National University of Computer and Emerging Sciences, Lahore 54770, Pakistan
[3]School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan
[4]School of Computer Science and Informatics, De Montfort University, Leicaster LE1 9BH, U.K.
[5]Department of Computer Engineering, Hankuk University of Foreign Studies, Yongin, Gyeonggi 17035, South Korea
[6]Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249, USA
[7]Department of Information and Communication Engineering, Inha University, Incheon 22212, South Korea
[8]Department of Physics, Lahore College for Women University, Lahore 54000, Pakistan

Corresponding authors: Muhammad Bilal (mbilal@hufs.ac.kr) and Kyung-Sup Kwak (kskwak@inha.ac.kr)

This work was supported by the National Research Foundation of Korea Grant through the Korean Government (Ministry of Science and ICT) under Grant NRF-2020R1A2B5B02002478.

This work did not involve human subjects or animals in its research.

**ABSTRACT** Advances in synthetic biology and nanotechnology have contributed to the design of tools that can be used to control, reuse, modify, and re-engineer cells' structure, as well as enabling engineers to effectively use biological cells as programmable substrates to realize Bio-NanoThings (biological embedded computing devices). Bio-NanoThings are generally tiny, non-intrusive, and concealable devices that can be used for *in-vivo* applications such as intra-body sensing and actuation networks, where the use of artificial devices can be detrimental. Such (nano-scale) devices can be used in various healthcare settings such as continuous health monitoring, targeted drug delivery, and nano-surgeries. These services can also be grouped to form a collaborative network (i.e., nanonetwork), whose performance can potentially be improved when connected to higher bandwidth external networks such as the Internet, say via 5G. However, to realize the IoBNT paradigm, it is also important to seamlessly connect the biological environment with the technological landscape by having a dynamic interface design to convert biochemical signals from the human body into an equivalent electromagnetic signal (and vice versa). This, unfortunately, risks the exposure of internal biological mechanisms to cyber-based sensing and medical actuation, with potential security and privacy implications. This paper comprehensively reviews bio-cyber interface for IoBNT architecture, focusing on bio-cyber interfacing options for IoBNT like biologically inspired bio-electronic devices, RFID enabled implantable chips, and electronic tattoos. This study also identifies known and potential security and privacy vulnerabilities and mitigation strategies for consideration in future IoBNT designs and implementations.

**INDEX TERMS** Bio-cyber interface, Internet of bio-nano things, bio-electronic device security, bio-inspired security approaches.

## I. INTRODUCTION

With recent pandemics and the associated lockdown regime, there has been renewed, if not accelerated, interest, in exploring electronic and remote delivery of healthcare services. One of the recent trends is in the Internet of Bio-Nano Things (IoBNT) systems, which comprise biological nanonetworks that sense biological and chemical changes in the environment (i.e., human body) and send the collected data over the Internet to data centers for further processing.

The associate editor coordinating the review of this manuscript and approving it for publication was Rakesh Matam.


This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

These nanonetworks can also perform medical actuation from the commands sent remotely by the relevant healthcare providers. Typically, biological nanonetworks consist of nanosized computing devices (also referred to as 'Bio-Nano Things'), which work collaboratively to achieve sensing and actuation tasks within the deployed environment [1]–[8].

Supported tasks include targeted drug delivery (TDD), continuous health monitoring, tissue engineering, and tumor detection [9]–[16]. Conventional wireless communication technologies are generally not suitable to support communications within the nanonetworks due to limitations in transceiver size, computation capability, and propagation channel of the bio-nano things. This necessitates the design of novel communication technologies for these nanonetworks [17], [18], and examples include molecular communication (MC) [19], [20], nano electromagnetic (EM) communication at Tera Hz band, acoustic and nanomechanical communication [21], [22].

To ensure the smooth operation of IoBNT devices and systems, seamless connections of intra body nanonetworks and external networks (such as the Internet) are essential in supporting more complex, real-world healthcare applications. External access to intrabody nanonetworks requires a hybrid interface device that understands both paradigms' communication protocols, specifically biochemical signals generated by intrabody nanonetworks and electromagnetic signals received from the Internet. Bio-cyber interfacing can be summarily defined as a set of operations performed in sequence to convert biochemical signals received from intra-body nanonetworks into electrical signals for the cyber domain of Internet and *vice versa* [23]. In other words, the design and modeling of the bio-cyber interface are crucial yet challenging in IoBNT implementation.

Interdisciplinary research efforts devoted to the development of these bio-electronic devices have resulted in frameworks such as second skin [24], bio-cyber interface [25], and bio driver [26]. Bio-electronic interfaces may be composed of materials characterized by electromagnetic properties, which can alter their formation in the presence of biological molecular complexes and accordingly modulate current in the electrical circuit. Popular examples of bio-electronic interfacing include wireless chemical sensors, RFID devices, and electronic tattoos.

Wireless chemical sensors sense the changes in levels of chemical substrates of the object and send them wirelessly over the Internet to processing applications [35]–[37]. Similarly, inkjet printable electronics which use nanomaterials based ink, have been utilized to facilitate fabrication of RFID enabled implantable devices that sense bodily parameters and send them to some nearby devices (e.g., mobile devices) via radio-frequency identification (RFID) [38]. Moreover, electronic tattoo based stick-able sensors can be skin-mounted to collect epidermal and sweat gland information, which can be used to facilitate continuous patient monitoring [39].

One of the many challenges in designing bio-cyber interfaces is how to accurately model molecular information collected by intra-body sensors into an equivalent electromagnetic signal. Several factors are limiting the wider adoption of these devices, for example, data security and user safety. For example, the capability to access our human body through IoBNT applications can be exploited to carry out "bio-cyber terrorism" [25], where attackers can identify and exploit vulnerabilities in these IoBNT applications and/or their underpinning infrastructure to directly manipulate human body functionality, (covertly) exfiltrate user information, or cause the human body to malfunction. The feasibility of conventional, as well as novel security measures, needs to be established for these (resource-constrained) devices, and lack of trust in security and privacy will limit the adoption of such systems. This necessitates the design of security measures to minimize the impact of a cyber-attack and unlawful profiling and surveillance of individuals. This work is a step towards providing a roadmap showing what has been done in IoBNT security and what needs to be done.

### A. EXISTING LITERATURE REVIEWS AND SURVEYS

The idea of integrating biological cells into the communication engineering perspective was first proposed by Akyildiz *et al.* [25]. The authors described the architecture of IoBNT and its potential applications, such as collecting vital physiological parameters from the human body and transmitting them to the remote healthcare provider. They also described the enabling technologies to realize the IoBNT paradigm and focused on molecular communication as the most promising intrabody communication technology. Furthermore, the challenges in developing safe and efficient techniques for the exchange of information and the development interface between the biological and cyber world (i.e., bio-cyber interface). Challenges and opportunities were presented.

Another article [27] overviews Nano communications, BAN (Body Area Network) communications, and the potential mechanisms that can be used for the interfacing between nano-micro-macro communications. This survey article identifies specific materials and molecules such as Light stimulated channelrhodopsins, BRET(Bioluminescence Resonance Energy Transfer), ATP(Adenosine Triphosphate), Photodetectors, and SPR (Surface Plasmon Resonance), which can be used as part of bio cyber interface to achieve the overall interfacing between nano and micro networking domains. Unlike our work, this survey article does not provide any insights into the bio cyber interface's complete design and prospective components. Moreover, this article does not discuss the security perspective of the communication between nano-micro and macro devices.

A roadmap paper has been presented in [32], which surveys the key enabling technologies of next generation wireless communications. This paper provides a detailed insight into the vital technologies that will play an integral role in 6G

networks and beyond, provides use cases of applications that will be enabled by 6G and the open research challenges in this domain. Moreover, this paper also review the early stage technologies such as Internet of Nano Things (IoNT), Internet of Bio Nano Things (IoBNT), and quantum communication, which are expected to benefit from 6G and beyond communications. This paper presents an overall picture of the next generation wireless technologies, discussing every enabling technology in general, whereas our research specifically focuses on a detailed and comprehensive overview of one of the 6G enabling technologies i.e., IoBNT.

Other surveys from related fields include those focusing on Internet of Nano-Things (IoNT) [22]. The authors introduced the IoNT architecture, and explained the individual components and functionality from an information-theoretic perspective. Also, it presents research challenges in terms of channel modeling, information encoding and protocols for nanonetworks and IoNT were presented.

Another survey on IoNT in the context of body centric communication was presented in [30]. Specifically, the authors described the IoNT architecture and proposed a novel hybrid communication medium for body centric networks. The hybrid communication scheme proposed using both MC and EM communication in parallel, for nano micro interfacing, to achieve efficient results. The authors also briefly discussed existing security approaches for IoNT.

Qadri *et al.* [40] discussed the possible emerging technologies for healthcare IoT (H-IoT), the options for enabling H-IoT (e.g., IoNT was identified as one of the enablers for healthcare applications). Another review on healthcare applications of IoNT was presented by Pramanik *et al.* [41], who presented a taxonomy of nanotechonolgy, nanoparticles and nanozymes, types and fabrication options for biosensors, and bionanosensors for healthcare applications of IoNT.

In the field of electronic tattoos, a review paper [34] presents the materials and engineering requirements, fabrication developments, and sensing and therapeutic advancements of electronic tattoos. According to the authors, there are three components of a theragnostic-based electronic tattoo i.e., Sensing components for diagnostics, supporting electronics for data transmission, and drug delivery component.

Another survey paper [42] that presents state-of-the-art in security and safety issues of the Brain Computer Interaction. This work thoroughly identifies some novel cyberattacks, their impact on security and safety and their countermeasures. Some of the attacks like misleading stimuli are strictly related to BCI as it indicates alteration of the nuerosignals generated by the patient. Other attacks and counter measures are generic for the fields of IoT, IMD, and even IoBNT. This paper is provides exceptional insights into the security aspect. The main difference in our study and this survey paper is that the purpose of our study is to cover some very important architectural and design aspects of IoBNT, specifically bio cyber interfaces, along with security issues of IoBNT.

To the best of the authors' knowledge, there is no comprehensive review of IoBNT security solutions in the literature; nevertheless, the following research from similar fields such as IoMT and BCI (Brain Computer Interaction) provide some preliminary insights into the security challenges. Keeping in view the recent pandemic and COVID-19 situation a review paper [33] has been published recently, which discusses the technological challenges and solutions for wearable bio-electronics for patient monitoring and domiciliary hospitalization. In the end, they have presented a case study application of the Internet of Medical Things(IoMT) for domiciliary hospitalization of COVID 19 patients.

However, there have been no unified works that have presented a unified view of the protocol stack models [40]. A survey on WBAN (Wireless Body Area Networks) was presented in [28], which focuses only on the security aspects. The authors proposed a four-tier architecture for WBAN and identified communication technologies for each tier. The communication technologies and devices of WBAN are similar to that of IoBNT.

Molecular communication is the key and most promising enabling technology for the healthcare applications of IoBNT [43]. A comprehensive review paper is presented by authors in [29]. This paper presents a layered architecture of Molecular Communication and identifies the possible attack types and possible counter measures in each layer.

In [31], the authors studied the security of big 5G-oriented IoNT and the potential utility of machine learning to deal with the (big) data generated by the large number of IoNT devices. The authors outlined the potential security attackers and attack types. The comparison of the existing surveys and this study is presented in Table 1.

### B. PAPER SCOPE AND CONTRIBUTIONS

This paper provides a comprehensive review of published research on IoBNT and the security and privacy considerations that it raises. To do so, relevant keywords were used to search published papers in databases such as IEEExplore, Science Direct, ACM Digital Library, and Google Scholar. The main keywords or combination of keywords used were ''Internet of Bio Nano Things'', ''Bio cyber Interface'', ''Electronic Tattoos'', ''Wearable Internet of Things (IoT)'', ''Radio Frequency Identification (RFID)'', ''IoBNT Security, and privacy'', ''Cyberattacks in IoT'', and ''Nano networks security'', published within 2010-2020 timeline. This resulted in around 80 papers after filtering by categories, topic relevance, time of publication, and contributions.

The distribution of papers across journals shows that the papers were mainly published in journals that cover interdisciplinary topics such as electrochemistry, biotechnology, wireless communication, theragnostics, and optogenetics. While there have been a number of survey and review articles on closely related fields (i.e., IoNT,IoMT and WBAN) (see Section I-A), as well as those on the underlying communication engineering principles (e.g., channel modeling, modulation techniques, enabling and communication technologies, and other networking protocols which are applicable to IoBNT) [30], [31], [41], there has been no

**TABLE 1.** The comparison of existing literature and surveys on IoBNT.

| Ref | Networking Domain | Main Focus | Bio Cyber Interfacing | Security | Description |
|---|---|---|---|---|---|
| [27] | Nano Communication Networks, Body Area Networks | Interfacing options for nano-micro communication | ✓ | X | Identifies potential materials and molecules that can be used for interfacing between Nano and micro communication technologies. |
| [28] | Wireless Body Area Networks | Security | X | ✓ | Description of Four-tiered architecture of WBAN, presentation of security issues in each layer. |
| [29] | Molecular Communication(MC) | Security in MC | X | ✓ | Comprehensive discussion on security and privacy issues of Molecular Communication and their potential countermeasures. |
| [22] | IoNT | Roadmap paper | X | X | Early investigation of IoNT to explore enabling technologies, architecture, challanges and opportunities in IoNT |
| [30] | IoNT and body-centric networking | Survey paper | ✓ | * | Overview of IoNT technology, and introduction of hybrid communication scheme for nano micro interfacing. |
| [31] | 5G oriented IoNT | Artificial Intelligence and security in IoNT | X | ✓ | This article provides a critical overview of the IoNT considering the main application areas, architecture, limitations, and design factors. Comprehensive overview of employing Artificial Intelligence for IoNT. Moreover, a brief discussion of attack types and attackers on IoNT. |
| [32] | 6G and next generation wireless networks | Roadmap paper | * | X | Usecases,enabling technologies and key drivers for 6g and beyound technologies i.e., IoNT, IoBNT and quantum computing |
| [33] | IoMT | Review paper | * | X | The technological challenges & solutions for wearable bio-electronics for patient monitoring and domiciliary hospitalization |
| [34] | Electronic Tattoos | Review paper | * | X | The materials and engineering requirements, fabrication developments, and sensing and therapeutic advances in electronic tattoos |
| Our study | IoBNT | Review paper | ✓ | ✓ | Interdisciplinary research on bio cyber interfacing options for IoBNT. - Security for IoBNT |

-Legends ✓= Completely addressed X = Not addressed * = Partially addressed

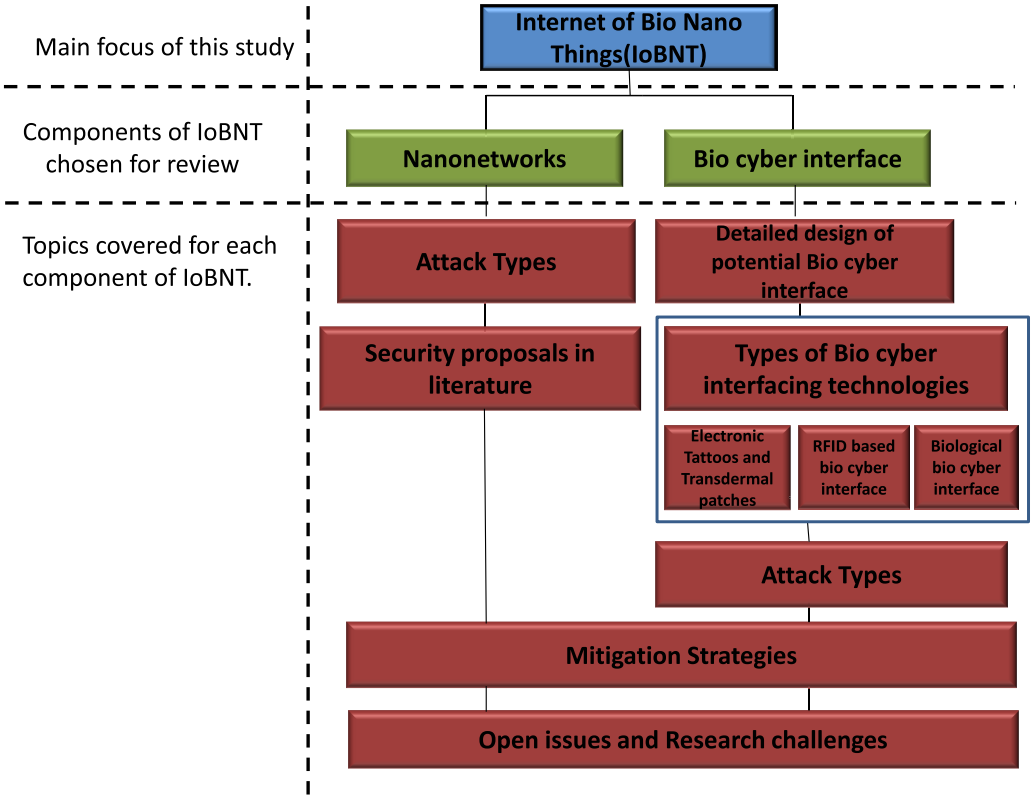



**FIGURE 1.** Overview of topics covered in this article.

survey or review article that focuses on IoBNT challenges and research opportunities.

This paper identifies and highlights the key design issues in the IoBNT implementations (e.g., interface design options between the biological and cyber world) and the related security challenges. A lot of prominent researches in the field of IoBNT and next generation technologies have emphasized on interdisciplinary research efforts to make these novel systems holistic and practical [25], [27], [32]. Therefore, this article's main contributions are to bring together insights from disciplines like physics, biology, optogenetics, and electrochemitry to explore more potential bio interfacing mechanisms that are being used in these fields and their applicability to IoBNT domain.

In summary this work aims to make following contributions:

- To provide a detailed design of the potential bio cyber interfacing device for IoBNT applications.
- To survey three different bio cyber interfacing technologies namely, biological bio cyber interface, electronic tattoos and RFID based bio cyber interface.
- To discuss various security issues and concerns that are specific to each bio cyber interfacing technology.
- To provide detailed discussion on security of IoBNT and individuating attacks and threats in IoBNT components i.e., nanonetworks and bio cyber interface.
- To provide novel and potential mitigation strategies for the security of IoBNT.
- To present open issues, challenges, and future research directions involving IoBNT and its security.

A detailed elaboration of the contributions and covered topics in this article is depicted in Figure 1.

### C. ARTICLE STRUCTURE

The rest of the paper is organized as follows. The architecture of IoBNT is described in the next section. The bio-cyber interface and the taxonomy of bio-cyber interface devices are introduced in Sections III and IV, respectively. The potential security threats and mitigation techniques connected with IoBNT are discussed in Sections V and VI, respectively. The last two sections address the problems and future research prospects, as well as the paper conclusion. Figure 2 depicts the overall taxonomy of this paper.

## II. INTERNET OF BIO NANO THINGS ARCHITECTURE

As previously discussed, the IoBNT network helps to sense biological and chemical changes around the environment and send the aggregated data to the data center for further processing [44]. To realize IoBNT, heterogeneous devices need to collaboratively work together at nano- to macro-scale, via some interfaces between the electrical domain of the Internet and the biochemical domain of the IoBNT networks [25]. For example, as shown in Fig. 3, the major components in a IoBNT communication network include bio-nano things, nanonetwork, bio-cyber interface, gateway devices, and some

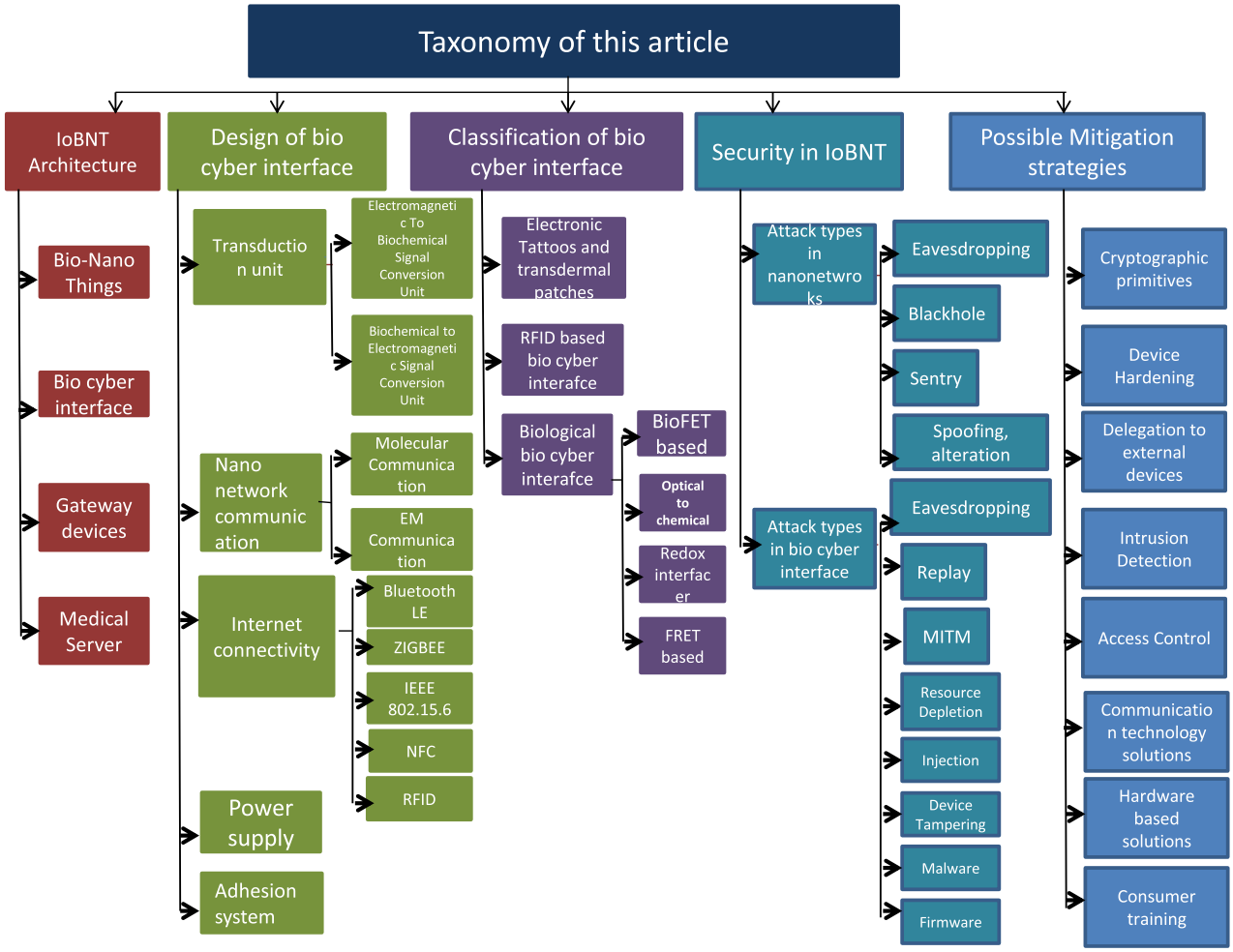



**FIGURE 2.** Taxonomy of Systematic Review of Bio-Cyber Interface Technologies and Security Issues in the Internet of Bio-Nano Things.

medical server(s). The components of IoBNT architecture are elaborated below:

### A. BIO-NANO THINGS

Bio-nano things are nanodevices that are not only a computing machine that can be reduced to a few nanometers in size, but also a device that uses the unique properties of nanocells and nanoparticles to detect and measure new types of phenomena at nanoscale. For example, nanodevices can detect chemical compounds in a fraction of a billion. Reference [45], [46], or the presence of different infectious agents such as virus or harmful bacteria [47], [48].

Nanodevice is essentially comprise of a number of hardware constituents and all the software and programming of the nanodevice is included in the information processing unit. There are two types of Nanodevices, electronic nanodevice, and biological nanodevice. Electronic nanodevices use novel nanotechnology materials like Carbon Nano Tubes (CNT) [49], [50] and Graphene Nano Ribbons [17] for device construction. Biological nanodevices are built using the tools from nanotechnology and synthetic biology.

Biological nanodevices can be fabricated by reprogramming biological materials [51], [52] like cells [53], viruses [54], [55], bacteria [56], bacteriophage [57], erythrocytes (i.e., a red blood cell), leukocytes (a type of white blood cell) and stem cells [58], [59] or by artificially synthesizing biomolecules like liposome, nanosphere, nanocapsule, micelle, dendrimer, fullerene and deoxyribonucleic (DNA) capsule. Moreover, hybrid nanodevices can be fabricated by applying both the above-mentioned approaches. The size of nano devices may range from macro molecule to typical biological cell.

The material used to compose nano devices can be only biological [60] (proteins, DNA sequences, lipids, biological cell) or they can be synthesized with non-biological materials such as magnetic particles and gold nanorods. There are a number of naturally occurring nano devices e-g protein motors that bind certain types of molecule on cargo transport them through filaments and unbind them at destination,

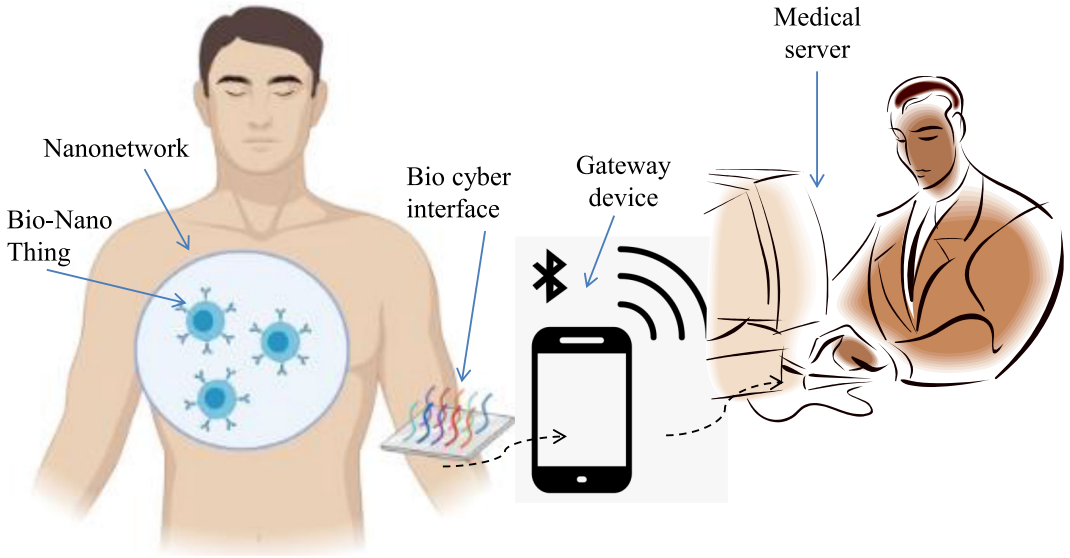



**FIGURE 3.** A Typical Internet of Bio-Nano Things Architecture, where a bio-chemical signal from inside the human body is converted into electromagnetic signal *via* bio cyber interface, and transmitted through Bluetooth or equivalent technology towards medical server for further analysis and processing.

liposomes capable of storing and releasing certain types of molecules, biological cells coated with non-biological material for non-cell native functions(e-g absorbing mercury). An envisioned bio-nano thing is presented in Figure 4.

### B. NANO NETWORK

Nano network is comprised of several nano-scale devices such as nano transmitter, nano receiver, nano router, and other specialized nanodevices to perform exclusive tasks like sensing, actuation, monitoring, and control. Intra-body nanonetwork is generally deployed in the environment (e.g., human body orally or through injection) to realize *invivo* biomedical applications. The nanonetwork consists of devices (e.g., nanomachine, nano router, and nano micro interface) at the nanoscale (1-100 nm), which work collaboratively to achieve sensing and actuation tasks [17]. Nanomachines can be interconnected to execute collaborative tasks in a distributed manner. The size of nanodevices makes them feasible for *in vivo* applications, where these non-invasive machines can easily be placed in hard-to-access areas (e.g., deep inside tissue) and perform therapeutic operations.

### C. BIO CYBER INTERFACE

Nano micro interface is mediating device between nano and micro scale communication; it is referred to as bio-cyber interface and bio electronics device throughout this article to keep the generality. Basically, this device converts electrical signals received as commands from the medical server of healthcare providers into biochemical signals understandable by intra-body nanonetworks and *vice versa* [61]. A detailed description of bio cyber interface design is presented in Section III.

### D. GATEWAY DEVICES

Gateway devices are now an integral part of most IoT applications, where they function as a relay device between sensors and the Internet. Gateway devices are computing devices such as smartphones, tablets, laptops, or mini-computers. A gateway device supports the mobility of patients and ensures efficient signal reception of low transmission range technologies (NFC, RFID, Bluetooth LE, etc). The wearable bio-electronic devices are usually designed to be compatible with the operating system requirements of smartphones [35], [62]. For RFID enabled applications, smartphones integrated with the RFID readout unit, which eliminates the need for external RFID tag readers. Similarly, for bio-electronic devices enabled with Bluetooth LE as the communication modality, smartphones are the ideal choice. Access point can be a cellular base station or a WiFi access point, which helps to route the body sensor's traffic to the medical server.

### E. MEDICAL SERVER

Medical server acts as a repository in which all the sensory data collected and sent from the patient's body is stored, analyzed and processed. This server may act as a terminal for real-time and continuous health monitoring, where emergency situations can be mitigated by sending alert messages. Only authorized entities can access this server to send commands and receive collected data, due to the critical nature of biomedical applications.

## III. A DETAILED DESIGN OF POTENTIAL BIO CYBER INTERFACE DEVICE

Bio-cyber interface is the hybrid and most sophisticated device, that is capable of communicating between nanoscale and microscale devices [22], [25], [44]. This device receives

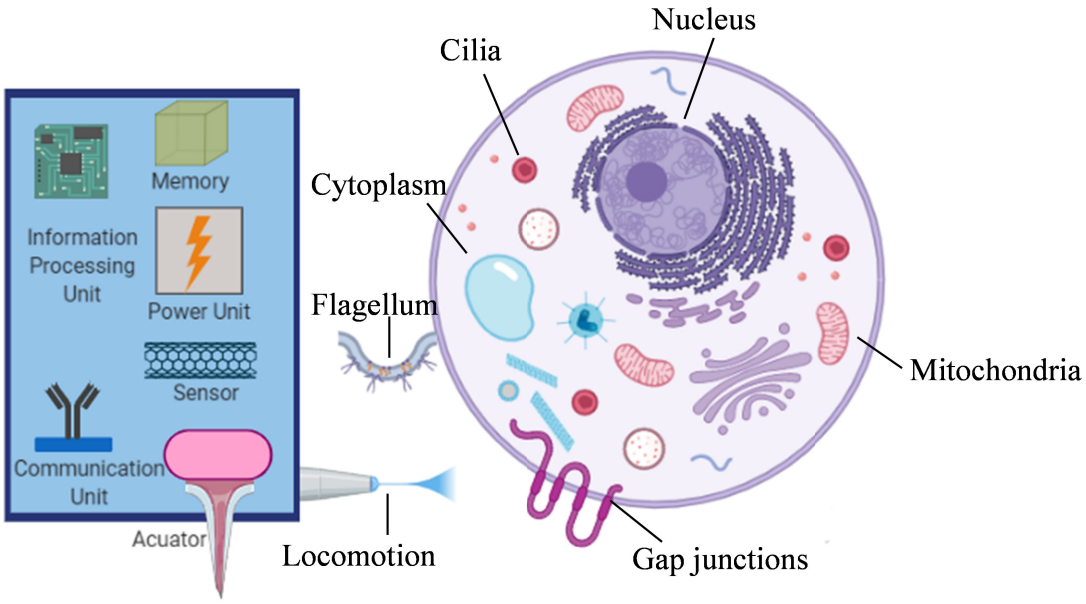



**FIGURE 4.** Bio-nano thing: A mapping between the components of a typical IoT embedded computing device, and the elements of a biological cell.

aggregated data from nanonetwork, processes nanoscale data in its transduction unit to convert it into a format suitable for the conventional network (e-g Internet) and sends it microscale devices. The components of envisioned bio-cyber interface are described in detail below:

### *A. TRANSDUCTION UNIT*

The transduction unit in the bio-cyber interface performs the operation of converting electrical signals from external devices into biochemical signals readable by Bio-Nano Things [63]. Transduction properties in bio-cyber interface can be achieved by engineering devices using biomaterials, artificially synthesized biomaterials, non-bio materials or by combining all the approaches to create hybrid design [64]. The transduction unit is further divided into two constituent parts, Electro-bio transduction unit, and Bioelectro transduction unit.

#### 1) ELECTROMAGNETIC TO BIOCHEMICAL SIGNAL CONVERSION UNIT

Electro – Bio Transduction Unit converts the electrical signals, received from external devices into biochemical signals, and transmits them to intra-body nanonetwork for further processing. This unit consists of a decoder, a drug storage unit, an external physical effect source, and an injection chamber. The decoder receives the signal transmitted from an external device and derives logic gates. The logic gates are binary commands that produce some physical effect in the environment like thermal, optical or magnetic radio-frequency (RF) signals. The physical effect source (thermal, optical or magnetic field) placed around the drug storage unit, stimulates the nanomachines to release their content in response to external changes in the environment. The injection chamber injects the released molecules into the blood vessel network.

The drug storage compartment of the bio-cyber interface contains nanomachines that are fabricated with materials sensitive to external physical effects like changes in light, temperature, pH or enzymes [65]. The injected nanomachines traverse the blood vessel network and are anchored at the targeted site due to high affinity. The nanomachines are equipped with ligands (i.e., signaling molecules in the MC channel) that bind to reciprocal receptors (i.e., receiving molecule) and are only expressed at the targeted site [63]. The process of electromagnetic to bio chemical signal conversion is depicted in Fig 5 [63]. Bio and non-bio materials can be used to engineer nanomachine, like liposomes that are drug nanocarriers fabricated with a coating that is sensitive to external environmental factors [64].

Photosensitive materials release encapsulated molecules when stimulated by light at certain wavelength emitted from an external laser source [66]. The process of photoisomerization destabilizes the bilayer membrane of liposome upon light illumination and allows the release of photoresponsive molecules. For example, caged compounds release molecules by bond breaking [67] and gold nanorods generate heat as a response to their conformational change [63], [68].

Temperature-sensitive materials release their contents upon a nonlinear sharp change in temperature of the environment such as temperature-sensitive liposomes [69], [70] and dendrimers [71]. Such a sharp change in temperature triggers the thermo-responsive liposomes to release encapsulated molecules in the environment. Thermoresponsive liposomes should ideally maintain their load at body temperature (37°C)

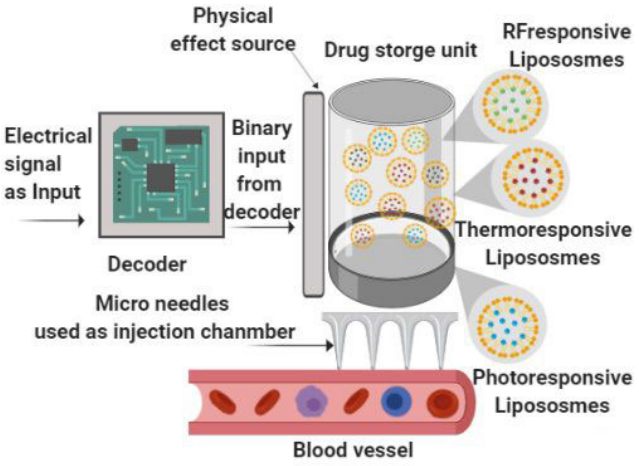



**FIGURE 5.** Schematic illustration of Electromagnetic to Biochemical signal conversation unit. The binary code is received from medical server, the decoder converts the binary signal and pass it to physical effect source which in turn activates the drug storage unit and release the drug.

and deliver the encapsulated drug only upon an increase intra-body temperature [63].

Magnetic particles release their contents in response to magnetic radio-frequency signals generated by an external source. For example, gold nanocrystals attached to DNA molecules induce the hybridization of the DNA molecules [72], generating double-stranded or signal stranded DNA molecules. An architecture for bio-cyber interface has been proposed in [63] which uses two kinds of liposomes that react to variations in light and temperature. According to the proposal when the decoded binary command from the external device is 011, thermal responsive liposomes release their contents. When the decoded command is 111 photosensitive liposomes release their contents. Another proposal [64] has performed a wet laboratory experiment to engineer artificially synthesized materials (ART) using polystyrene bead, to operate as in-messaging nanomachine to forward messages to intra-bodynanonetwork The functionality in the ART based nano device is not yet implemented and is reserved for future research work.

An information-theoretic model for glucose monitoring as an application of IoBNT has been proposed in [73]. The model utilizes pancreatic beta-cell to transmit insulin molecules into the intra-body network via blood vessel channel according to commands received from the healthcare provider. The feedback of glucose level is transmitted by muscle cells towards the beta cell to be transmitted towards the healthcare provider. The model is currently designed for intra-body nanonetworks in this proposal and can be made online for continuous health monitoring by using cyber-interfaced beta cells.

#### 2) BIOCHEMICAL TO ELECTROMAGNETIC SIGNAL CONVERSION UNIT

The bio electro transduction unit detects the concentration of received molecules and converts the molecular signals into electrical form. According to [63], this unit employs a cell structure to be used as a bioluminescence bioreporter. The bioreporter works on the principle bioluminescence reaction that produces a reporter protein upon excitation from an analyte.

The analyte here can be transmitted information molecules, moving towards the receiving nanomachines and the reporter protein is Luciferase (LU). Bioluminescence is the production and emission of light by living organisms as a result of a chemical reaction during which chemical energy is converted into light energy. When the two chemical enzymes Luciferin (L) and Luciferase (LU), catalyze oxygen in the presence of ATP, a chemical reaction releases energy in the form of light. Fluorescence molecules such as rhodamine derivatives are another form of luminescent materials that can be used to produce light energy [64].

These materials emit fluorescence upon excitation from microbiological conditions, which can be detected by external devices with the help of fluorescence microscopy. The emitted light energy is detected by a nanoscale light-sensitive sensor, which produces an equivalent electric signal in response. The electrical signal drives the transmitter to send the derived information through the wireless channel. Research contributions towards the realization of bio-cyber interface have resulted in some excellent theoretical frameworks for the Bio electrotransduction unit. The transduction unit for bio-cyber interface can be designed using natural/synthesized biological materials or novel nanotechnology materials like carbon and graphene.

### B. COMMUNICATION UNIT

The connection of the human body with the Internet is the basic notion behind the IoBNT paradigm. bio-cyber interface can be used as a module for connecting the human body to the Internet. bio-cyber interface must possess the capability to wirelessly transmit the aggregated intra-body data to the healthcare provider. Bio cyber interface is responsible for communication with the intra body nano networks as well as with the internet. Therefore, it must contain two communication units i.e., one for intra body communication and one for external communication with the internet.

#### 1) NANO NETWORK COMMUNICATION

As discussed earlier the intrabody nano network communication cannot be realized through the traditional wireless communication technologies due to the minute size of nano transceivers inside the human body. Therefore, novel enabling technologies have been investigated that are feasible for communication inside the human body and provides an interface to access the human body. These technologies include molecular communication [43] and nano-electromagnetic communication at the THz band. Both of these technologies are discussed in detail below:

#### a: MOLECULAR COMMUNICATION (MC)

Molecular communication performs the exchange of messages between bio-nano machines through information encoded molecules [20], [74]. To generalize MC into a communication engineering perspective, researchers have defined an architecture of MC that consists of key communication concepts and processes [74]. The basic components of MC architecture include the sender bio nanomachine, receiver bio nanomachine, and the propagation medium. The sender bio nanomachine encodes the information molecules, usually in the form of molecular concentration (i.e., the number of information molecules per unit volume of solvent molecules) modulated over time or some other form according to application. The encoded information is then released into the environment through unbinding from the sender bio nanomachine.

The propagation medium for *in-vivo* applications is an aqueous medium that allows the flow of molecules towards the destination. The process of molecule propagation can be active or passive. In active or walkway based propagation, molecules are encapsulated in vesicles and are transported through molecular motors towards the destination. Whereas in passive or diffusion-based propagation [75], information molecules diffuse away into the environment and are transported towards the destination through guide molecules. The receiver bio nanomachine captures the information molecules form the propagation medium and decodes them into some chemical reaction. Chemical reactions may include the production of some signal for other molecules, performing some simple task or producing other molecules.

In [20] state-of-the-art in MC have been presented, discussing architecture, theoretical and physical modeling and challenges and opportunities in the development of MC based systems. Some researchers have also related MC with traditional networking protocols such as [19] proposed a TCP like molecular communication which is a connection oriented protocol. Moreover, another proposal [74] presents an OSI like layered architecture for MC. The functionality of each layer and relevant research challenges and opportunities according to each have been discussed in detail.

In [76], a comprehensive survey on recent advancements on MC according to communication, perspective has been presented, which provides a detail discussion on the transmitter, receiver and propagation medium of MC systems. Some other works on the development of MC systems include the transmitter and receiver design [77]–[79] modulation techniques [80]–[83], channel modeling and noise analysis [84]–[88]. The most prominent application area of MC is healthcare and nanomedicine. In this direction, a comprehensive survey paper [89]on the medical applications of MC has been proposed that discusses a taxonomy of potential medical applications of MC, challenges, and opportunities in realizing them and future directions. Among the medical applications of MC, Targeted Drug Delivery (TDD) has got the most attention from the research community. A very comprehensive survey paper on the MC based TDD that discusses system models and design requirements/challenges for MC based TDD systems have been conducted by authors in [90].

Other work on MC based TDD can be found in [91]–[96]. MC is the most promising IoBNT technology due to its bio-inspired nature [25] and suitability for bio medical applications. Therefore most of the work in nanocommunication and IoBNT domain is dominanted by MC.

#### b: NANO ELECTROMAGNETIC (EM) COMMUNICATION

Nano EM communication at THz band is another communication option for intrabody communication, whose feasibility was first discussed in [17]. In this technology, EM waves are used as an information carrier between source and destination. The advancement in novel nanomaterials such as Carbon nanotubes (CNT) and graphene derivatives such as graphene nanoribbons (GNR) has opened up doors for EM communication at the nanoscale [21]. The THz spectrum is less vulnerable to propagation effects such as scattering, which makes it ideal for intrabody communication due to its safety for biological tissue i.e., non ionization [97].

The state-of-the-art in EM nano communication was proposed by Akyildiz and Jornet [21], which discusses the components, architecture and manufacturing possibilities of nanosensors for nano EM communication. Moreover, this paper also discusses the potential application areas of nano EM networks and challenges in realizing them. A new channel modeling scheme for nano EM networks based on radiative transfer theory is proposed in [98]. This paper also investigated the channel capacity of THz band based EM communication using different power allocation schemes. A state-of-the-art review paper that discusses possible biomedical applications of THz EM communication, current models and possible antenna designs, is proposed by Abbasi *et al.* [99].

### 2) COMMUNICATION WITH THE INTERNET

For better signal reception and to increase the mobility of patients with bio-cyber implants, smartphone devices are used as gateway devices to the internet [63]. Smartphone devices have now become an integral part of many IoT applications due to its ubiquity, advanced computational capabilities and opensource [100]. Wireless Body Area Networks (WBANs), Wireless Chemical Sensors (WCS) and other body area sensors are now being developed to be compatible with the operating system of the smartphone.

This section includes wireless technologies that are feasible for the connection between bio-cyber interface and smartphone device. Wireless Body Area Networks (WBANs) is a similar field of IoBNT which utilize implanted sensor devices to wirelessly transmit, measured human body parameters to healthcare applications via the Internet [101]. Research in WBANs is relatively mature as compared to IoBNT, therefore, a literature survey from WBANs has been included in this section. Moreover, researchers in the field of chemical engineering have been working on wireless chemical sensors (WCS) for more than a decade now [26].

**TABLE 2.** Communication mechanisms for the internet connectivity of bio-electronic devices.

| Technology | Data Rate | Transmission Range | RF Band | Exemplary References |
|---|---|---|---|---|
| Bluetooth LE | 1 Mbps | 10 m | 2.4 GHz ISM | [102], [103] |
| ZigBee | 250 Kbps | 10-100 m | 2.4 GHz | ] [101], [104] |
| IEEE 802.15.6 | 10 Kbps-10 Mbps | 3 m | 16-27 MHz | [105]–[109] |
| RFID | 10-100 Kbps | 1-100 m | 860-960 MHz | [101], [104], [111] |
| NFC | $< 424Kbps$ | $<$ 20 cm | 13.56 MHZ | [101], [104], [110] |

WCSs are wearable patches that are capable of transmitting sensed bodily chemical values to the connected smartphone for analysis and processing by healthcare applications. The wireless communication technologies that are suitable with bio-cyber interface design are identified through a literature review of relevant domains such as WBANs and WCSs. This work also go through some of the important factors to consider when designing a bio-cyber interface, such as size, power supply requirements, data rate, real-time vs. on-demand data transfer, transmission range, and warning capability. Selection of suitable wireless technology depends upon the bio-cyber interface application system requirements and the underlying mode of operation of the wireless technology.

There are a number of active and passive wireless technologies available today to establish human-Internet connectivity. Active wireless technologies contain transponders able to transmit and receive radio frequency waves at high data rates and long-distance. Active wireless technologies require a continuous battery supply for transmission and to power the circuitry. Examples of active wireless technologies include Zigbee and Bluetooth, and IEEE 802.15.6. While passive wireless technologies include RFID and Near Field Communication (NFC). These technologies are briefly explained below and are illustrated in Table 2.

#### *a: BLUETOOTH LOW ENERGY (LE) COMMUNICATION*

Bluetooth (LE) Low Energy technology was introduced to wirelessly connect small low power devices to mobile terminals. This technology is ideal to be integrated with implants for healthcare applications as it supports ultra-low power consumption [102]. It contains tiny Bluetooth radio to actively send and receive messages from nearby smartphone devices. The transmission range of Bluetooth LE is up to 10 m, the data rate is 1 Mbps and the frequency band is 2.4 GHz ISM [103]. Pairing time with other devices is in milliseconds, which is appropriate for alarm and emergency conditions in healthcare applications [104].

#### *b: ZIGBEE*

ZigBee has an active transmitter able to communicate with mobile devices over a distance of 10-100 m. Zigbee is considered the most cost-effective technology due to its low power and low data rates. ZigBee can operate on three ISM bands with data rates from 20 Kbps to 250 Kbps [104]. Although ZigBee provides a large transmission range, it is not a good candidate for continuous health monitoring applications due to its low data rates [101].

#### *c: IEEE 802.15.6 STANDARD*

The rapid popularity of Wireless Body Area Networks (WBANs) and Consumer Electronics called for a standard communication medium to address the special needs of the WBANs such as low power, low cost, low complexity, high throughput and short-range wireless communication in and around the human body. IEEE standards association established the IEEE 802.15 Task Group 6 for the standardization of WBAN [105], [106]. It quotes: "The IEEE 802.15 Task Group 6 (BAN) is developing a communication standard optimized for low power devices and operation on, in or around the human body (but not limited to humans) to serve a variety of applications including medical, consumer electronics personal entertainment and other"[IEEE 802.15 WPAN Task Group 6 Body Area Networks. 2011]. IEEE.802.15.6 has different frequency bands in different countries ranging from 16- 27 MHz [107].

Medical Implant Communications Service (MICS) band is a licensed band used for implant communication and has the same frequency range (402-405 MHz) in most of the countries [105]. MICS band is suitable to be integrated for bio-cyber interface as it defines protocols that are compatible with system requirements of bio-cyber interface. IEEE.802.15.6 can operate within a transmission range of 3 m with data rates up to 10 Mbps [108].

IEEE.802.15.6 has also been recognized to be used as a standard for Human Body Communication (HBC). HBC uses the human body as signal propagation medium, therefore certain concerns must be taken into account such as increased mobility of the patient, lower power consumption, small battery size yet life to span around a time several months, and management to aggregate burst data in presence of continuous triggers from physiological data. Considering these HBC concerns [109] proposed a medium access method for statistical frame-based time division multiple access (S-TDMA) protocol that demonstrates lower data latency, lower power consumption, and higher transmission efficiency.

#### d: NEAR FIELD TECHNOLOGY (NFC)

NFC is a passive communication designed to operate in the ultra-low transmission range of up to 20 cm. NFC technology contains NFC tag similar to the RFID tag, which is powered by a readout device. Communication in NFC requires devices to touch each other or be in close vicinity to each other. Smartphone transmits power wirelessly to resonant circuits through inductive coupling which turns ''ON'' the NFC tag. Once the transmission session is complete, the tag is marked as ''OFF'' and becomes unreadable [110].

This technology is ideal for implantable devices with a low power source as the communication is powered by the reader device (in our case smartphone). Ultra-Low transmission range in NFC is not a drawback, rather it is a strength as it provides rapid connection [101].

#### e: RFID (ISO/IEC 18000-6)

RFID is a passive wireless technology that consists of a transponder (tag) to be read by an RFID reader. RFID based implants are feasible in situations where battery supply is a major issue [101]. Entire transmission in passive RFID systems is powered by the reader side [111], which in our case can be RFID reader enabled smartphone devices. The read range of RFID is 1- 100 m with the data rate of 10- 100Kbps [104]. Battery-powered RFIDs with active radio transmitters are available which comes with a high cost yet low data rates.

### C. POWER SUPPLY

Bio cyber interfaces need a continuous power supply for data collection, processing, and transmission. The battery is mass vise the largest unit in the bio-cyber interface and other body implants. Although considerable progress has been done in lithium rechargeable batteries, yet they cannot keep pace with the novel technology requirements and size constraints. Miniaturization of a battery source, energy harvesting methods based on human body movements, and wireless battery recharge techniques have been explored by researchers of MIT for implants in Wireless Body Area Networks (WBANs).

Evanescent waves have been considered in [112] to wirelessly power the electronic devices over a short distance. Other efforts include solar rechargeable batteries [113], piezoelectric nanogenerators [114], micro-supercapacitors [115] and endocochlear potential-based bio batteries [116]. Implantable devices in IoBNT need a continuous power supply and prolong battery life, for this purpose mechanism has been investigated to scavenge power supply from the epidermal layer of the wearer [116]. These energy scavenging batteries are called biofuel cells (BFC), which convert chemical energy into electrical energy through biocatalytic reactions [117]–[119]. Researchers from the University of California San Diego have demonstrated an epidermal BFC [120] to scavenge continuous energy from human preparation. Lactate is used as biofuel as it is present in human sweat in an abundant amount [120]. Similarly, energy scavenging techniques from the human body can be adapted for power supply in the bio-cyber interface. A detailed energy model for nanoscale devices has been demonstrated in [121] which discusses the power consumption of each component in the nanonetwork.

### D. ADHESION SYSTEM

This section briefly discusses the patch material, as bio-cyber interface is envisioned to be a wearable/stick-able bio-electronic device. The adhesive material for the patch is under high interdisciplinary research investigation as human skin is extraordinarily stretchable ($\epsilon > 100\%$ *where* $\epsilon$ is the strain), highly rough (superlative height 40 $\mu$m), and generally covered with sweat and hairs [122]. Hence, delivering adequate adhesion of skin patches against human skin persists to be a challenging task. Adhesion materials should be carefully chosen to prevent issues like cytotoxicity (i.e., condition of being toxic), skin contamination, damages, risks of infection, and loss of wet adhesion make them less effective. Adhesion materials using electronic materials are extensively reviewed in [35] and bio-inspired approaches for adhesion like gecko-/beetle-inspired mushroom-shaped architectures, endoparasite-like microneedles, octopus inspired suction cups and slug-like adhesive with energy dissipation layer, has been keenly investigated in [122]. Special measures should be taken into account while selecting the adhesive material to prevent data loss and wireless connection due to strain and physical pressure on the patch while patient movement, wrinkling of skin or other factors.

### E. SUMMARY OF BIO CYBER INTERFACE

There exist a few proposals in the literature that present interface either using nano EM or MC communication. In the nano EM domain [123] have proposed an architecture of nanonetworks-based Coronary Heart Disease (CHD) monitoring system. The proposed model consists of nanomacro interface (NM) and nanodevice-embedded Drug Eluting Stents (DESs), termed as nanoDESs. The algorithm exploits the periodic change in mean distance between a nanoDES, inserted inside the affected coronary artery, and the NM, fitted in the intercostal space of the rib cage of a patient suffering from a CHD utilizing THz band. Another paper proposes a straight forward communication scheme utilizing the TeraHertz Band. The architecture consists of nano nodes and nano router, deployed in the dorsum of the human hand. Nano nodes circulate in the blood vessel for the collection of medical data and transmit the aggregated data to the nano router. Nanorouter then transmits the data to BAN (Body Area Network) device through THz band communication, which is then relayed to the Internet.

Some theoretical models have adopted MC paradigm for the design of bio-cyber interface device. For example, authors in [64] have conducted a wet-lab experiment by utilizing artificially synthesized materials as an interface between the biological and electrical world. The proposal employs optical

sensitive molecules(pH rodo molecules) that activate upon expression of fluorescence through fluorescent microscopy.

The above-mentioned proposals that utilize nano nodes and nanoDES in THz communication, may not be biocompatible due to the non-biological nature of these devices. Secondly, the use of external devices like a fluorescent microscope can also cause mobility issues for the patient, which negates the whole notion of IoBNT. A novel hybrid approach is presented [30], which suggests utilizing MC based communication inside the human body for its biocompatible and noninvasive properties. The MC can communicate with graphene-based nanosensor, implanted over the human body for communication with external devices. The nano micro interface will, therefore, consist of a THz based antenna and micro/macro antenna. The idea is to limit the non-bio devices inside the human body and to read the intra-body parameters efficiently outside the body.

## IV. CLASSIFICATION OF BIO CYBER INTERFACING TECHNOLOGIES AND THEIR SECURITY ISSUES

The design of a bio-cyber interface is a major challenge in the realization of IoBNT. In the introductory paper of IoBNT, Akyildiz et al highlighted the design challenges of bio-cyber interface and the possibility of using electronic tattoos, and RFID based sensors as bio-cyber interface. In order to study the possibilities of electronic tattoos and RFID-based tattoos as bio-cyber interfaces, previous proposals on electronic tattoos and RFID-based tattoos are evaluated below. Furthermore, some preliminary work on a biologically-inspired bio-cyber interface presented by the notable MC engineering research community is discussed.

### A. ELECTRONIC TATTOOS AND TRANSDERMAL PATCHES

Flexible and stretchable wearable electronics are getting interdisciplinary research attention as they promise to deliver continuous patient monitoring [23], [124] while circumventing the possible discomfort caused by regular wearable electronics. There are a number of biomedical conditions that require frequent monitoring of patients at regular intervals, for example, glucose monitoring for diabetic patients, fitness monitoring of athletes, real-time detection of pathogens in biofluids for the plausible onset of disease [125]. Traditional methods to measure these chemical analytes require extracting fresh blood or other bodily samples every time. This continuous and invasive blood sampling can cause discomfort to the patient's especially elderly patients and homophobic patients.

To address some of these concerns, researchers have ventured into the development of wearable sensors which provide non-invasive ways to continuously sense the patient's vital signs and transmit the collected data to data centers for further processing. Researchers have devised non-invasive ways of drawing out samples by utilizing the epidermal layer of the human skin [126].

Human skin contains several electrolytes that provide clinically useful information about patients' overall health such as temperature, physiological, electro-physiological and biochemical parameters [127]. Human perspiration is also an information-rich epidermal secretion that is readily available and can be used to extract information about chemical compositions like metallic ions, minerals, glucose, lactose, lactic acid, urea, volatile organic compounds, in the human body [128]. Variously, human epidermis experiences continuous bending, stretching, and deformation while performing daily life physical activities.

The mechanical properties of wearable electronics might mismatch with unique mechanophysiology of the human skin and can cause degradation of device capability and discomfort to the wearer. Novel fabrication techniques for developing flexible and comfortable wearable devices are trending in academic and industrial research [35], [122], [129].

To overcome the aforementioned issue, wearable electronics are now being fabricated by adapting the design principles of temporary tattoos. Temporary tattoos are a form of body art that firmly attaches to the skin as ''secondary skin'', while their presence is barely noticed by the wearer. Tattoos are comfortable to be worn and provide ease of performing daily life activities to the wearer, by bearing mechanical stress, washing, and other harsh conditions. These favorable properties of tattoos have attracted researchers of wearable electronics to develop tattoo based electronics. The electronic tattoos typically include sensors, memory, electronic circuits, and drug reservoir units [130]. The electronic tattoos analyze the sensed information to determine the dose and release timing of the drug contained in the unit.

Screen printing techniques can be used to print electronic tattoos of desirable shape capable of extracting rich chemical information from our epidermis and transmit these analytical data wirelessly to a smartphone. Moreover, dry free form cut and paste technology [131], [132] is also been introduced for electronic tattoo fabrication. A summarization of existing proposals for electronic tattoos in healthcare monitoring is presented in Table 3.

Traditional methods of drug delivery through oral intake of medicine and via injections are now quickly being replaced by transdermal drug delivery patches. These patches are good alternatives to traditional methods as they promise minimally invasive and painless drug delivery. The transdermal patch is usually made of flexible and stretchable material that contains microneedles on the sticking side of the patch. Microneedles are actually drug containers that release their payload upon external stimulation. Fourth-generation transdermal drug delivery systems [133] are now capable to release controlled amounts of the drug upon receiving commands wirelessly through the internet. A number of wearable electronic patches based therapeutic stimulators and drug delivery patches are available now that have proven to provide accurate results when compared with regular laboratory equipment.

**TABLE 3.** Summarization of electronic tattos and patches.

| Ref | Device Type | Functionality | Communication Unit | Description |
|---|---|---|---|---|
| [136] | Electronic Tattoo | Glucose Sensing, Alcohol Sensing | 2.4 GHz BLE | An epidermal biosensing system for continuous sampling and analysis of two biofluids i.e., glucose and alcohol. The electronic tattoo is screen printed which facilitates sweat stimulations at anode and ISF at the cathode. |
| [125] | Electronic Tattoo | Sodium Sensing | Bluetooth Radio | An electronic tattoo with wireless transmitting capabilities to measure and transmit sodium levels from perspiration of athletes during training. |
| [137] | Electronic Tattoo | Alcohol Sensing | Bluetooth radio | An iontophoretic-biosensing system has been integrated in electronic tattoo to monitor alcohol consumptions in patients. An alcohol-oxidase enzyme and the Prussian Blue electrode transducer is used for the detection of ethanol in the induced sweat. |
| [131] | Electronic Tattoo | Temperature and light-sensing | NFC | The tattoo can sense the temperature and light variations in the human skin and send it wirelessly to NFC enabled through NFC technology smartphone |
| [138] | Drug delivery implant | Remote control drug delivery of enalapril and methotrexate | Bluetooth | The implant is capable to deliver two kinds of drugs namely enalapril and methotrexate for hypertension and arthritis patients respectively. The diffusion of drugs across the Nanofluidic membrane is accomplished through a low-intensity electric field. |

#### 1) SECURITY CONCERNS IN ELECTRONIC TATTOOS AND TRANS DERMAL PATCHES

Electronic tattoos and transdermal patches can be exposed to security threats as they are continuously connected with the wireless technology. The following are some of the threats that electronic tattoos and transdermal patches may encounter.

##### *a: WIRELESS COMMUNICATION RISKS*

Electronic tattoos and transdermal patches need continuous wireless network supply in order to receive and send information to the healthcare provider. Mainly the electronic tattoos are connected with a gateway device (smart phone) that relays the information over the internet. In the currently published literature for electronic tattoos, it is noticed that most of the proposals have used Bluetooth or BLE as communication mechanisms between electronic tattoo and gateway device. Bluetooth technology works within close proximity and is considered safe as attacker must be present within the patient's vicinity to launch an attack. However, Bluetooth version 5.0 has a transmission range of upto 400m moreover, the range can be magnified up to a mile through omni directional antennas. Researchers from Singapore University of Technology and design have discovered 12 different Bluetooth bugs which can affect 450 type of IoT devices including implantable medical devices. Moreover, the security flaw named ''SweynTooth'' associated with BLE can crash the device, deadlock the device or bypass security to access device functionality. Another critical threat to Bluetooth technology is Blueborne attack. In this attack, hackers infect the devices with malwares and gains access to the device to execute malicious operations [134].

##### *b: PHYSICAL HARM*

The electronic tattoos currently manufactured are tested rigorously to withstand mechanical deformation caused

by external strain. However, in cases of long term use and extreme physical stress conditions, the device abilities might be degraded and cause unwanted behaviour. The bio-electronic devices which are presently designed in the form of electronic tattoo and implantable patches that do not require any surgical procedures to affix on the human body. Non-medical professionals can apply these devices easily on human skin like stickers. This nonsurgical relaxation can be exploited by local attackers to replace the bio-electronic device with an illegitimate device on an unconscious patient. The illegitimate device now becomes part of the communication and can launch several passive and active attacks like eavesdropping, replay attack, and data modification, etc.

*Countermeasures*: Some of the possible countermeasures for above mentioned attacks are Tamper-proofing and self destruction: Use of tamper proof package for sensing devices and enable self destruction mode upon countering an intruder attack. Minimize information leakage: Protective measures like generating artificial noise, shielding and adding randomized delay can be taken to minimize information leakage. [135] Run-time attestation: Generation of proof about updation of firmware by a remote entity. [135].

### B. RFID TAG SENSORS AS BIO-ELECTRONIC DEVICE

RFID tags are utilized for the identification of objects in many IoT and Cyber-Physical Systems (CPS) due to their wireless communication capability and easy integration in the Internet cloud system [139]. RFID tag sensors have already been extensively studied for industrial applications like food safety, logistics, healthcare, public transport, fake medicine and environmental pollution [38].

The role of RFID sensors in envisioned healthcare applications IoBNT is promising due to their easy integration with implanted interfaces for communication with the Internet. RFID enabled technology is being used for several healthcare applications like real-time tracking of patients, improving their safety, and in management and medical supplies in hospitals [140]–[147]. RFID is a wireless technology that utilizes RF signals to identify objects with RFID tags. RFID system has two components: a tag which is a microchip to store electronic information and radio antenna to receive signals. There are two types of RFID systems, passive that require no battery and are powered by the reader, and an active RFID system that has a battery to power the transmission on its own [38].

Passive RFID tags are ideal for IoBNT applications due to their properties of cost-effectiveness, long battery life, and low power consumption. RFID technology can be used as sensors [148], for sensing applications of IoBNT and can be used as a bio-electronic interface on its own. RFID antennas that are sensitive to environmental changes like gas [149], moisture [150] and temperature [151], have already been developed. The sensing capabilities of the RFID system can be exploited to measure the chemical and biological values of the human body. 13.56 MHz) or ultrahigh-frequency (UHF, 400 MHz) bands, has proven adequate in powering the adaptive threshold rectifier. The HF band is for patch sensors, whereas the UHF band supports' implantable sensors [30]. The sensor consumes 12 $\mu$W to implement an electrocardiogram analog front end, and an analog-to-digital converter (ADC). The envisioned Bio-electronic interface with RFID enabled technology is likely to have the following components to be operational in the IoBNT domain. RFID sensor tags that contain chemically coated thin- film resonant sensing antenna for sensing target chemical substances in the environment. Recent RFID tags are thin and flexible, allowing them to be embedded easily in the human body for health monitoring purposes [37].

RFID sensors can be integrated with sensing materials such as water-absorbing molecules to sense humidity and carbon nanostructures as gas sensors [152]. The chemical, physical, or electrical reaction of the sensing materials in the presence of the sensed parameters modify their electrical properties (permittivity, conductivity) resulting in easy-to-observe electrical metrics, such as a shift of the resonant frequency of the RFID tag antenna, verifying the simplicity and power efficiency of RFID-enabled sensors [153]. Moreover, RFID tag sensors contain IC microchips to store and process sensed data. Novel methods for the fabrication of electronic devices through inkjet printing are getting research attention in Consumer Electronics (CE). Nanomaterials like graphene, carbon nanotubes, silver, gold and copper nanoparticles, conductive polymer and their based materials are used as inkjet ink to print electronic devices.

A comprehensive review of inkjet-printed nanomaterial-based flexible radio frequency identification (RFID) tag sensors for the Internet of nano things has been presented in [38]. According to the review, inkjet printed nanomaterials are cheaper and flexible to be used as wearable electronics as long as they do not interfere with the biological signaling capability of the human body. In context of IoT applications, Kassal *et al.* [36] demonstrates a low-power RFID tag sensor for potentiometric sensitivity. The RFID tag has the ability to measure and store the potential of electrode, which is then wirelessly transferred to a smartphone by near field communication (NFC). The RFID / NFC tagged chemical sensor is suitable for detecting pH or ion selective electrodes as part of a network of chemical sensors for IoT. The practical application of the RFID / NFC tagging sensor was tested to detect deterioration of milk by monitoring the pH value of milk over a period of 6 days. The measurements showed the fluctuation of pH value between 5.89 and 6.10 over the 5 days, averaged to a pH of 6.03. Therefore, RFID/NFC tag sensors show potential for IoT applications. Another smart health proposal using RFID technology has been presented in [62], where smart bandage manages chronic wounds by wirelessly transmitting wound pH status to an external readout unit in the smartphone, using radiofrequency identification (RFID). This is a lightweight, noninvasive bandage proposal that saves the patient from regular hospital visits for dressing change. The pH assessment calculated in smart bandage shows high precision and accurate results when compared with regular

pH meter in the laboratory. An RFID enabled adhesive skin patch is demonstrated in [154] which monitors important biomarkers in sweat and surface temperature. In this demonstration, a commercial RFID chip is adapted with minimum components to allow potentiometric sensing of solutes in sweat, and surface temperature, as read by an Android smartphone app with 96% accuracy at 50 mM $Na+$ (*in vitro tests*).

#### 1) SECURITY CONCERNS IN RFID BASED BIO CYBER INTERFACE

RFID tags, when used with interconnected devices in environments like IoT and IoBNT can be easily compromised by attackers. Following are a few possible security threats that must be considered when using RFID based technology as bio cyber interfacing option [135]. More attack types for all types of bio cyber interfaces are presented in Section V-B.

##### *a: HARDWARE TROJAN*

Hardware trojans can modify IC of the tag hardware to allow attacker an access to its software components. This attack can be launched internally at the design phase of the RFID tag and can be launched externally through some sensors or antenna.

##### *b: SIDE CHANNEL ATTACKS*

Attacker can use specialized tool to intercept information exchange between RFID Tag and its reader and use it for malicious purpose. This attack can take place even when the messages are encrypted.

##### *c: TAG CLONING*

Attacker can clone the tag and steal sensitive information from the tag and even impersonate the tag for communication with the reader.

##### *d: TAG COUNTERFEITING*

In this type of attack, attacker gains access to tag and modifies its identity using tag manipulation techniques. Unlike tag cloning this attack can be launched with very less information.

##### *e: TAG TRACKING*

Each RFID tag has a unique identifier number. Attacker can read the tag identifier attached to a person and track his/her location at any time.

##### *f: TAG INVENTORYING*

RFID tags also contain meta information about the tag like product code and manufacturers code. This information contains the type and purpose of RFID tag. For example in medical applications attacker can get access to what type of disease a person is suffering from, through tag inventorying attack.

*Counter measures* Some of the possible countermeasures for RFID tags are

Side channel analysis: Using side channel signal i.e., timing, power and spatial temperature to detect hardware Trojans and malicious firmware.

Isolating: Protecting RFID tags from external EM waves through active radio jammers or other isolation techniques [135].

Blocking: Restricting access to the tag by public readers by using privacy bit technique. Setting the privacy bit to '1' means public scanning of tag is not possible [155].

Anonymous tag: To prevent tracking of the RFID tag from hackers, an anonymous ID is assigned to the RFID tag. Mapping between anonymous ID and genuine ID should be stored in a look up table [156].

Distance estimation: Identification of distance between tag and reader using signal to noise ratio [157].

### C. BIOLOGICALLY INSPIRED BIO CYBER INTERFACE

The domain of IoBNT is biologically inspired and adapts the design of devices and their communication mechanisms from nature. Therefore researchers are investigating methods to develop skin-mounted bio-electronics that support the seamless integration of biological materials with electrical components of the IoBNT network. In this direction, some proposals have been presented by exploiting the biochemical properties of biologically engineered materials and synthetic artificial cells to be used as device components. The device called bio-cyber interface [25], [63] is not only capable of sensing but also contains drug reservoirs to release controlled amounts of the drug upon commands received from external devices. A bioresorbable device [158] was fabricated using naturally occurring silk as the first step towards the development of remote control implantable devices. This device biodegradable device is used to eliminate Staphylococcus aureus infection from *in-vitro* environments by triggering thermal stimulations and targeted drug delivery operations. The device has the wireless capability to be turned on wirelessly and it disappears once it has performed the required task, thus eliminating the need to remove the device through surgical procedures. The use of biologically inspired materials for transmission processes in bio-cyber interfaces is described in the following scholarly works. A summarization of biologically inspired bio-cyber interfaces is presented in Table 4.

#### 1) BIOFET BASED MOLECULAR RECIEVER

Field-effect transistors (FETs) are a type of transistors that use an electric field to control the flow of current. FETs consist of three electrodes namely source, drain, and gate. In traditional FETs, voltage is applied to the gate electrode which in turn modulates the conductance between source and drain electrodes. The conductance is reflected as the voltage-current alteration in the output channel. FET based technology is now being utilized for affinity-based electrical sensing using nanomaterials (nanowires, nanotubes, and graphene) as transducer unit [30], [159]. FET transistors can be utilized for biosensing by replacing the gate electrode with

**TABLE 4.** Existing proposals for biologically inspired interface devices in academic literature.

| Name of Device | Transduction Mechanism | Description |
|---|---|---|
| Biologically Inspired Bio Cyber Interface [63] | Electrical to biochemical signal through Photoresponsive biomolecules. and Thermal responsive biomolecules - Biochemical to electrical signal through the Bioluminescence phenomenon. | - A theoretical model for bio cyber interface has been proposed as an interface between biological and electrical domains. The model comprises of transduction units that convert an electrical signal into biochemical signals through the bioluminescence process and biochemical signals into electrical signals through photoresponsive and thermal responsive biomolecules. |
| SiNW bioFET based Molecular receiver [78] | Biological to electrical signal conversion through bioFET technology. | - The Silicon Nanowire (SiNW) is used as the conductive nanomaterial for a molecular antenna. Microfluidic channel has been considered as a propagation medium for information molecules to flow from transmitter to receiver in unidirectionally through diffusion. |
| Biological Optical-to-Chemical Signal Conversion Interface [168] | Optical to chemical signal through illumination effects. | - A biological signal conversion interface is designed based on E Coli bacteria that can change the pH of the surroundings by pumping protons in response to external light stimuli. |
| Redox based Chemical to Electrical Interface [173] | Chemical to electrical signal conversion through redox modality. | - The interface prototype device consists of a dual film with inner film contains hydrogel-based film entrapping E.Coli bacteria and the outer film consists of a redox capacitor to amplify electrical signals. |
| FRET-based biocyber interface [175] | Optical to electrical and vice versa signal conversion through FRET Technology | - FRET technology has been utilized to model the uplink/downlink biocyber interface for targeted drug delivery applications of IoBNT. SIR epidemic model is adopted to model downlink and the bioluminescent reaction has been utilized to generate an uplink signal. |

a biofunctionalized surface called Biorecognition Unit (BU), for the detection of target molecules in the environment [79].

The BU contains receptors on the surface of the FET channel which binds ligands with intrinsic charges which result in accumulation depletion of carriers in the semiconductor channel, and hence modulation of conductance and current. The addition of BU in conventional FETs for molecular recognition makes them bio-inspired and is therefore called BioFETs. The bioFETs work on the principle of ligand-receptor pairing i.e., binding of a ligand (signaling molecule) to its receptor (receiving molecule) and to produce a response e.g., signal transmission. There a number of ligand-receptor pairs that can be used in modeling BU of bioFETS e.g., antibody-antigen, aptamer-natural ligand, natural receptor/ligand [160] depending upon the target molecule. Semiconductor materials like NW [161],

single-walled carbon nanotubes(SWCNT) [162], graphene [163], molybdenum polymers(MoS2) [164] and organic nanomaterials like conducting polymers [165] can be used as transducer channel of bioFETs. Among NW materials, Silicon nanowire (SiNW) has been proven to be the best fit for bioFETs due to their low power consumption, high-speed sampling, high integration density, and high sensitivity [140], [166], [167].

In this direction, Kuscu and Akan [78] have proposed SiNW bioFET based molecular antenna which receives information molecules as biochemical signals and converts them into equivalent electrical signals. The proposed model employs the theory of ligand-receptor binding and considers microfluidic advection-diffusion channel for the propagation of information ligands. The receiver model consists of three functional units. The Biorecognition Unit (BU) works as the interface for sensing the concentration of ligands. In the Transducer Unit (TU), ligand-receptor regulates the gate potential of the FET through the field effect resultant from their built-in current charges. The output unit shows the current flow as a result of the modulated gate potential. Moreover, an analysis and optimization framework has been presented by providing a closed-form expression for fundamental performance metrics, such as SNR and SEP. The proposed SiNW bioFET is capable of providing efficient in-device, label free and continuous processing of sensed molecules.

#### 2) OPTICAL TO CHEMICAL BIOLOGICAL INTERFACE

Grebenstein *et al.* [168] proposed a microscale modulator to transduce optical signals into chemical signals. The modulator is realized using synthetically engineered E.Coli bacteria that express protons into the environment upon stimulation from an external light source. Light-emitting diode (LED) of the modulator uses proton pump gloeorhodopsin (GR) to express light. The E.Coli bacteria change the pH level of their surrounding environment as a chemical reaction to an external light source. The proposed testbed achieves higher data rates on the order of 1 bit/min as opposed to previous proposals with data rates of 1 bit/hour.

#### 3) REDOX BASED CHEMICAL TO ELECTRICAL INTERFACE

New research in biology has recommends the usage of redox as a global signaling modality. Authors in [169] have adopted an approach that is inspired by sonar, which access the redox information through collaborative electrochemical probing. Authors further utilize attuned electrical inputs that are coupled with diffusible redox mediators (electron shuttles) to access redox information in a local environment and generate complex but interpretable electrical output signatures. Redox (Oxidation-Reduction) reaction is also utilized for biochemical-electronic transduction mechanisms in a number of proposals [170]–[174]. A wet lab interface prototype has been proposed recently in [173] for transducing chemical signals into electrical signals by the virtue of redox modality. The nterface prototype device consists of a dual film with inner film contains hydrogel-based film entrapping E.Coli bacteria and the outer film consists of a redox capacitor to amplify electrical signals. These cells are engineered as reporters, which respond to the presence of a certain molecule (signaling molecule AI-2) by converting the redox inactive substrate 4-Aminophenyl $\beta$-D-galactopyranoside (PAPG) molecules into redox-active p-aminophenol (PAP).

#### 4) FRET BASED UPLINK/DOWNLINK BIO CYBER INTERFACE

FRET (Fluorescence Resonance Energy Transfer) mechanism has been adopted by Abd El-Atty *et al.* [175] to model uplink/downlink bio-cyber interface for the Internet of bio nano things. In FRET-based optical sensing, bio-cyber interface is designed for targeted drug delivery applications of IoBNT. The downlink of bio-cyber interface is designed by adopting spreading principals of SIR (Susceptible, Infected, Recovered) epidemic scheme and decode forward (DF) basis. Three types of nanomachines are used in the downlink model to realize the targeted drug delivery namely nanoreciever, nano transmitter (Infected) and nanorelay(Susceptible) according to SIR epidemic scheme. The recovered nanomachines are ones that have transmitted their exciton to the nano receiver. The uplink is designed by considering two types of nanomachines namely nanosensors and nanoactuators. Uplink signal notifies the medical server about successful drug delivery through bioluminescence reaction.

#### 5) SECURITY CONCERNS IN BIOLOGICALLY INSPIRED BIO CYBER INTERFACE

Currently the research bio cyber interface security is immature and there is a minimum published literature in this field. Reference [176] have presented the possibility of ML based adversarial attacks for biologically inspired bio cyber interface which are presented below. Details of possible generic attacks on bio cyber interfaces can be found in Section V-B.

#### 6) MACHINE LEARNING ADVERSARIAL ATTACKS

In the case of bio-luminescent or thermal signaling based bio cyber interface adversaries might launch an attack by manipulating the internet-enabled parameters. By manipulating the parameters, attackers can cause inappropriate amount of drug release, initiate self-annihilation of drug molecules and modify monitoring information provide by bio chemical processes. In redox based bio cyber interfaces, changing the input electrical signal can lead the capacitor charging and unwanted redox activity such as activating/deactivating the redox substrate to affect enzyme production. Bio FETs work on the principals of ligand binding through charging of electrodes. The attacker can launch sentry attack to repel required ligands or black hole attack to attract unwanted ligands to bind to the receptor to affect the current control. The changes in external current control can cause the Bio FET based bio cyber interface to exhibit unwanted behavior.

*Countermeasures* The attacks related to biologically inspired bio cyber interfaces can be categorized as

ML-adversarial attacks. Possible countermeasures to ML adversarial attacks are [42]

Data sanitization: This process refers to pre-processing, validating all the input data, and rejecting the harmful samples.

Adversarial training: Inclusion of adversary information in the training samples to recognize attack vector.

Defence distillation: Creating secondary ML model with less sensitivity and more general results.

Differentail privacy: A cryptographic mechanism of adding noise to susceptible features of data. Hormonic encryption. A cryptographic mechanism to perform computations over ciphered data to generate encrypted result.

### D. SUMMARY OF BIO CYBER INTERFACE CLASSIFICATION

It is obvious from the above-mentioned literature that there are a lot of possibilities for designing a bio-cyber interface. The design model of the bio-cyber interface primarily depends on the application scenario. For example, a bio-cyber interface design and components for sensing applications will be different from drug delivery applications. Our take on the choice of bio-cyber interface option goes in the favor of bio-inspired interfaces. The reason being biocompatible in nature and the research in these interfaces in line with the direction of IoBNT. Extensive in-vitro and wet-lab experiments are required to validate the theoretical proposals for the bio-cyber interface.

## V. SECURITY IN IoBNT

The advent of skin implanted bio-electronics and the IoBNT paradigm will not only open up a plethora of novel biomedical applications but also its wireless connection capability will enable the adversaries to utilize it malevolently. Connecting the intra-body biological environment with the cyber domain through bio-electronic devices will provide the attackers with an apparent opportunity to devise new terrorist mechanisms to harm the patient remotely. Maliciously accessing the human body through the internet to steal personal information or to create new types of diseases by malevolent programming of bio-electronic devices and intra-body nanonetworks is termed as bio-cyber terrorism [25]. Bio-cyber terrorism can take advantage of wirelessly accessing the human body to launch fatal and life-threatening attacks from a remote site. Therefore security features have to be embedded either in a separate component of the bio-electronic device, which may enlarge the size of the device or might be infeasible in some applications. Another possibility is to delegate security services to external devices in close proximity with sophisticated resources as compared to bioelectronics devices. For example, in a similar field of IMD (Implantable Medical Device), some researchers propose to assign security functionality to an external device like Cloaker or MedMon [177]. Nonetheless, the bio-electronic device must execute a lightweight authentication mechanism at least once to establish a secure connection with external devices. Bio-electronic devices will also be linked to a gateway device (such as a smartphone) to send and receive information from the healthcare practitioner. Because of the technological differences, this section discusses the security needs for nanonetworks and bio-cyber interfaces separately. The security goals, regardless of the underlying technological variations, remain the same. The STRIDE threat approach can be used to model security threats against IoBNT. STRIDE is the acronym for Spoofing, Tampering, Repudiation, and Information Disclosure, Denial of Service and Elevation of privilege. These six categories present a broad classification of threats and can be further divided into other related threats. Each threat category is related to a security goal: Spoofing-Authentication, Tampering-Integrity, Repudiation, Non-Repudiation, Information Disclosur, Confidentiality, Denial of Service- Availability, and Elevation of privileges-Authorization [178], which is presented in Table. 5.

**Authentication (Au):** Authentication ensures that the identity of each communicating party is established before executing any operation. Moreover, authentication also ensures that the data is coming from the authorized source and unauthorized users cannot access or modify the data. Authentication needs to be done on users as well as a message [29], [179].

**Integrity (I):** Integrity ensures that the message exchanged between legitimate entities is not tampered or modified by unauthorized entities.

**Non- Repudiation (NR):** In the traditional networking paradigm, all the communication transactions are logged to track the network anomalies and gain the attacker's profile in case the attacker tries to misuse his/her privileges. Nonrepudiation can be violated if the attacker gets access to the logs and delete the records to remove traces.

**Confidentiality (C):** Confidentiality ensures that the attacker should not learn the content of the message exchanged between the sender and receiver. The data must only be accessible to authorized personnel upon authentication through some mechanism priory.

**Availability (A):** This goal ensures that the services and communication of the device are always available on request.

**Authorization (Auth):** Authorization property ensures that only those entities can execute a specific operation that has privileges to order it. Authorization requires that an entity must have been authenticated previously through the regular login (ID, password) procedure to establish the identification.

### A. ATTACK TYPES IN NANONETWORKS

This section presents the possible attacks and existing proposals related to the nanonetworks. A summarization of security proposals for nanonetworks is presented in Table 6.

#### 1) EAVESDROPPING

Eavesdropping refers to passively listening to the transmission between two nodes. The listened information can be stored and later used maliciously to launch attacks. Eavesdropping in nanonetworks can take place when

**TABLE 5.** STRIDE threat model categories, related security goals and attack possibilities in IoBNT.

| Threat | Security Goal | Possible IoBNT Scenario |
|---|---|---|
| Spoofing | Authentication | Security breach by interception of communication between bio-electronic device and the smartphone. |
| Tampering | Integrity | The dosage prescribed by the medical server can be altered during transmission by the attacker and drug is released according to altered values. |
| Repudiation | Non-Repudiation | Deletion of access logs to remove traces of malicious user activities. |
| Information Disclosure | Confidentiality | Security breach by interception of communication between bio-electronic device and smartphone. |
| Denial of Service | Availability | Inability to transmit irregular vital signs of an elderly or unconscious patient who is solely dependant on the bio-electronic device for communication with the medical server. |
| Elevation of Privileges | Authorization | An internal attacker can misuse access privileges to steal or tamper information. |

two legitimate nanomachines are exchanging messenger molecules and a nearby malicious nanomachine intercepts the messenger molecules silently. The passive eavesdropper can be detected in nanonetworks by a mechanism such as stochastic geometry, distance estimation techniques. The active eavesdropper might absorb the messenger molecules in the case where MC is used as a communication medium, this attack might be prevented through secrecy capacity. Other anticipated eavesdropping prevention mechanisms include beamforming, game theory (collation formation games), and artificial noise generation.

Several proposals have been demonstrated to detect eavesdropper location and secure the nano communication paradigm from eavesdropping attacks.

Islam *et al.* [180] proposed a secure channel for Molecular communication. Firstly, a Diffie–Hellman algorithm-based secure key is exchanged between sender nanomachine and receiver nanomachine. Then hardware ciphering is performed using the secret key. As MC is a resource-constrained paradigm, therefore, Exclusive OR (XOR) cipher is used in this work due to its simple implementation and inexpensive computation. Moreover, hardware ciphering used in this work further reduces the associated time, instead of its software counterpart. The results are presented through simulation. In our opinion, the proposed method is simple and computationally less expensive but the overall security is compromised as MC needs more mathematically resilient models for security.

Guo *et al.* [181] have proposed a mathematical model for eavesdropper detection and localization in a random walk channel. This is the only work in MC that considers the detection of an absorbing malicious receiver in a random walk channel. The authors have chosen transmitter side detection of the eavesdropper because the MC channels are 1-D and receivers cannot affect the transmission and secondly the molecules absorbed at the receiver are quite small that do not aid in detecting eavesdropper presence. Simulation has shown accurate results in detecting the eavesdropper's presence.

Recently a proposal for physical layer authentication for Diffusion Based Molecular Communication (DbMC) has been proposed in [182]. The channel impulse response of 1-D DbMC has been exploited to detect transmitting eavesdropper in the transmission region.

### 2) BLACKHOLE ATTACK

Blackhole attack refers to the attack where malicious nodes spread attractant molecules to draw the network traffic towards a different location from the intended target. Blackhole attack is similar to sinkhole attack in WSNs but the sinkhole attack disrupts the routing process while the blackhole attack physically moves legitimate nodes away from the target. When it comes to blackhole attacks in nanonetworks, there are a variety of approaches that can be taken. For example in scenario of artificial immune system support application, the white blood cells that are responsible for detecting and tackling with the infection, can be attracted by malicious nodes to stop them from detecting an infection in the host system.

Blackhole attack and its countermeasure using two approaches, Bayes rule and simple threshold approach for

**TABLE 6.** Security proposals for nanonetworks in literature.

| Ref. | Communication Medium | Type of Attack | Proposal Description |
|---|---|---|---|
| Secure Channel for Molecular Communications [180]. | Molecular Communication | Eavesdropping | Encryption using Diffie–Hellman algorithm. |
| Eavesdropper localization in random walk channels [181] | Molecular Communication | Eavesdropping | Eavesdropper detection and localization by reverse estimating its location. |
| Congestion Control in Molecular Cyber-Physical Systems [185]. | Molecular Communication | Congestion | Congestion detection algorithm for Diffusion Based MC. |
| Security Vulnerabilities and Countermeasures for Target Localization in Bio-NanoThings Communication Networks [183]. | Molecular Communication | Black hole, Sentry Attacks | Construction of decision process using two approaches, Bayes rule and simple threshold approach for the robustness of legitimate nanomachines. |
| Physical Layer Authentication in Nano Networks at Terahertz Frequencies for Biomedical Applications [184] | Nano Electromagnetic Communications | Spoofed, Altered, Replay message attack. | A distance-dependent path loss based authentication scheme. |
| In-sequence molecule delivery over an aqueous medium [186] | Molecular Communication | Desynchronization | A formal model for in-sequence message delivery for MC which can possibly prevent Desynchronization attack. |
| Channel Impulse Response-based Physical Layer Authentication in a Diffusion-based Molecular Communication System [182] | Molecular Communication | Eavesdropping | The channel impulse response of the physical layer has been exploited to propose an authentication scheme for the detection of transmitting eavesdropper in the broadcast region. |

MC have been proposed in [183]. Blackhole attacks are type of DoS (Denial of Service) attack in which nanomachines can be drawn away for target e-g in case of targeted drug delivery the actuator nodes might not reach the target due to Blackhole attack.

### 3) SENTRY ATTACK

Sentry attacks are opposite to Blackhole attacks where legitimate nanomachines are impeded away from the target, due to a large number of repellent molecules spread around the target location by malicious nodes. This kind of attack can be fatal in medical applications where instant lifesaving action needs to be taken e-g nanorobots that are designated to prevent bleeding by repairing veins are attacked by a sentry to impede from reaching the target. Sentry attack and its countermeasure using two approaches, Bayes rule, and simple threshold approach have been proposed in [183]. Giaretta *et al.* [183] have proposed a blackhole attack and sentry attack for MC. The authors have described two scenarios where (L-BNTs) Legitimate Bio-Nano Things are repelled from reaching the targeted site in targeted drug delivery application, thus keeping Bio-Nano Things from performing the normal operation. In the second scenario called black hole attack, M-BNTs (Malicious Bio-Nano Things) are attracted to the targeted site which can lead in a delivery unwanted dosage of medication in the targeted area.

Next, in the proposal, a countermeasure that enables the Bio- NanoThings to make decisions and cooperate in order to overcome blackhole and sentry attacks during target localization is proposed. The mechanisms are based on known cellular decision processes using Bayes' rule as well as artificially designed genetic circuits that evaluate chemical signal threshold (this will be known as Thresholdbased decision process), which are both lightweight enabling them to be easily implementable on resource constrained Bio- NanoThings. Results show that the proposed countermeasure is effective against the attack, where L-BNTs successfully move towards the target.

#### 4) SPOOFED, ALTERED, REPLAY MESSAGE ATTACK

This attack can be launched by malicious nodes by spoofing legitimate nodes identities to become trustable and enter the network. Furthermore, the malicious nodes then send fake messages in the network and alter the data. In the case of nanonetworks, consider an exemplary communication scenario where a legitimate node 'Alice' is transmitting messages to receiver 'Bob'. Attack can be launched by an intruder ''Eave'' impersonates to be Alice and tries to control Bob by sending malicious commands.

A distance-dependent path loss based authentication scheme for nanonetworks using the terahertz band has been proposed in [184] for spoofing attacks. Rahman *et al.* [184] have proposed an authentication scheme for terahertz band EMbased nanonetworks. This work exploits physical layer attribute i.e., distance-dependent path loss for authentication at nano receiver. Moreover, an algorithmic solution has been proposed for the authentication scheme. Experimentation verification of authentication scheme via tera hertz time-domain spectroscopy setup at QMUL, UK.

### B. ATTACK TYPES IN BIO CYBER INTERFACE

To ensure an end-to-end protection of IoBNT applications, the security of these bio-electronic devices is a prerequisite. In order to pursue a preliminary investigation for types of attacks that are possible in bio-electronic devices, the attack vectors are explored in related fields like WBAN. (Wireless Body Area Network) [28], IMD (Implantable Medical Devices) [178] and Wireless sensor networks [187]. This investigation has helped us to individuate attacks that are likely to occur in bio-electronic devices. The major objective of a bio-electronic device in the IoBNT healthcare application is to enable two-way communication between intra-body nanonetworks and healthcare provider. The communication mode is divided into two categories: inbound and outbound, making it easier to recognize and categorize attacks. Figure 6 presents possible attack types in case of bio cyber interface.

#### 1) EAVESDROPPING

Eavesdropping is a passive attack that enables the attacker to covertly gain access to confidential information. The bio-electronic device might possess critical information like patient identification information, clinical history, disease detail, treatment detail, patient location, and battery status, etc. This confidential information can be exploited not only to breach a patient's privacy, but also to launch other types of active attacks. Eavesdropping can be realized during the communication of bio-electronic devices with biological nanonetworks and during communication with the gateway devices.

*Countermeasures:*Traditional networking paradigms employ encryption schemes like RSA and DES, to prevent against eavesdropping attacks. These encryption schemes are effective for the prevention of eavesdropping attacks, but these are computationally expensive and must be adopted after analyzing the resources of bio-electronic devices [188]. Lightweight encryption schemes like Elliptic Curve cryptography has been proven to be effective for resource-constrained devices [189], also a review on other lightweight encryption schemes has been presented in [190].

#### 2) REPLAY ATTACK

This type of attack can be launched after a successful eavesdropping attempt. The eavesdropped authentication sequence of the legitimate devices can be replayed to get illegitimate access into the communication channel. Moreover, an attacker can copy previously sent commands from legitimate users to replay the message again which in the case of bio-electronic can have a number of consequences like drug release multiple times which harm patient's health, unnecessary and repeated queries for patients physiological values to engage and deplete the resources, etc.

*Countermeasures:* Authentication schemes, Intrusion detection, delegate authentication to external devices. (See Section VI).

#### 3) MAN-IN-THE-MIDDLE (MITM) ATTACK

A MITM attack is projected through illegitimate devices when they become part of communication between legitimate transmitting devices, and legitimate devices are spoofed to believe that they are communicating with the authorized device. In the case of bio-electronic devices, the attacker must be in the vicinity of the patient to launch the MITM attack. From the communication perspective, the MITM attack can be achieved by replaying the legitimate authentication sequence to get access to the communication channel. MITM is the type of an active eavesdropping attack where the attacker not only listens to the communication but also alters the data and communication sequence.

*Countermeasures*:Traditionally MITM is prevented using encryption schemes. A lightweight scheme to prevent implantable medical devices from MITM attacks has been proposed that utilize chaotic generators for randomness and a signature algorithm to prevent third-party interference [191].

#### 4) RESOURCE DEPLETION (RD)

Bio-electronic devices are essentially capable of performing *in-situ* [77] operations and for this purpose they contain built-in processing unit, memory unit, and power unit. However, these units are only able to perform trivial tasks due to

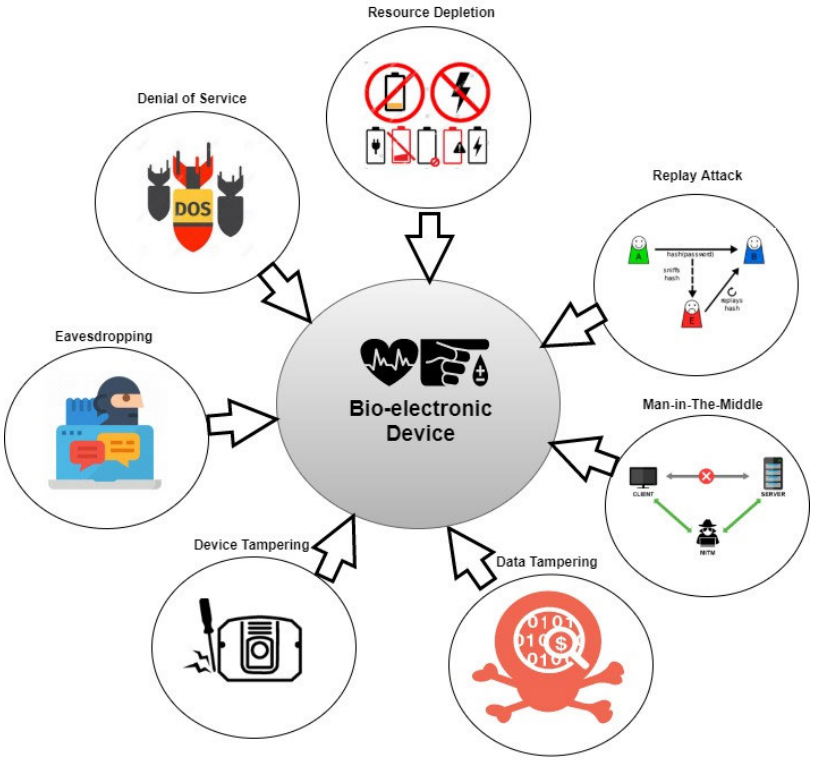



**FIGURE 6.** Types of possible attacks for Bio Cyber Interface.

resource limitation in terms of space, power consumption and computation complexity, which comes with their minute size. The attacker can cause resource depletion by sending multiple authentication messages with the wrong credentials to occupy the processer. Each authentication request is processed which exploits the memory to create access logs and drains the battery. Moreover, bogus communication packets sent by MITM can utilize and drain the resources. *Countermeasures:* Access control mechanisms, Anomaly detection system, user notification, and use of rechargeable batteries. Moreover, mitigation from resource depletion attacks can be achieved by using passive wireless communication media like RF signals and the use of novel energy preserving techniques like ZPD (ZeroPower Defence) [192].

### 5) INJECTION ATTACKS

Injection attack can be performed by the illegitimate users in three ways, insertion, alteration and replication [135]. In insertion attack, hacker generates new seemingly legitimate data packet into the communication channel. In alteration attack, hacker captures the data packet from communication link, tamper the values of dosage commands from the inbound channel and alter the values of bodily parameters in the outbound channel. In replication attack, attacker re-sends previously executed commands into the system. Insecure communication between bio-electronic and gateway devices can result in an injection attack. This attack can have fatal consequences on the patient. For example in a scenario where a diabetic patient is fully dependent on wirelessly controlled insulin and glucose monitoring pump [73], the alteration in dosage values received from health care provider can result in hazardous consequences like under-dose can cause hyperglycemia and overdose can result in hypoglycemia both of which can be fatal [193]. *Countermeasures:* Careful mitigation strategies are needed to be designed which include authentication protocols [194], access control mechanisms [178] Intrusion Detection, Input validation, and Authorization techniques.

### 6) DEVICE TAMPERING

This attack is majorly launched in the bio-electronic devices by local attackers, due to low transmission range of bio-electronic devices. The device can be reprogrammed or physically replaced to perform the malicious tasks that are not intended by the device in the first place. This attack can also be launched by accessing the device remotely by sending fake firmware update and device upgrade message that alter the software configuration of the device to perform maliciously [195]. This attacker can alter the original treatment prescribed by the healthcare provider and replace it with false treatment which can cause life threatening consequences. *Countermeasures:*Tamper proofing and

self destruction, device hardening, and Physically unclonable Function (PUF).

#### 7) DENIAL OF SERVICE (DOS) ATTACK

Denial of service attack causes disruption and blockage of information flow between legitimate communicating parties. An attacker tries to suspend services of the bio-electronic device to make it unavailable for communication and processing. DoS can be launched in the form of any of the above-mentioned attacks. The DoS attacks such as battery drainage, sleep deprivation and outage attacks can be performed by hackers after getting access to the devices. As the power source of these devices is limited and attackers can send an unlimited number of messages, causing the battery to drain. In outage attacks the device can be made unavailable by stopping it from carrying its essential functions, behaving abnormally or premature shutdown. These types of attacks can pose serious consequences for the patients [135]. Moreover, the hacker can intentionally drop the forwarded packets, making the recipient deprived of requested data. *Countermeasures:* Intrusion Detection.

#### 8) MALWARE ATTACKS

Malware attack is another type of network attack that is common in IoT based applications. Malware attack is used to remote control a distant device maliciously, steal sensitive information from a device and use it to launch further malware attacks. A system infected with malware attack may start running certain programs automatically like sending messages, re-configuring internal software and turning of anti virus. In case of IoBNT application an infected bio cyber interface might start dispensing inappropriate amount of drugs, thus causing harm to the patient. Some of the popular malware attacks that are still active in IoT environments are Mirai, Echobot, Reaper, Emotet, Gamut and Nucer [196]. There different types of malware attacks, but malware attacks specific to IoBNT applications can be botnets, rootkit, ransomware, and keylogger attack.

**Botnets:** In this type of attack, attacker gains access to a number interconnected devices by launching malware and further control them to steal information, launch DDoS (Destributed Denial of Service) attack to launch unplanned system downtime and even sell network access to other cyber criminals.

**Ransomeware:** The attacker gets hold of the device by encrypting user's data and locks the device, thus, restricting access of the owner to the device. The attacker than demands for some ransome amount by displaying messages on the device screen.

**Keylogger:** It is a malicious piece of code that records the keystrokes of user to gain access to ID and passwords. This attack is dangerous than brute force attacks and strong passwords does not provide protection against this malware.

**Rootkit:** A malicious piece of code is installed on IoT device that hides its identity to steal data, reconfigure the device, or control the system by executing malicious commands. This kind of attack is most dangerous as it bypasses all the security mechanisms and successfully hides its presence.

*Countermeasures:* Access control, device hardening and system monitoring, Antivirus, Intrusion Detection. (See Section VI).

#### 9) FIRMWARE ATTACKS

Firmware updates are necessary in order to ensure proper device functioning. The firmware updates can be done remotely or directly(through usb port). An advertisement is usually broadcast on the network whenever a new version of the firmware update is available. Hackers can send false firmware update requests to the users in order to access the firmware and program it with malicious code. Fake firmware updates can cause fatal consequences to the patients. *Countermeasures:* Firmware Encryption, periodic firmware updates, malicious firmware detection.

### C. SUMMARY ON THE SECURITY OF IOBNT

The protection of IoBNT based systems is crucial as the consequences of security compromise can be detrimental. A summarization of existing security proposals for nanonetworks is presented in Table 6. Apart from the software attacks mentioned in the above section, there exist some other attributes can effect the security of IoBNT. The origin from where the attack has been instantiated can help in providing some insights into the profile and goals of the attacker. Local attacks require the attacker to be close to the physical location of the patient. Local attackers can replace the bio-electronics device with a maliciously programmed device, can eavesdrop the communication between bio-electronic devices and gateway devices to gather information to launch an active attack remotely. Remote attacks are launched outside the premises of the bio-electronic devices. These attacks can be launched by accessing the smartphone of the patient that is delegated a gateway device, to send malware and reconfiguration requests to reprogram the device. In wireless communication, attackers can evade the system in two possible ways: active and passive. Passive attack is launched by an attacker silently without revealing their presence in the system. A passive attack can violate the privacy of the patient and can reveal confidential information about the device. By just intercepting the communication, a passive attacker can gather information like the patient's location, diagnosed disease, type of treatment, etc. This information can be used to further mount active attacks. Active attacker not only enables the attacker to read the transmission but also uses this information to disrupt the communication. The active attacker can modify the messages in transit, drop the messages so they do not arrive at the destination, block the communication, reprogram the device and even induce a shock to the patient by manipulating the device. As the major application of area of IoBNT is bio medicine, therefore, breach in security means life threatening consequences.

## VI. POTENTIAL MITIGATION STRATEGIES

This section discusses the network security methods employed in typical wireless networks, as well as the potential for each measure to be applied to the domain of bio-electronic devices.

### A. CRYPTOGRAPHIC MECHANISMS

Cryptographic primitives are efficient security mechanisms that protect the wireless channel from attacks that cause device tampering and information disclosure. Moreover, cryptographic mechanisms enforce access control to ensure that information is accessible to authorized entities only. Cryptographic solutions depend upon key management and distribution. There are three possible ways in which key distribution can take place i.e., unkeyed, symmetric key and public-key cryptography. Unkeyed cryptography does not use any key and is mainly implemented as hash functions or one-way permutations. This scheme can be implemented using Message Authentication Codes, pseudo-random sequences, block ciphers, and identification primitives [178]. In asymmetric key distribution schemes, a secret key is shared between communicating parties which is used to generate an authentication token. The authentication token is used to access the device and to encrypt the communication. In symmetric cryptography key distribution can take in two ways; pre key distribution and on-demand key distribution. In pre key distribution, key is pre-loaded inside the communicating entities. Pre key distribution is efficient in the environments where number of communication parties is less and fixed. On demand key distribution is suitable for distributed and scalable environments. In asymmetric or public cryptography two sets of keys i.e., public and private, need to be shared among communicating entities. This scheme depends upon high message exchange for authentication procedure which makes it expensive in terms of computation and power consumption. Additionally, ciphers in this scheme result in complex circuits that demand high computation resources [197], [198]. Due to these limitations, public-key cryptography is not feasible for resource-constrained devices. The feasibility and application of cryptographic schemes for bio-electronic device security are questionable. The envisioned bio-electronic devices have limited memory and maximum of which will be occupied by biomedical functionality. Inclusion of expensive security primitives is not possible in the current situation; however additional memory chips can be integrated into the device for security functionality. This might also not be recommendable as it will increase the size of the device [178].

### B. DEVICE HARDENING

Device hardening and system monitoring has been pointed out in [199] to mitigate malware attacks. The device hardening refers to restrict unauthorized access to the device by blocking unused communication ports and denying access to unknown IP addresses, blocking reboot from alternate media. In security monitoring the event logs of network traffic to and from bio cyber interface must be continuously monitored to detect an anomaly at early stages.

### C. DELEGATION TO EXTERNAL DEVICES

As discussed above that limited memory of bio-electronic devices restraint them from executing sophisticated security solutions. Some authors in a similar domain of resource-constrained devices have suggested delegating a part or all of the security functionality to external devices. These devices will not be part of the human body but can be thought of as wearable bracelets, watches or even a smartphone that patient carries all the time. Delegation of security to an external device will allow using expensive encryption, cryptographic and accessing control mechanisms. These external devices will work as an authenticating device that checks the incoming requests before transmitting them to the bio-electronic device. Some proposals in this direction can be found for security in IMD like MedMon [177], IMD Cloaker [200] and RFID Guardian [201]. The idea of using an external device has some drawbacks as well. The external device can itself be compromised and impersonated by malicious entities to communicate with the bio-electronic device. Moreover, if the device is lost the bio-electronic device will become unavailable to queries and commands from remote healthcare providers.

### D. INTRUSION DETECTION (ID)

There are two types of intrusion detection schemes; signature-based intrusion detection and anomaly-based intrusion detection. In signature-based ID schemes new data is confronted with the pre-recorded intrusions dataset and in case of match countermeasure mechanisms are activated. Intrusion detection techniques are used as a classical security solution to thwart DoS attacks. DoS attack can be launched in bio-electronic devices by depleting the limited resources and ultimately making the device unavailable. Anomaly detection in wireless communication is generally performed by evaluating observable wireless patterns (time, frequency, location, etc.). Hei et. al. [202] have proposed a Support Vector Machine (SVM) based algorithm to defend against RD and DoS attacks. The application runs on the patient's smartphone and takes five types of input data to carry out detection: reader action, a time interval of reader action, time of the day, location, day of the week. The classifier is trained with regular input patterns. When the new request comes in, SVM validates the input data and reply accordingly. Access is granted if the data is valid, access is denied if the credential is wrong and if a request is repeated frequently with wrong credentials, the application sends sleep command to IMD and turns off to external requests. Similar to proposals of IMD and other resource-constrained devices, intrusion detection techniques can be implemented for bio-electronic that employ active jamming techniques to deny access to an adversary. Research efforts in security are now utilizing Artificial Intelligence (AI) for intrusion detection systems. There are three

main catagories of AI that can be utilized to detect intrusions in a system. Supervised learning category can include techniques based on SVM and naïve bayes classifier, the second category is the semi supervised learning that includes techniques such as K-means and K-nearest neighbours and the third category id deep learning. A review on AI based ID techniques for software defined wireless sensor networks can be found in [203]. An intrusion detection system for wireless nanosensors has been proposed [204] that aims at detecting malicious nodes and data. This proposal is based on a literature survey and does not provide satisfactory experimental results.

### E. ACCESS CONTROL

Access control mechanisms enforce rules and policies to prevent unauthorized access to the devices. Most of the access control schemes revolve around the concepts of a subject, object, and rights. A subject is an entity that requests to access the device, an object is an entity that needs to be accessed e.g., file, data, image, etc. Rights are the permissible operations that can be performed by a subject e.g., read, write, modify, etc. Access control policies are applied to the subjects after authentication, which provides the identification of requester and access grant decision is made on the basis of requestor identity. Two popular access control methods are ACLs (Access Control Lists) and PKI (Public Key Infrastructure) [178]. ACL is based on discretionary access control that provides a matrix containing subjects, objects they can access and rights that they possess over the objects. While PKI is a certificate-based solution, the requester receives an authentication certificate in each session of connection establishment with the object. The most popular authentication schemes in access control are RBAC(Role based Access Control) and ABAC(Role based Access Control). In RBAC, access is granted over the object according to the rights of roles. Where as in ABAC access to an objected is granted after evaluating attributes of the requester. Another light weight authentication scheme for IoT environments is ACE (Authentication and Authorization for Constrained Environments) [205]. Access control mechanisms can be used in parallel with other encryption or cryptographic measures.

### F. COMMUNICATION TECHNOLOGY SPECIFIC SECURITY

Bio cyber interfaces can communicate with gateway devices using a number of communication technologies such as Bluetooth, 4G and other next generation technologies, BLE, and Wi-Fi, to name a few. Each communication technology poses security threat to user's. Therefore, security in communication technologies must be preserved.

### G. HARDWARE BASED SOLUTIONS

To counter the device tampering attack, some hardware based solution can be implemented [135]. Tamper proofing and self destruction: Use of tamper proof packages for bio electronic devices and execution of self destruction mode upon encountering a physical attack. PUF(Physically Unclonable Function): PUF is a function in which a noisy fuction is added to the IC(Intergrated Circuit) of the device. PUF is unclonable and tamper-proof. Moreover, PUFs has unique object identification and authentication which can detect unintentended changes in the IC.

### H. CONSUMER TRAINING

End users i.e., patients, clinicians or care takers must be given training and demo sessions about the possible risks of this technology [42]. Moreover, users must be notified if an attack is detected to take part in defense by turning of the device.

### I. SUMMARY OF ATTACK MITIGATION TECHNIQUES

Along with the implementation of countermeasures, below are listed some of the general security guidelines for a secure holistic IoBNT eco-system [135].

- IoBNT is envisioned to use the IoT communication backbone for communication *via* internet. The already established field of IoT provides security solutions for each layer i.e., link layer, transport layer and network layer [135]. These security solutions are equally application for IoBNT applications.
- Secure boot process for the device is a critical security requirement as hackers might add a malicious patch which leads to replacing device's firmware with malicious one.
- Multi-factor authentication schemes like biometric information of the patient and strong access control mechanisms will make the access challenging to the hackers.
- Creating logs of device activity and access events will aid in detecting the anomalies both malicious and unintentional.
- Initiatives for user awareness and risk factors of this novel technology will definitely aid in a secure IoBNT system.

## VII. CHALLENGES AND OPPORTUNITIES

This section provides a detailed discussion on the challenges and opportunities for IoBNT and its security.

### A. CHALLENGES FOR IOBNT

The knowledge of computer scientists is far from being complete in the field of biology, electrochemistry, mechanical engineering, and physics. The seamless interface between biological and electrical world is only possible when researchers form interdisciplinary fieldwork in close integration. These devices need a collaboration of researchers for the above-mentioned disciplines to make them a reality. In this direction, research groups from chemical engineering, mechanical engineering, biological sciences, and computer sciences are already working individually.

#### 1) NANO NETWORKS CHALLENGES

The functionality of nanomachines can be heavily affected by changes in surrounding environmental factors such as pH

**TABLE 7.** Attack types, Counter measures and compromised security goals in Bio cyber interface.

| Attack Type | Possible Countermeasure | Compromised goal |
|---|---|---|
| Eavesdropping | Access Control Strong cryptographic schemes | Non-Repudition Confidentiality Authorization |
| Replay | Intrusion detection Delegate authentication to external devices | Authentication Confidentiality |
| MITM | Cryptographic primitives | Availability Authentication |
| Resource Depletion | Access control mechanisms Anomaly detection system User notification Use rechargeable batteries | Availability |
| Device Tempering | Tamper proofing and self destruction Device Hardening Physically unclonable Function (PUF) | All |
| DoS | Intrusion Detection Analysis of the physical medium Use of directional antennas | Intergrity Availability Non-Repudition Authorization |
| Malware | Access control Device hardening and system monitoring Antivirus Intrusion Detection | Confidentiality Integrity Availability Authentication |
| Firmware attack | Firmware Encryption Periodic Firmware updates Malicious Firmware detection | All |
| Injection Attacks | Intrusion Detection Input Validation Authorization Techniques | Integrity Non-Repudiation Authorization |

levels and temperature etc. An attacker might alter the environmental factors with malicious intent to make the communication ineffective. Moreover, if an attacker gains physical access to the human body there are some possible attacks that an attacker can launch to disturb the functionality of nanomachines. For example, attackers might inject reprogrammed nanomachines to destroy the previous therapeutic nanonetwork. The physical medium in which the nanonetworks are deployed poses unique fluidic medium physical attacks that are specific to the surrounding environment where nanonetwork is deployed. For example attacks such as:

- Viruses in the human body might compromise the communication between deployed nanomachines.
- Inherent Human Immune System of the patient's body may try to destroy the nanomachines by interpreting them as intruders.
- Data might become unreliable due to signal propagation and changes in the propagation medium.

Other specific nanonetworking challenges are listed below:

#### *a: TRANSMITTER AND RECIEVER DESIGN*

The design of nano transceivers is the preliminary step towards the realization of fully operational nanonetworks. There are two approaches found in theory that can be adopted for the development of envisioned nano transceivers; biological structures enabled by synthetic biology and nanomaterials based structures. The MC theory still relies on assumptions as there is no implementation of artificial nano/microsystem to date, yet the theory is loaded with a plethora of design options for nano transmitters and receivers, the feasibility of which could not be validated. There is a clear discrepancy between theory and practice, further research, in theory, should be coupled with experimental validation. Particularly, *in-vitro* wet labs should be envisioned for healthcare applications that will be subjected to further clinical trials.

#### *b: ADDRESSING IN NANONETWORK*

Another major challenge related to nanonetworks is the naming and addressing of nanomachines. There are a huge number of nanomachines in a nano network, addressing each nanomachine with a unique identity is not feasible. However, novel addressing schemes such as FCNN (Function Centric Nano Networking) [206] is an option for dealing with the addressing issue. Instead of addressing each and every node, FCNN based approach assigns addresses to functions and location of the body.

#### c: POWERING NANOMACHINES

The issue of power source is very crucial in nanomachines, as nanomachines are not connected to an external power source. Moreover, the battery unit is mass wise the largest unit which may increase the size of nanomachines which is undesirable. Therefore, energy scavenging schemes for drawing energy from inside the body needs to be investigated.

#### d: SAFETY CHALLENGES

Physical protection of patients is very crucial so that the attacker might not be able to access the patient's body with malicious intent. Physical attacks can be launched via administering the medicine orally that contains maliciously programmed nanomachines or injecting malicious nanomachines into the patient's body. Moreover, the use of THz wave on the human skin can cause heat and effect the tissue of skin, therefore a communication and sensing standard should be maintained.

### 2) BIO CYBER INTERFACE CHALLENGES

Despite having made tremendous research, wearable bioelectronic devices face challenges in the way of wide acceptance and adoption. There are just a few examples of fully functional, successfully deployed and FDA (Food and Drug Administration) approved bio-electronic devices found in the literature. Some proposals are demonstrated through theoretical models, models of some devices are being simulated and some are under clinical trials. The research in these devices needs collaborations between university research teams, clinical organizations, community health service providers, small companies emerging with specific technology offerings, and large worldwide corporations interested to influence their existing technologies into new market offerings. This section provides challenges and their possible solutions towards the overall challenges in IoBNT domain and its security. Main goal of bio cyber interface is to accurately read and convert chemical and biological processes from inside body into electrical signals. For this goal, possible solutions might be found in chemical, physical and biological sensors which promise unprecedented sensing abilities. Therefore, for biologically inspired bio cyber interfaces challenges like ligand-receptor selection, realistic ICT-based modeling of artificial structures and, biological circuits complexity must be addressed. Moreover, these devices are intended to operate directly in contact with the epidermal biological environment. The issues of biocompatibility, biodegradability, stretch ability, and befouling must be taken into account while designing these devices. When these devices are implanted the body may perceive it as a foreign agent and biological plaque starts building up around the sensor device, which causes degradation of sensor performance. Therefore, bio-inspired approaches and material must be considered while designing these devices. Enhancing comfort while minimizing the size of the device will increase the likelihood of device adoption. Flexible materials based on CNT [207], [208] and graphene [209], [210] are constantly being investigated for the fabrication of these devices. Electronic tattoos are body-compliant wearable devices that combine an attractive performance of electrochemical devices with a favorable substrate-skin elasticity of temporary tattoos and resistance to mechanical stress. The realization of these electronic tattoos and their integration with a domain like IoBNT will open up a plethora of applications in the healthcare domain. The currently developed electronic tattoos are able to withstand strain and deformations without deteriorating the device performance. The tattoos are used temporarily as compared to other counterpart bio-electronic devices; hence leaching reagents (i.e., detaching from its carrier) is not a critical issue. However to use these electronic tattoos for long term use issues like leaching reagents, need for re-calibration, effects of washing and increased stretch ability for wearers comfort must be revisited and addressed. The devices currently manufactured are tested rigorously to withstand mechanical deformation caused by external strain. However, in cases of long term use and extreme physical stress conditions, the device abilities might be degraded. To counter this deformation effect, self-healing [211]–[213] devices are being manufactured [214] that utilize healing agents encapsulated in microcapsules [215]. The healing agents quickly dissolve the crack in the device by filling it with agents like hexyl acetate. Summing up, the interface design encompasses expertise from the different disciplines such as wireless communication, physics, biology and optogenetics. Moreover, there is a need to take a step ahead from theoretical research and computer simulations towards experimental research. Wet labs are currently not available or ae extremely costly to perform experimental validation of healthcare applications of IoBNT.

### 3) BIG DATA ANALYTICS

Realization of Internet of Bio-Nano Things leads to the interconnection of millions of devices from nano to macro scale. The interconnection of these devices means the generation of big data in large volume, velocity, and variety [216]. Efficient monitoring and diagnostic in IoBNT critically depend upon the quality of collected sensory data and management of this big data is important to obtain clean data for further analysis. Currently, bio-electronics are being developed using divergent technology, equipment, and services. This diversity of technology yields in data generation of having diverse formats and transfer protocols. A unified solution is needed which provides some standard for light data formats and protocols for better efficiency of real-time health monitoring applications [217]. Another issue with an increased amount of data is increased noisy data and erroneous and missing values. This bad quality of data affects performance analytics and may lead to incorrect findings. New data validation and big data analytics algorithms are the need of time to improve the quality of raw data.

Data aggregation of intra-body nanosensors and data collected from subsequent smart hops is also an issue. New rules

**TABLE 8.** Summarization of challenges in Internet of bio nano things.

| Area of Concentration | Brief Description | Research Initiatives |
|---|---|---|
| Nano Network Challanges | -Transmitter and Receiver Design<br>-Addressing in nanonetwork<br>-Powering Nanomachines<br>-Safety Challenges | -Stochastic simulations and experiments to validate the performance.<br>-Realistic ICT-based modeling of artificial structures.<br>-Function Centric Nano Networking(FCNN) based approach assigns addresses to functions and location of the body. |
| Bio Cyber Interface Challanges | -Need to accurately read and convert chemical and biological processes into chemical signals.<br>-Interdisciplinary research<br>-Experimental validation.<br>-Bio compatible design | -Exploration of potential materials and mechanisms for interfacing between nano,micro and macro communications Needs collaborations between university research teams(Wireless communication, physics, biotechnology disciplines), clinical organizations, community health service providers.<br>-Wet lab experiments<br>Use of biological materials to prevent biofouling and formation of plaque around the device surface. |
| Big Data Analytics | -Unavailability of realistic data for feature selection in ML algorithms.<br>-Data produced is in diverse formats and transfer protocols | -Use of deep learning techniques to automate feature selection<br>-A unified solution is needed which provides some standard for light data formats and protocols for better efficiency of real-time health monitoring applications |
| Security in IoBNT | -Compromise of devices and data<br>-Compromise of patient privacy and safety | -Design and validation procedures that address Confidentiality, Integrity, and Availability.<br>-Access control methods to limit unauthorized access. -newline -Development of novel security frameworks for resource constraint devices. |

of data aggregation are also needed to be developed to ensure smooth processing, sharing, and analysis of data. Early detection and prevention of disease can only be achieved when intelligent knowledge extraction techniques are applied to collected sensory big data. For real-time monitoring, bio-electronic devices must provide high data rates, which require powerful data storage and processing ability. Keeping in mind the small size of these devices, the above-mentioned capabilities cannot be implemented in these devices. Therefore researchers are exploring cloud-enabled integration [218], [219] with these devices to store and process raw sensory data in cloud platforms.

### B. CHALLENGES IN SECURITY OF IOBNT

The leverage to connect and control the human body through the internet not only opens up exciting IoBNT applications but also open up gateways for hackers to use the same with malicious intent. This event will pose a serious security threat to the patients termed as ''Bio cyber terrorism'' in [25]. Security is, therefore, the most important and critical challenge for the implementation and adoption of bio-electronic devices. Data generated by these devices is highly confidential as it reveals the most sensitive information of the patient. Hackers and adversaries can launch a number of attacks by misusing this data which can lead to fatal consequences. Data

tampering and alteration by the middle man (hacker) can lead to incorrect physiological values, which in turn results in an erroneous analysis of the patient's condition and flawed prescriptions from healthcare provider. The overall communication route from device to healthcare provider needs protection from security breaches down the way. Solutions to security issues of IoBNT cannot be found in existing mechanisms of traditional wireless networking. As the networking domain of IoBNT is itself novel and has diverse system requirements. The security mechanisms and access control [220] methods for IoBNT must be lightweight and compatible with resource-constrained [221] IoBNT devices and nanonetwork.

#### 1) CRYPTOGRAPHIC PRIMITIVES

As IoBNT deals with sensitive physiological parameters of patients, strong cryptographic mechanisms must be implemented to ensure user privacy. Considering the resource-constrained environment of IoBNT, symmetric and asymmetric cryptographic systems are computationally very expensive. The selection of a feasible cryptographic system for IoBNT depends upon the following characteristics of cryptosystems; Energy, memory and execution time. A novel field of bio-chemical cryptography has been proposed by Dressler and Kargl [222] which seems promising for nanonetworks. Biochemical cryptography techniques proposed so far use DNA molecules for encryption. There a number of proposals using DNA cryptography as an encryption scheme [223]–[230].

#### 2) AUTHENTICATION

Authentication and access control schemes might not be possible for intra body nanonetworks. However, the source of data and messages communicated to the gateway devices must be authenticated before forwarding to intra body nanonetworks.

Nano communication mediums i.e., MC, nanoelectromagnetic communication, and nano-acoustic communication should be considered separately when designing authentication schemes. An authentication scheme for nano-electromagnetic communication has been proposed [184] recently which exploits distance-dependent path loss as a device fingerprint to discriminate the data sent by legitimate transmitter and intruder. In the case of MC, this authentication scheme might not be feasible due to underlying communication differences. For MC the emerging field of biochemical cryptography [222] i.e., the use of biological molecules such as DNA and Ribonucleic Acid (RNA) as a source of encryption might be explored to solve authentication problems of molecular communications at nano-scale. However, it comes with entirely new challenges for the researchers and collaboration of biologists, computer scientists and biochemists might be required for investigation innovative ways [28].

#### 3) ENCRYPTION

Key management is still a major challenge in nanonetworks whether it be pre-distribution before network deployment or pro-active distribution before data transmission. Both the schemes have their drawbacks at the nano-scale,

**TABLE 9. Summary of notations.**

| Abbr. | Full Form |
|---|---|
| AIS | Artificial Immune System |
| ATP | Adenosine Triphosphate |
| BAN | Body Area Network |
| BFC | Biofuel Cell |
| BRET | Bioluminescence Resonance Energy Transfer |
| CHD | Coronary Heart Disease |
| CNT | Carbon Nano Tubes |
| CPS | Cyber Physical System |
| DbMC | Diffusion Based Molecular Communication |
| DES | Drug Eluting Stents |
| DNA | Deoxyribonucleic Acid |
| DoS | Denial of Service |
| ECC | Elliptic Curve Cryptography |
| EM | Electromagnetic Communication |
| FES | Functional Electric Stimulations |
| FET | Field Effect Transistor |
| FRET | Fluorescence Resonance Energy Transfer |
| HIS | Human Immune System |
| IC | Integrated Circuit |
| ICT | Information and Communication Technology |
| IMD | Implantable Medical Device |
| IoBNT | Internet of Bio Nano Things |
| IoMt | Internet of Medical Things |
| IoNT | Internet of Nano Things |
| IoT | Internet of Things |
| L | Luciferin |
| LU | Luciferase |
| MICS | Medical Implant Communications Service |
| MITM | Man-In-The-Middle |
| MC | Molecular Communication |
| NFC | Near-Field-Communication |
| OSI | Open Systems Interconnection |
| PDA | Personal Digital Assistant |
| RFID | Radio-frequency IDentification |
| Rx | Reciever |
| SIR | Susceptible, Infected,Recovered |
| SPR | Surface Plasmon Resonance |
| SVM | Support Vector Machine |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TDD | Targeted Drug Delivery |
| THz | Tera Hertz |
| Tx | Transmitter |
| WBAN | Wireless Body Area Network |
| WCS | Wireless Chemical Sensor |

pre-distribution is not feasible as storing a large number of pairwise keys is not possible considering the limited storage capacity of nano-devices. Pro-active or on demand key distribution needs online access to the devices, which are not feasible *in-vivo* nanonetwork applications where online access to nanonetwork is limited.

Some researchers have proposed ECC (Elliptic Curve Cryptography) [231]–[233] for resource-constrained devices, but in real-time ECC based primitives are still expensive in terms of time complexity. Moreover, quantum based cryptographic algorithms in resource constrained devices have proven to efficient [234]. In nanocommunication networks, the use of public-key cryptography is not very realistic due to the very high resource limitations, however biochemical cryptography [222] or DNA cryptography [227] might be potentially suitable cryptography mechanisms at the nano-scale.

Bio-inspired algorithms are now being adopted for computing and networking problems, which work on the principle of nature-inspired solutions [235], [236]. Bio-inspired computing is a research field that finds principles of problem-solving in nature and maps them into algorithms for computing domain. A subclass of this domain is bio-inspired algorithms for security, which provides algorithms involving techniques adopted by nature to defend against intruders [237], [238]. The most popular natural defense system is the human immune system, which fights against intruders and external viruses to prevent them from entering the body. In this direction, some proposals have been presented to improve cyber security in the field of wireless sensor networks. Bio-inspired algorithms such as Artificial Immune System (AIS) [239], Genetic mutation [240] and Ant Colony Optimization (ACO) [241] are utilized to mitigate against certain cyber-attacks.

The bio-inspired algorithms are a promising novel security approach that is scalable and robust and provides plenty of algorithms that can be adopted to mitigate against attacks in IoBNT. One of the goals for future work is to use bio-inspired algorithms to provide security solutions for IoBNT.

## VIII. CONCLUSION

IoBNT is an emerging research domain that holds significant promises in various healthcare applications. These applications range from early symptom detection to remote diagnosis to treatments of patients (e.g., via targeted drug delivery), and so on. The design and integration of device components are dependent on individual IoBNT deployment requirements and settings (e.g., in sensing applications, relevant sensors must be integrated to sense individual biochemical substances like pH, sodium, and calcium). However, there are a number of challenges such as those identified and discussed in this paper and the challenges moving forward are interdisciplinary (e.g., physics, chemical engineering, biology, mechanical engineering, and computer science). In addition to these challenges, this research highlights prospective research avenues for future researchers as well as IoBNT hardware and software designers and engineers.

The field of security in to IoBNT technologies is not yet mature, generating opportunities for attackers, even non-sophisticated attacks can have a significant impact on both IoBNT technologies and users' safety. There is a current opportunity for standardization initiatives to unify IoBNT in terms of information security. The well established fields like IoT, WBANs and IMDs have been helpful in identifying attack types in IoBNT. Apart from software and hardware security mechanisms, there is a need for user's training and awareness for wide adoption of these novel technologies. One of the future plans is to build and implement systems that can detect and mitigate security attacks affecting the theragnostics process in real time.

## ACKNOWLEDGMENT

This research work is intended to be included in the Ph.D. thesis of Sidra Zafar, supervised by Dr. Mohsin Nazir and Dr. Aneeqa Sabah. The authors would like to thank all the other coauthors for their contributions in this research work.

## REFERENCES

[1] E. B. Steager, M. S. Sakar, C. Magee, M. Kennedy, A. Cowley, and V. Kumar, "Automated biomanipulation of single cells using magnetic microrobots," *Int. J. Robot. Res.*, vol. 32, no. 3, pp. 346–359, Mar. 2013.

[2] D.-H. Kim, P. K. Wong, J. Park, A. Levchenko, and Y. Sun, "Microengineered platforms for cell mechanobiology," *Annu. Rev. Biomed. Eng.*, vol. 11, no. 1, pp. 203–233, Aug. 2009.

[3] O. Ergeneman, G. Dogangil, M. P. Kummer, J. J. Abbott, M. K. Nazeeruddin, and B. J. Nelson, "A magnetically controlled wireless optical oxygen sensor for intraocular measurements," *IEEE Sensors J.*, vol. 8, no. 1, pp. 29–37, Jan. 2008.

[4] T. Nakamura and A. Terano, "Capsule endoscopy: Past, present, and future," *J. Gastroenterol.*, vol. 43, no. 2, pp. 93–99, Feb. 2008.

[5] J. M. Dubach, D. I. Harjes, and H. A. Clark, "Fluorescent ion-selective nanosensors for intracellular analysis with improved lifetime and size," *Nano Lett.*, vol. 7, no. 6, pp. 1827–1831, Jun. 2007.

[6] C.-J. Chen, Y. Haik, and J. Chatterjee, "Development of nanotechnology for biomedical applications," in *Proc. Conf., Emerg. Inf. Technol.* Taipei, Taiwan: IEEE, 2005, pp. 1–4.

[7] R. W. Carlsen and M. Sitti, "Bio-hybrid cell-based actuators for microsystems," *Small*, vol. 10, no. 19, pp. 3831–3851, Oct. 2014.

[8] J. W. Aylott, "Optical nanosensors—An enabling technology for intracellular measurements," *Analyst*, vol. 128, no. 4, pp. 309–312, 2003.

[9] B. P. Timko, T. Dvir, and D. S. Kohane, "Remotely triggerable drug delivery systems," *Adv. Mater.*, vol. 22, no. 44, pp. 4925–4943, Nov. 2010.

[10] G. Pan and L. Wang, "Swallowable wireless capsule endoscopy: Progress and technical challenges," *Gastroenterol. Res. Pract.*, vol. 2012, Oct. 2011, Art. no. 841691.

[11] R. Fernández-Pacheco, C. Marquina, J. G. Valdivia, M. Gutiérrez, M. S. Romero, R. Cornudella, A. Laborda, A. Viloria, T. Higuera, A. García, J. A. G. de Jalón, and M. R. Ibarra, "Magnetic nanoparticles for local drug delivery using magnetic implants," *J. Magn. Magn. Mater.*, vol. 311, no. 1, pp. 318–322, Apr. 2007.

[12] Z. Liao, R. Gao, C. Xu, and Z.-S. Li, "Indications and detection, completion, and retention rates of small-bowel capsule endoscopy: A systematic review," *Gastrointestinal Endoscopy*, vol. 71, no. 2, pp. 280–286, Feb. 2010.

[13] J. Li, T. Peng, and Y. Peng, "A cholesterol biosensor based on entrapment of cholesterol oxidase in a silicic sol-gel matrix at a Prussian blue modified electrode," *Electroanalysis*, vol. 15, no. 12, pp. 1031–1037, Jul. 2003.

[14] T. Kawahara, M. Sugita, M. Hagiwara, F. Arai, H. Kawano, I. Shihira-Ishikawa, and A. Miyawaki, "On-chip microrobot for investigating the response of aquatic microorganisms to mechanical stimulation," *Lab Chip*, vol. 13, no. 6, pp. 1070–1078, 2013.

[15] M. Fluckiger and B. J. Nelson, "Ultrasound emitter localization in heterogeneous media," in *Proc. 29th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Aug. 2007, pp. 2867–2870.
[16] R. A. Freitas, "Pharmacytes: An ideal vehicle for targeted drug delivery," *J. Nanoscience Nanotechnol.*, vol. 6, nos. 9–10, pp. 2769–2775, Sep. 2006.
[17] I. F. Akyildiz, F. Brunetti, and C. Blázquez, "Nanonetworks: A new communication paradigm," *Comput. Netw.*, vol. 52, no. 12, pp. 2260–2279, Aug. 2008.
[18] J. L. Marzo, J. M. Jornet, and M. Pierobon, "Nanonetworks in biomedical applications," *Current Drug Targets*, vol. 20, no. 8, pp. 800–807, May 2019.
[19] L. Felicetti, M. Femminella, G. Reali, T. Nakano, and A. V. Vasilakos, "TCP-like molecular communications," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 12, pp. 2354–2367, Dec. 2014.
[20] T. Nakano, M. J. Moore, F. Wei, A. V. Vasilakos, and J. Shuai, "Molecular communication and networking: Opportunities and challenges," *IEEE Trans. Nanobiosci.*, vol. 11, no. 2, pp. 135–148, Jun. 2012.
[21] I. F. Akyildiz and J. M. Jornet, "Electromagnetic wireless nanosensor networks," *Nano Commun. Netw.*, vol. 1, no. 1, pp. 3–19, Mar. 2010.
[22] I. F. Akyildiz and J. M. Jornet, "The Internet of nano-things," *IEEE Wireless Commun.*, vol. 17, no. 6, pp. 58–63, Dec. 2010.
[23] E. Velloso, D. Cardador, K. Vega, W. Ugulino, A. Bulling, H. Gellersen, and H. Fuks, "The Web of Things as an infrastructure for improving users' health and wellbeing," in *Proc. 2nd Workshop Brazilian Inst. Web Sci. Res.*, Rio de Janeiro, Brazil, 2011, pp. 1–7.
[24] F. Michel and M. Folcher, "Optogenerapy: When bio-electronic implant enters the modern syringe era," *Porto Biomed. J.*, vol. 2, no. 5, pp. 145–149, 2017.
[25] I. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, "The Internet of bio-nano things," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 32–40, Mar. 2015.
[26] R. Kirichek, R. Pirmagomedov, R. Glushakov, and A. Koucheryavy, "Live substance in cyberspace—Biodriver system," in *Proc. 18th Int. Conf. Adv. Commun. Technol. (ICACT)*. Pyeongchang, South Korea: IEEE, 2016, pp. 274–278.
[27] P. Kulakowski, K. Turbic, and L. M. Correia, "From nano-communications to body area networks: A perspective on truly personal communications," *IEEE Access*, vol. 8, pp. 159839–159853, 2020.
[28] M. Usman, M. R. Asghar, I. S. Ansari, and M. Qaraqe, "Security in wireless body area networks: From in-body to off-body communications," *IEEE Access*, vol. 6, pp. 58064–58074, 2018.
[29] V. Loscri, C. Marchal, N. Mitton, G. Fortino, and A. V. Vasilakos, "Security and privacy in molecular communication and networking: Opportunities and challenges," *IEEE Trans. Nanobiosci.*, vol. 13, no. 3, pp. 198–207, Sep. 2014.
[30] K. Yang, D. Bi, Y. Deng, R. Zhang, M. M. Ur Rahman, N. A. Ali, M. A. Imran, J. M. Jornet, Q. H. Abbasi, and A. Alomainy, "A comprehensive survey on hybrid communication for Internet of nano-things in context of body-centric communications," 2019, *arXiv:1912.09424*. [Online]. Available: http://arxiv.org/abs/1912.09424
[31] F. Al-Turjman, "Intelligence and security in big 5G-oriented IoNT: An overview," *Future Gener. Comput. Syst.*, vol. 102, pp. 357–368, Jan. 2020.
[32] I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: The future of wireless communications systems," *IEEE Access*, vol. 8, pp. 133995–134030, 2020.
[33] A. F. Silva and M. Tavakoli, "Domiciliary hospitalization through wearable biomonitoring patches: Recent advances, technical challenges, and the relation to covid-19," *Sensors*, vol. 20, no. 23, p. 6835, Nov. 2020.
[34] N. X. Williams and A. D. Franklin, "Electronic tattoos: A promising approach to real-time theragnostics," *J. Dermatology Skin Sci.*, vol. 2, no. 1, pp. 5–16, 2020.
[35] J. Y. Oh and Z. Bao, "Second skin enabled by advanced electronics," *Adv. Sci.*, vol. 6, no. 11, Jun. 2019, Art. no. 1900186.
[36] P. Kassal, I. M. Steinberg, and M. D. Steinberg, "Wireless smart tag with potentiometric input for ultra low-power chemical sensing," *Sens. Actuators B, Chem.*, vol. 184, pp. 254–259, Jul. 2013.
[37] P. Kassal, M. D. Steinberg, and I. M. Steinberg, "Wireless chemical sensors and biosensors: A review," *Sens. Actuators B, Chem.*, vol. 266, pp. 228–245, Aug. 2018.
[38] R. Singh, E. Singh, and H. S. Nalwa, "Inkjet printed nanomaterial based flexible radio frequency identification (RFID) tag sensors for the Internet of nano things," *RSC Adv.*, vol. 7, no. 77, pp. 48597–48630, 2017.
[39] A. J. Bandodkar, W. Jia, and J. Wang, "Tattoo-based wearable electrochemical devices: A review," *Electroanalysis*, vol. 27, no. 3, pp. 562–572, Mar. 2015.
[40] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare Internet of Things: A survey of emerging technologies," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1121–1167, 2nd Quart., 2020.
[41] P. K. D. Pramanik, A. Solanki, A. Debnath, A. Nayyar, S. El-Sappagh, and K.-S. Kwak, "Advancing modern healthcare with nanotechnology, nanobiosensors, and Internet of nano things: Taxonomies, applications, architecture, and challenges," *IEEE Access*, vol. 8, pp. 65230–65266, 2020.
[42] S. López Bernal, A. Huertas Celdrán, G. M. Pérez, M. T. Barros, and S. Balasubramaniam, "Security in brain-computer interfaces: State-of-the-art, opportunities, and future challenges," 2019, *arXiv:1908.03536*. [Online]. Available: http://arxiv.org/abs/1908.03536
[43] M. B. Dissanayake and N. Ekanayake, "On the exact performance analysis of molecular communication via diffusion for Internet of bio-nano things," *IEEE Trans. Nanobiosci.*, early access, Apr. 9, 2021, doi: 10.1109/TNB.2021.3072230.
[44] F. Al-Turjman, "A cognitive routing protocol for bio-inspired networking in the Internet of nano-things (IoNT)," *Mobile Netw. Appl.*, vol. 25, pp. 1929–1943, Oct. 2017.
[45] C. Roman, F. Ciontu, and B. Courtois, "Single molecule detection and macromolecular weighting using an all-carbon-nanotube nanoelectromechanical sensor," in *Proc. 4th IEEE Conf. Nanotechnol.*, Aug. 2004, pp. 263–266.
[46] F. Schedin, A. K. Geim, S. V. Morozov, E. W. Hill, P. Blake, M. I. Katsnelson, and K. S. Novoselov, "Detection of individual gas molecules adsorbed on graphene," *Nature Mater.*, vol. 6, no. 9, pp. 652–655, Sep. 2007.
[47] P. Tallury, A. Malhotra, L. M. Byrne, and S. Santra, "Nanobioimaging and sensing of infectious diseases," *Adv. Drug Del. Rev.*, vol. 62, nos. 4–5, pp. 424–437, Mar. 2010.
[48] H.-Y. Yeh, M. V. Yates, W. Chen, and A. Mulchandani, "Real-time molecular methods to detect infectious viruses," in *Seminars in Cell & Developmental Biology*, vol. 20. Amsterdam, The Netherlands: Elsevier, 2009, pp. 49–54.
[49] F. Büther, F.-L. Lau, M. Stelzner, and S. Ebers, "A formal definition for nanorobots and nanonetworks," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems* St. Petersburg, Russia: Springer, 2017, pp. 214–226.
[50] L. F. C. Pereira and M. S. Ferreira, "Electronic transport on carbon nanotube networks: A multiscale computational approach," *Nano Commun. Netw.*, vol. 2, no. 1, pp. 25–38, Mar. 2011.
[51] J.-W. Yoo, D. J. Irvine, D. E. Discher, and S. Mitragotri, "Bio-inspired, bioengineered and biomimetic drug delivery carriers," *Nature Rev. Drug Discovery*, vol. 10, no. 7, pp. 521–535, Jul. 2011.
[52] Y. Nishimura, J. Ishii, C. Ogino, and A. Kondo, "Genetic engineering of bio-nanoparticles for drug delivery: A review," *J. Biomed. Nanotechnol.*, vol. 10, no. 9, pp. 2063–2085, Sep. 2014.
[53] S. Tan, T. Wu, D. Zhang, and Z. Zhang, "Cell or cell membrane-based drug delivery systems," *Theranostics*, vol. 5, no. 8, p. 863, 2015.
[54] D. Lockney, S. Franzen, and S. Lommel, "Viruses as nanomaterials for drug delivery," in *Biomedical Nanotechnology*. Berlin, Germany: Springer, 2011, pp. 207–221.
[55] N. Esfandiari, M. K. Arzanani, M. Soleimani, M. Kohi-Habibi, and W. E. Svendsen, "A new application of plant virus nanoparticles as drug delivery in breast cancer," *Tumor Biol.*, vol. 37, no. 1, pp. 1229–1236, Jan. 2016.
[56] L. Steidler, "Live genetically modified bacteria as drug delivery tools: At the doorstep of a new pharmacology?" *Expert Opinion Biol. Therapy*, vol. 4, no. 4, pp. 439–441, 2004.
[57] I. Yacoby, H. Bar, and I. Benhar, "Targeted drug-carrying bacteriophages as antibacterial nanomedicines," *Antimicrobial Agents Chemotherapy*, vol. 51, no. 6, pp. 2156–2163, Jun. 2007.
[58] E. V. Batrakova, H. E. Gendelman, and A. V. Kabanov, "Cell-mediated drug delivery," *Expert Opinion Drug Del.*, vol. 8, no. 4, pp. 415–433, Apr. 2011.

[59] Y. Su, Z. Xie, G. B. Kim, C. Dong, and J. Yang, "Design strategies and applications of circulating cell-mediated drug delivery systems," *ACS Biomaterials Sci. Eng.*, vol. 1, no. 4, pp. 201–217, Apr. 2015.

[60] G. Strobel and J. Mittnacht, "Richard, are we there yet?—An Internet of nano things information system architecture," in *Proc. 54th Hawaii Int. Conf. Syst. Sci.*, 2021, p. 4578.

[61] Y. Koucheryavy, A. Yastrebova, D. P. Martins, and S. Balasubramaniam, "A review on bio-cyber interfaces for intrabody molecular communications systems," 2021, *arXiv:2104.14944*. [Online]. Available: http://arxiv.org/abs/2104.14944

[62] P. Kassal, M. Zubak, G. Scheipl, G. J. Mohr, M. D. Steinberg, and I. M. Steinberg, "Smart bandage with wireless connectivity for optical monitoring of pH," *Sens. Actuators B, Chem.*, vol. 246, pp. 455–460, Jul. 2017.

[63] U. A. K. Chude-Okonkwo, R. Malekian, and B. T. Maharaj, "Biologically inspired bio-cyber interface architecture and model for Internet of bio-NanoThings applications," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3444–3455, Aug. 2016.

[64] T. Nakano, S. Kobayashi, T. Suda, Y. Okaie, Y. Hiraoka, and T. Haraguchi, "Externally controllable molecular communication," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 12, pp. 2417–2431, Dec. 2014.

[65] Q. Hu, P. S. Katti, and Z. Gu, "Enzyme-responsive nanomaterials for controlled drug delivery," *Nanoscale*, vol. 6, no. 21, pp. 12273–12286, 2014.

[66] Y. I. Wu, D. Frey, O. I. Lungu, A. Jaehrig, I. Schlichting, B. Kuhlman, and K. M. Hahn, "A genetically encoded photoactivatable rac controls the motility of living cells," *Nature*, vol. 461, no. 7260, pp. 104–108, Sep. 2009.

[67] G. C. R. Ellis-Davies, "Caged compounds: Photorelease technology for control of cellular chemistry and physiology," *Nature Methods*, vol. 4, no. 8, pp. 619–628, Aug. 2007.

[68] L. Dykman and N. Khlebtsov, "Gold nanoparticles in biomedical applications: Recent advances and perspectives," *Chem. Soc. Rev.*, vol. 41, no. 6, pp. 2256–2282, 2012.

[69] D. Needham, G. Anyarambhatla, G. Kong, and M. W. Dewhirst, "A new temperature-sensitive liposome for use with mild hyperthermia: Characterization and testing in a human tumor xenograft model," *Cancer Res.*, vol. 60, no. 5, pp. 1197–1201, 2000.

[70] B. M. Dicheva, T. L. M. T. Hagen, L. Li, D. Schipper, A. L. B. Seynhaeve, G. C. V. Rhoon, A. M. M. Eggermont, L. H. Lindner, and G. A. Koning, "Cationic thermosensitive liposomes: A novel dual targeted heat-triggered drug delivery approach for endothelial and tumor cells," *Nano Lett.*, vol. 13, no. 6, pp. 2324–2331, Jun. 2013.

[71] K. Kono, T. Miyoshi, Y. Haba, E. Murakami, C. Kojima, and A. Harada, "Temperature sensitivity control of alkylamide-terminated poly (amidoamine) dendrimers induced by guest molecule binding," *J. Amer. Chem. Soc.*, vol. 129, no. 23, pp. 7222–7223, 2007.

[72] K. Hamad-Schifferli, J. J. Schwartz, A. T. Santos, S. Zhang, and J. M. Jacobson, "Remote electronic control of DNA hybridization through inductive coupling to an attached metal nanocrystal antenna," *Nature*, vol. 415, no. 6868, pp. 152–155, Jan. 2002.

[73] N. A. Abbasi and O. B. Akan, "An information theoretical analysis of human insulin-glucose system toward the Internet of bio-nano things," *IEEE Trans. Nanobiosci.*, vol. 16, no. 8, pp. 783–791, Dec. 2017.

[74] T. Nakano, T. Suda, Y. Okaie, M. J. Moore, and A. V. Vasilakos, "Molecular communication among biological nanomachines: A layered architecture and research issues," *IEEE Trans. Nanobiosci.*, vol. 13, no. 3, pp. 169–197, Sep. 2014.

[75] H. K. Rudsari, M. R. Javan, M. Orooji, N. Mokari, and E. A. Jorswieck, "TDMA-MTMR-based molecular communication with ligand-binding reception," *IEEE Trans. Mol., Biol. Multi-Scale Commun.*, early access, Jan. 27, 2021, doi: 10.1109/TMBMC.2021.3054902.

[76] N. Farsad, H. B. Yilmaz, A. Eckford, C.-B. Chae, and W. Guo, "A comprehensive survey of recent advancements in molecular communication," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1887–1919, 3rd Quart., 2016.

[77] M. Kuscu, E. Dinc, B. A. Bilgin, H. Ramezani, and O. B. Akan, "Transmitter and receiver architectures for molecular communications: A survey on physical design with modulation, coding, and detection techniques," *Proc. IEEE*, vol. 107, no. 7, pp. 1302–1341, Jul. 2019.

[78] M. Kuscu and O. B. Akan, "Modeling and analysis of SiNW FET-based molecular communication receiver," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3708–3721, Sep. 2016.

[79] M. Kuscu and O. B. Akan, "On the physical design of molecular communication receiver based on nanoscale biosensors," *IEEE Sensors J.*, vol. 16, no. 8, pp. 2228–2243, Apr. 2016.

[80] N.-R. Kim and C.-B. Chae, "Novel modulation techniques using isomers as messenger molecules for nano communication networks via diffusion," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 12, pp. 847–856, Dec. 2013.

[81] M. S. Kuran, H. B. Yilmaz, T. Tugcu, and B. Özerman, "Energy model for communication via diffusion in nanonetworks," *Nano Commun. Netw.*, vol. 1, no. 2, pp. 86–95, Jun. 2010.

[82] N. Garralda, I. Llatser, A. Cabellos-Aparicio, E. Alarcón, and M. Pierobon, "Diffusion-based physical channel identification in molecular nanonetworks," *Nano Commun. Netw.*, vol. 2, no. 4, pp. 196–204, Dec. 2011.

[83] M. S. Kuran, H. B. Yilmaz, T. Tugcu, and I. F. Akyildiz, "Modulation techniques for communication via diffusion in nanonetworks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2011, pp. 1–5.

[84] N. Farsad, N.-R. Kim, A. W. Eckford, and C.-B. Chae, "Channel and noise models for nonlinear molecular communication systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 12, pp. 2392–2401, Dec. 2014.

[85] I. Llatser, I. Pascual, N. Garralda, A. Cabellos-Aparicio, M. Pierobon, E. Alarcon, and J. Sole-Pareta, "Exploring the physical channel of diffusion-based molecular communication by simulation," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Houston, TX, USA, USA: IEEE, Dec. 2011, pp. 1–5.

[86] C. T. Chou, "Extended master equation models for molecular communication networks," *IEEE Trans. Nanobiosci.*, vol. 12, no. 2, pp. 79–92, Jun. 2013.

[87] A. Noel, K. C. Cheung, and R. Schober, "Improving receiver performance of diffusive molecular communication with enzymes," *IEEE Trans. Nanobiosci.*, vol. 13, no. 1, pp. 31–43, Mar. 2014.

[88] M. Pierobon and I. Akyildiz, "A physical end-to-end model for molecular communication in nanonetworks," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 4, pp. 602–611, May 2010.

[89] L. Felicetti, M. Femminella, G. Reali, and P. Liò, "Applications of molecular communications to medicine: A survey," *Nano Commun. Netw.*, vol. 7, pp. 27–45, Mar. 2016.

[90] U. A. K. Chude-Okonkwo, R. Malekian, B. T. Maharaj, and A. V. Vasilakos, "Molecular communication and nanonetwork for targeted drug delivery: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 3046–3096, 2017.

[91] U. A. K. Chude-Okonkwo, R. Malekian, and B. T. S. Maharaj, "Molecular communication model for targeted drug delivery in multiple disease sites with diversely expressed enzymes," *IEEE Trans. Nanobiosci.*, vol. 15, no. 3, pp. 230–245, Apr. 2016.

[92] U. Chude-Okonkwo, R. Malekian, and B. Maharaj, "Nanosystems and devices for advanced targeted nanomedical applications," in *Advanced Targeted Nanomedicine*. Berlin, Germany: Springer, 2019, pp. 39–58.

[93] Y. Chahibi, I. F. Akyildiz, and S. O. Song, "Antibody-based molecular communication for targeted drug delivery systems," in *Proc. 36th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Chicago, IL, USA: IEEE, Aug. 2014, pp. 5707–5710.

[94] Y. Chahibi and I. F. Akyildiz, "Molecular communication noise and capacity analysis for particulate drug delivery systems," *IEEE Trans. Commun.*, vol. 62, no. 11, pp. 3891–3903, Nov. 2014.

[95] Y. Chahibi, I. F. Akyildiz, S. Balasubramaniam, and Y. Koucheryavy, "Molecular communication modeling of antibody-mediated drug delivery systems," *IEEE Trans. Biomed. Eng.*, vol. 62, no. 7, pp. 1683–1695, Jul. 2015.

[96] Y. Chahibi, M. Pierobon, and I. F. Akyildiz, "Pharmacokinetic modeling and biodistribution estimation through the molecular communication paradigm," *IEEE Trans. Biomed. Eng.*, vol. 62, no. 10, pp. 2410–2420, Oct. 2015.

[97] G. Piro, K. Yang, G. Boggia, N. Chopra, L. A. Grieco, and A. Alomainy, "Terahertz communications in human tissues at the nanoscale for healthcare applications," *IEEE Trans. Nanotechnol.*, vol. 14, no. 3, pp. 404–406, May 2015.

[98] J. M. Jornet and I. F. Akyildiz, "Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3211–3221, Oct. 2011.

[99] Q. H. Abbasi, K. Yang, N. Chopra, J. M. Jornet, N. A. Abuali, K. A. Qaraqe, and A. Alomainy, "Nano-communication for biomedical applications: A review on the state-of-the-art from physical layers to novel networking concepts," *IEEE Access*, vol. 4, pp. 3920–3935, 2016.

[100] D. Zhang and Q. Liu, "Biosensors and bioelectronics on smartphone for portable biochemical detection," *Biosensors Bioelectron.*, vol. 75, pp. 273–284, Jan. 2016.
[101] S. Movassaghi, P. Arab, and M. Abolhasan, "Wireless technologies for body area networks: Characteristics and challenges," in *Proc. Int. Symp. Commun. Inf. Technol. (ISCIT)*. Gold Coast, QLD, Australia: IEEE, Oct. 2012, pp. 42–47.
[102] H. H. Strey, P. Richman, R. Rozensky, S. Smith, and L. Endee, "Bluetooth low energy technologies for applications in health care: Proximity and physiological signals monitors," in *Proc. 10th Int. Conf. Expo Emerg. Technol. Smarter World (CEWIT)*. Melville, NY, USA: IEEE, Oct. 2013, pp. 1–4.
[103] E. Georgakakis, S. A. Nikolidakis, D. D. Vergados, and C. Douligeris, "An analysis of Bluetooth, zigbee and Bluetooth low energy and their use in WBANs," in *Proc. Int. Conf. Wireless Mobile Commun. Healthcare*. Berlin, Germany: Springer, 2010, pp. 168–175.
[104] H. Cao, V. Leung, C. Chow, and H. Chan, "Enabling technologies for wireless body area networks: A survey and outlook," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 84–93, Dec. 2009.
[105] J. H. Kurunathan, "Study and overview on WBAN under IEEE 802.15.6," *U. Porto J. Eng.*, vol. 1, no. 1, pp. 11–21, Sep. 2017.
[106] I. W. Group, *IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements—Part 11: Wireless Lan Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*, IEEE Standard TR 11, 2010.
[107] D. Lewis, "IEEE p802.15.6/d0 draft standard for body area network (vol. 6)," IEEE, Piscataway, NJ, USA, Tech. Rep. IEEE P802.15-08-0780-12-0006, 2010.
[108] A. Mile, G. Okeyo, and A. Kibe, "Hybrid IEEE 802.15.6 wireless body area networks interference Mitigation model for high mobility interference scenarios," *Wireless Eng. Technol.*, vol. 9, no. 2, pp. 34–48, 2018.
[109] Z. Nie, Z. Li, R. Huang, Y. Liu, J. Li, and L. Wang, "A statistical frame based TDMA protocol for human body communication," *Biomed. Eng. OnLine*, vol. 14, no. 1, p. 65, Dec. 2015.
[110] S. Jena, A. Gupta, R. K. Pippara, and P. Pal, "Wireless sensing systems: A review," in *Sensors for Automotive and Aerospace Applications*. Berlin, Germany: Springer, 2019, pp. 143–192.
[111] J. Grosinger, "Feasibility of backscatter RFID systems on the human body," *EURASIP J. Embedded Syst.*, vol. 2013, no. 1, pp. 1–10, Dec. 2013.
[112] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, and M. Soljačić, "Wireless power transfer via strongly coupled magnetic resonances," *Science*, vol. 317, no. 5834, pp. 83–86, Jul. 2007.
[113] Y.-H. Lee, J.-S. Kim, J. Noh, I. Lee, H. J. Kim, S. Choi, J. Seo, S. Jeon, T.-S. Kim, J.-Y. Lee, and J. W. Choi, "Wearable textile battery rechargeable by solar energy," *Nano Lett.*, vol. 13, no. 11, pp. 5753–5761, Nov. 2013.
[114] J.-H. Lee, K. Y. Lee, M. K. Gupta, T. Y. Kim, D.-Y. Lee, J. Oh, C. Ryu, W. J. Yoo, C.-Y. Kang, S.-J. Yoon, J.-B. Yoo, and S.-W. Kim, "Highly stretchable piezoelectric-pyroelectric hybrid nanogenerator," *Adv. Mater.*, vol. 26, no. 5, pp. 765–769, Feb. 2014.
[115] J. Bae, M. K. Song, Y. J. Park, J. M. Kim, M. Liu, and Z. L. Wang, "Fiber supercapacitors made of nanowire-fiber hybrid structures for wearable/flexible energy storage," *Angew. Chem. Int. Ed.*, vol. 50, no. 7, pp. 1683–1687, Feb. 2011.
[116] P. P. Mercier, A. C. Lysaght, S. Bandyopadhyay, A. P. Chandrakasan, and K. M. Stankovic, "Energy extraction from the biologic battery in the inner ear," *Nature Biotechnol.*, vol. 30, no. 12, pp. 1240–1243, Dec. 2012.
[117] M. T. Meredith and S. D. Minteer, "Biofuel cells: Enhanced enzymatic bioelectrocatalysis," *Annu. Rev. Anal. Chem.*, vol. 5, no. 1, pp. 157–179, Jul. 2012.
[118] A. Zebda, C. Gondran, A. Le Goff, M. Holzinger, P. Cinquin, and S. Cosnier, "Mediatorless high-power glucose biofuel cells based on compressed carbon nanotube-enzyme electrodes," *Nature Commun.*, vol. 2, no. 1, pp. 1–6, Sep. 2011.
[119] L. Halámková, J. Halámek, V. Bocharova, A. Szczupak, L. Alfonta, and E. Katz, "Implanted biofuel cell operating in a living snail," *J. Amer. Chem. Soc.*, vol. 134, no. 11, pp. 5040–5043, Mar. 2012.
[120] W. Jia, G. Valdés-Ramírez, A. J. Bandodkar, J. R. Windmiller, and J. Wang, "Epidermal biofuel cells: Energy harvesting from human perspiration," *Angew. Chem. Int. Ed.*, vol. 52, no. 28, pp. 7233–7236, Jul. 2013.
[121] S. Canovas-Carrasco, A.-J. Garcia-Sanchez, and J. Garcia-Haro, "A nanoscale communication network scheme and energy model for a human hand scenario," *Nano Commun. Netw.*, vol. 15, pp. 17–27, Mar. 2018.
[122] S. Baik, H. J. Lee, D. W. Kim, J. W. Kim, Y. Lee, and C. Pang, "Bioinspired adhesive architectures: From skin patch to integrated bioelectronics," *Adv. Mater.*, vol. 31, no. 34, Aug. 2019, Art. no. 1803309.
[123] N. Islam and S. Misra, "'Catch the Pendulum': The problem of asymmetric data delivery in electromagnetic nanonetworks," *IEEE Trans. Nanobiosci.*, vol. 15, no. 6, pp. 576–584, Sep. 2016.
[124] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[125] A. J. Bandodkar, D. Molinnus, O. Mirza, T. Guinovart, J. R. Windmiller, G. Valdés-Ramírez, F. J. Andrade, M. J. Schöning, and J. Wang, "Epidermal tattoo potentiometric Sodium sensors with wireless signal transduction for continuous non-invasive sweat monitoring," *Biosensors Bioelectron.*, vol. 54, pp. 603–609, Apr. 2014.
[126] A. J. Bandodkar and J. Wang, "Non-invasive wearable electrochemical sensors: A review," *Trends Biotechnol.*, vol. 32, no. 7, pp. 363–371, Jul. 2014.
[127] E. K. Lee, M. K. Kim, and C. H. Lee, "Skin-mountable biosensors and therapeutics: A review," *Annu. Rev. Biomed. Eng.*, vol. 21, no. 1, pp. 299–323, Jun. 2019.
[128] H. Jin, Y. S. Abu-Raya, and H. Haick, "Advanced materials for health monitoring with skin-based wearable devices," *Adv. Healthcare Mater.*, vol. 6, no. 11, Jun. 2017, Art. no. 1700024.
[129] J. R. Windmiller, A. J. Bandodkar, G. Valdés-Ramírez, S. Parkhomovsky, A. G. Martinez, and J. Wang, "Electrochemical sensing based on printable temporary transfer tattoos," *Chem. Commun.*, vol. 48, no. 54, pp. 6794–6796, 2012.
[130] J. Di, S. Yao, Y. Ye, Z. Cui, J. Yu, T. K. Ghosh, Y. Zhu, and Z. Gu, "Stretch-triggered drug delivery from wearable elastomer films containing therapeutic depots," *ACS Nano*, vol. 9, no. 9, pp. 9407–9415, Sep. 2015.
[131] H. Jeong, T. Ha, I. Kuang, L. Shen, Z. Dai, N. Sun, and N. Lu, "NFC-enabled, tattoo-like stretchable biosensor manufactured by 'cut-and-paste' method," in *Proc. 39th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2017, pp. 4094–4097.
[132] H. Jeong and N. Lu, "Electronic tattoos: The most multifunctional but imperceptible wearables," in *Smart Biomedical and Physiological Sensor Technology XV*, vol. 11020. Bellingham, WA, USA: International Society for Optics and Photonics, 2019, Art. no. 110200P.
[133] H. Lee, C. Song, S. Baik, D. Kim, T. Hyeon, and D.-H. Kim, "Device-assisted transdermal drug delivery," *Adv. Drug Del. Rev.*, vol. 127, pp. 35–45, Mar. 2018.
[134] V. Hassija, V. Chamola, B. C. Bajpai, and S. Zeadally, "Security issues in implantable medical devices: Fact or fiction?" *Sustain. Cities Soc.*, vol. 66, Mar. 2021, Art. no. 102552.
[135] H. A. Abdul-Ghani and D. Konstantas, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective," *J. Sensor Actuator Netw.*, vol. 8, no. 2, p. 22, Apr. 2019.
[136] W. Jia, A. J. Bandodkar, G. Valdés-Ramírez, J. R. Windmiller, Z. Yang, J. Ramírez, G. Chan, and J. Wang, "Electrochemical tattoo biosensors for real-time noninvasive lactate monitoring in human perspiration," *Anal. Chem.*, vol. 85, no. 14, pp. 6553–6560, Jul. 2013.
[137] J. Kim, I. Jeerapan, S. Imani, T. N. Cho, A. Bandodkar, S. Cinti, P. P. Mercier, and J. Wang, "Noninvasive alcohol monitoring using a wearable tattoo-based iontophoretic-biosensing system," *ACS Sensors*, vol. 1, no. 8, pp. 1011–1019, Aug. 2016.
[138] N. Di Trani, A. Silvestri, G. Bruno, T. Geninatti, C. Y. X. Chua, A. Gilbert, G. Rizzo, C. S. Filgueira, D. Demarchi, and A. Grattoni, "Remotely controlled nanofluidic implantable platform for tunable drug delivery," *Lab Chip*, vol. 19, no. 13, pp. 2192–2204, 2019.
[139] R. Lodato and G. Marrocco, "Close integration of a UHF-RFID transponder into a limb prosthesis for tracking and sensing," *IEEE Sensors J.*, vol. 16, no. 6, pp. 1806–1813, Mar. 2016.
[140] K.-I. Chen, B.-R. Li, and Y.-T. Chen, "Silicon nanowire field-effect transistor-based biosensors for biomedical diagnosis and cellular recording investigation," *Nano Today*, vol. 6, no. 2, pp. 131–154, Apr. 2011.
[141] N. Kumar, K. Kaur, S. C. Misra, and R. Iqbal, "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud," *Peer Peer Netw. Appl.*, vol. 9, no. 5, pp. 824–840, Sep. 2016.

[142] J. Zhang, G. Tian, A. Marindra, A. Sunny, and A. Zhao, "A review of passive RFID tag antenna-based sensors and systems for structural health monitoring applications," *Sensors*, vol. 17, no. 2, p. 265, Jan. 2017.

[143] S. Kumar, G. Livermont, and G. McKewan, "Stage implementation of RFID in hospitals," *Technol. Health Care*, vol. 18, no. 1, pp. 31–46, Feb. 2010.

[144] A. Cangialosi, J. E. Monaly, and S. C. Yang, "Leveraging RFID in hospitals: Patient life cycle and mobility perspectives," *IEEE Commun. Mag.*, vol. 45, no. 9, pp. 18–23, Sep. 2007.

[145] A. Dey, B. S. Vijayaraman, and J. H. Choi, "RFID in US hospitals: An exploratory investigation of technology adoption," *Manage. Res. Rev.*, vol. 39, no. 4, pp. 399–424, Apr. 2016.

[146] A. A. A. Asaimi, M. I. Razzak, and R. Alshammari, "Developing ontology for RFID based infant protection system," *Adv. Sci. Lett.*, vol. 22, no. 10, pp. 2759–2763, Oct. 2016.

[147] R. P. Baptista, G. Morris, R. Jones, N. Ridley, G. Kushinga, A. Arshad, J. Douglas, A. Ricketts, and D. Moss, "Radio frequency identification (RFID) as a solution for track and trace of cryogenically-stored cell and gene therapies," *Cytotherapy*, vol. 19, no. 5, p. S122, May 2017.

[148] S. Manzari and G. Marrocco, "Modeling and applications of a chemical-loaded UHF RFID sensing antenna with tuning capability," *IEEE Trans. Antennas Propag.*, vol. 62, no. 1, pp. 94–101, Jan. 2014.

[149] R. A. Potyrailo and C. Surman, "A passive radio-frequency identification (RFID) gas sensor with self-correction against fluctuations of ambient temperature," *Sens. Actuators B, Chem.*, vol. 185, pp. 587–593, Aug. 2013.

[150] J. Virtanen, L. Ukkonen, T. Bjorninen, A. Z. Elsherbeni, and L. Sydänheimo, "Inkjet-printed humidity sensor for passive UHF RFID systems," *IEEE Trans. Instrum. Meas.*, vol. 60, no. 8, pp. 2768–2777, Aug. 2011.

[151] J. J. Martínez-Martínez, F. J. Herraiz-Martínez, and G. Galindo-Romera, "Design and characterization of a passive temperature sensor based on a printed MIW delay line," *IEEE Sensors J.*, vol. 16, no. 22, pp. 7884–7891, Nov. 2016.

[152] S. Kim, C. Mariotti, F. Alimenti, P. Mezzanotte, A. Georgiadis, A. Collado, L. Roselli, and M. M. Tentzeris, "No battery required: Perpetual RFID-enabled wireless sensors for cognitive intelligence applications," *IEEE Microw. Mag.*, vol. 14, no. 5, pp. 66–77, Jul. 2013.

[153] R. Vyas, V. Lakafosis, H. Lee, G. Shaker, L. Yang, G. Orecchini, A. Traille, M. M. Tentzeris, and L. Roselli, "Inkjet printed, self powered, wireless sensors for environmental, gas, and authentication-based sensing," *IEEE Sensors J.*, vol. 11, no. 12, pp. 3139–3152, Dec. 2011.

[154] D. P. Rose, M. E. Ratterman, D. K. Griffin, L. Hou, N. Kelley-Loughnane, R. R. Naik, J. A. Hagen, I. Papautsky, and J. C. Heikenfeld, "Adhesive RFID sensor patch for monitoring of sweat electrolytes," *IEEE Trans. Biomed. Eng.*, vol. 62, no. 6, pp. 1457–1465, Jun. 2015.

[155] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy," in *Proc. 10th ACM Conf. Comput. Commun. Secur. (CCS)*, 2003, pp. 103–111.

[156] Y.-Y. Chen, J.-C. Lu, S.-I. Chen, and J.-K. Jan, "A low-cost RFID authentication protocol with location privacy protection," in *Proc. 5th Int. Conf. Inf. Assurance Secur.*, 2009, pp. 109–113.

[157] A. Juels, "RFID security and privacy: A research survey," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 381–394, Feb. 2006.

[158] H. Tao, S.-W. Hwang, B. Marelli, B. An, J. E. Moreau, M. Yang, M. A. Brenckle, S. Kim, D. L. Kaplan, J. A. Rogers, and F. G. Omenetto, "Silk-based resorbable electronic devices for remotely controlled therapy and *in vivo* infection abatement," *Proc. Nat. Acad. Sci. USA*, vol. 111, no. 49, pp. 17385–17389, Dec. 2014.

[159] M. Curreli, R. Zhang, F. N. Ishikawa, H.-K. Chang, R. J. Cote, C. Zhou, and M. E. Thompson, "Real-time, label-free detection of biological entities using nanowire-based FETs," *IEEE Trans. Nanotechnol.*, vol. 7, no. 6, pp. 651–667, Nov. 2008.

[160] R. A. Robergs, F. Ghiasvand, and D. Parker, "Biochemistry of exercise-induced metabolic acidosis," *Amer. J. Physiol.-Regulatory, Integrative Comparative Physiol.*, vol. 287, no. 3, pp. R502–R516, 2004.

[161] F. Patolsky, G. Zheng, and C. M. Lieber, "Nanowire-based biosensors," *Anal. Chem.*, vol. 78, no. 13, pp. 4260–4269, 2006.

[162] B. Kim, H. S. Song, H. J. Jin, E. J. Park, S. H. Lee, B. Y. Lee, T. H. Park, and S. Hong, "Highly selective and sensitive detection of neurotransmitters using receptor-modified single-walled carbon nanotube sensors," *Nanotechnology*, vol. 24, no. 28, Jul. 2013, Art. no. 285501.

[163] Y. Ohno, K. Maehashi, and K. Matsumoto, "Label-free biosensors based on aptamer-modified graphene field-effect transistors," *J. Amer. Chem. Soc.*, vol. 132, no. 51, pp. 18012–18013, Dec. 2010.

[164] J. Shan, J. Li, X. Chu, M. Xu, F. Jin, X. Wang, L. Ma, X. Fang, Z. Wei, and X. Wang, "High sensitivity glucose detection at extremely low concentrations using a $MoS_2$-based field-effect transistor," *RSC Adv.*, vol. 8, no. 15, pp. 7942–7948, 2018.

[165] L. Torsi, M. Magliulo, K. Manoli, and G. Palazzo, "Organic field-effect transistor sensors: A tutorial review," *Chem. Soc. Rev.*, vol. 42, no. 22, pp. 8612–8628, 2013.

[166] X. Duan, Y. Li, N. K. Rajan, D. A. Routenberg, Y. Modis, and M. A. Reed, "Quantification of the affinities and kinetics of protein interactions using silicon nanowire biosensors," *Nature Nanotechnol.*, vol. 7, no. 6, p. 401, 2012.

[167] D. P. Tran, M. A. Winter, B. Wolfrum, R. Stockmann, C.-T. Yang, M. Pourhassan-Moghaddam, A. Offenhäusser, and B. Thierry, "Toward intraoperative detection of disseminated tumor cells in lymph nodes with silicon nanowire field effect transistors," *ACS Nano*, vol. 10, no. 2, pp. 2357–2364, Feb. 2016.

[168] L. Grebenstein, J. Kirchner, R. S. Peixoto, W. Zimmermann, F. Irnstorfer, W. Wicke, A. Ahmadzadeh, V. Jamali, G. Fischer, R. Weigel, A. Burkovski, and R. Schober, "Biological optical-to-chemical signal conversion interface: A small-scale modulator for molecular communications," *IEEE Trans. Nanobiosci.*, vol. 18, no. 1, pp. 31–42, Jan. 2019.

[169] Y. Liu, E. Kim, J. Li, M. Kang, W. E. Bentley, and G. F. Payne, "Electrochemistry for bio-device molecular communication: The potential to characterize, analyze and actuate biological systems," *Nano Commun. Netw.*, vol. 11, pp. 76–89, Mar. 2017.

[170] Y. Liu, J. Li, T. Tschirhart, J. L. Terrell, E. Kim, C. Tsao, D. L. Kelly, W. E. Bentley, and G. F. Payne, "Connecting biology to electronics: Molecular communication via redox modality," *Adv. Healthcare Mater.*, vol. 6, no. 24, Dec. 2017, Art. no. 1700789.

[171] Y. Liu, C. Tsao, E. Kim, T. Tschirhart, J. L. Terrell, W. E. Bentley, and G. F. Payne, "Using a redox modality to connect synthetic biology to electronics: Hydrogel-based chemo-electro signal transduction for molecular communication," *Adv. Healthcare Mater.*, vol. 6, no. 1, Jan. 2017, Art. no. 1600908.

[172] E. Kim, J. Li, M. Kang, D. L. Kelly, S. Chen, A. Napolitano, L. Panzella, X. Shi, K. Yan, S. Wu, J. Shen, W. E. Bentley, and G. F. Payne, "Redox is a global biodevice information processing modality," *Proc. IEEE*, vol. 107, no. 7, pp. 1402–1424, Jul. 2019.

[173] M. Kang, E. Kim, J. Li, W. E. Bentley, and G. F. Payne, "Redox: Electron-based approach to bio-device molecular communication," in *Proc. IEEE 19th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jun. 2018, pp. 1–5.

[174] Y. Liu, J. S. McGrath, J. H. Moore, G. L. Kolling, J. A. Papin, and N. S. Swami, "Electrofabricated biomaterial-based capacitor on nanoporous gold for enhanced redox amplification," *Electrochimica Acta*, vol. 318, pp. 828–836, Sep. 2019.

[175] S. M. A. El-atty, R. Bidar, and E.-S.-M. El-Rabaie, "MolCom system with downlink/uplink biocyber interface for Internet of bio-NanoThings," *Int. J. Commun. Syst.*, vol. 33, no. 1, p. e4171, Jan. 2020.

[176] T. Bakhshi and S. Shahid, "Securing Internet of bio-nano things: ML-enabled parameter profiling of bio-cyber interfaces," in *Proc. 22nd Int. Multitopic Conf. (INMIC)*, Nov. 2019, pp. 1–8.

[177] M. Zhang, A. Raghunathan, and N. K. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Trans. Biomed. Circuits Syst.*, vol. 7, no. 6, pp. 871–881, Dec. 2013.

[178] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Informat.*, vol. 55, pp. 272–289, Jun. 2015.

[179] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, Dec. 2011.

[180] S. M. R. Islam, F. Ali, H. Moon, and K.-S. Kwak, "Secure channel for molecular communications," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2017, pp. 1–4.

[181] W. Guo, Y. Deng, B. Li, C. Zhao, and A. Nallanathan, "Eavesdropper localization in random walk channels," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1776–1779, Sep. 2016.

[182] S. Zafar, W. Aman, M. M. U. Rahman, A. Alomainy, and Q. H. Abbasi, "Channel impulse response-based physical layer authentication in a diffusion-based molecular communication system," in *Proc. UK/ China Emerg. Technol. (UCET)*, Glasgow, U.K., Aug. 2019, pp. 1–2.
[183] A. Giaretta, S. Balasubramaniam, and M. Conti, "Security vulnerabilities and countermeasures for target localization in bio-NanoThings communication networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 665–676, Apr. 2016.
[184] M. M. U. Rahman, Q. H. Abbasi, N. Chopra, K. Qaraqe, and A. Alomainy, "Physical layer authentication in nano networks at terahertz frequencies for biomedical applications," *IEEE Access*, vol. 5, pp. 7808–7815, 2017.
[185] L. Felicetti, M. Femminella, and G. Reali, "Congestion control in molecular cyber-physical systems," *IEEE Access*, vol. 5, pp. 10000–10011, 2017.
[186] T. Nakano and M. Moore, "In-sequence molecule delivery over an aqueous medium," *Nano Commun. Netw.*, vol. 1, no. 3, pp. 181–188, Sep. 2010.
[187] G. Sharma, S. Bala, and A. K. Verma, "Security frameworks for wireless sensor networks-review," *Procedia Technol.*, vol. 6, pp. 978–987, Jan. 2012.
[188] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proc. IEEE*, vol. 102, no. 8, pp. 1174–1188, Aug. 2014.
[189] N. Ye, Y. Zhu, R.-C. Wang, R. Malekian, and L. Qiao-Min, "An efficient authentication and access control scheme for perception layer of Internet of Things," *Appl. Math*, vol. 8, no. 4, pp. 1–59, 2014.
[190] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions," *J. Ambient Intell. Humanized Comput.*, vol. 4, pp. 1–18, May 2017.
[191] T. Belkhouja, A. Mohamed, A. K. Al-Ali, X. Du, and M. Guizani, "Lightweight solution to defend implantable medical devices against man-in-the-middle attack," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*. Abu Dhabi, UAE: IEEE, Dec. 2018, pp. 1–5.
[192] M. A. Siddiqi and C. Strydis, "Towards realistic battery-DoS protection of implantable medical devices," in *Proc. 16th ACM Int. Conf. Comput. Frontiers* Alghero, Italy: ACM, Apr. 2019, pp. 42–49.
[193] H. Anhalt and N. J. V. Bohannon, "Insulin patch pumps: Their development and future in closed-loop systems," *Diabetes Technol. Therapeutics*, vol. 12, no. S1, pp. S-51–S-58, Jun. 2010.
[194] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informat. J.*, vol. 18, no. 2, pp. 113–122, Jul. 2017.
[195] M. Kintzlinger and N. Nissim, "Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems," *J. Biomed. Informat.*, vol. 95, Jul. 2019, Art. no. 103233.
[196] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT malware detection approaches: Analysis and research challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019.
[197] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proc. ACM SIGCOMM Conf. (SIGCOMM)*. Toronto: ACM, 2011, pp. 2–13.
[198] Y. K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede, "Elliptic-curve-based security processor for RFID," *IEEE Trans. Comput.*, vol. 57, no. 11, pp. 1514–1527, Nov. 2008.
[199] S.-K. Choi, C.-H. Yang, and J. Kwak, "System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats," *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 2, pp. 906–918, 2018.
[200] S. Son, K. Lee, D. Won, and S. Kim, "U-healthcare system protecting privacy based on cloaker," in *Proc. IEEE Int. Conf. Bioinf. Biomed. Workshops (BIBMW)*. Hong Kong: IEEE, Dec. 2010, pp. 417–423.
[201] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "RFID Guardian: A battery-powered mobile device for RFID privacy management," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Brisbane, QLD, Australia: Springer, 2005, pp. 184–194.
[202] X. Hei and X. Du, "The resource depletion attack and defense scheme," in *Proc. Secur. Wireless Implant. Med. Devices*. Berlin, Germany: Springer, 2013, pp. 9–18.
[203] S. M. Wa Umba, A. M. Abu-Mahfouz, T. D. Ramotsoela, and G. P. Hancke, "A review of artificial intelligence based intrusion detection for software-defined wireless sensor networks," in *Proc. IEEE 28th Int. Symp. Ind. Electron. (ISIE)*. Vancouver, BC, Canada: IEEE, Jun. 2019, pp. 1277–1282.
[204] A. Rahim and P. Malone, "Intrusion detection system for wireless nano sensor networks," in *Proc. IEEE 3rd Int. Conf. Inf. Sci. Technol. (ICIST)*. London, UK: IEEE, Dec. 2013, pp. 327–330.
[205] S. Aragon, M. Tiloca, M. Maass, M. Hollick, and S. Raza, "ACE of spades in the IoT security game: A flexible IPsec security profile for access control," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, May 2018, pp. 1–9.
[206] M. Stelzner, F. Dressler, and S. Fischer, "Function centric nano-networking: Addressing nano machines in a medical application scenario," *Nano Commun. Netw.*, vol. 14, pp. 29–39, Dec. 2017.
[207] L. Liu, L. Ding, D. Zhong, J. Han, S. Wang, Q. Meng, C. Qiu, X. Zhang, L.-M. Peng, and Z. Zhang, "Carbon nanotube complementary gigahertz integrated circuits and their applications on wireless sensor interface systems," *ACS Nano*, vol. 13, no. 2, pp. 2526–2535, Jan. 2019.
[208] C. Wang, K. Xia, H. Wang, X. Liang, Z. Yin, and Y. Zhang, "Advanced carbon for flexible and wearable electronics," *Adv. Mater.*, vol. 31, no. 9, Mar. 2019, Art. no. 1801072.
[209] H. Huang, S. Su, N. Wu, H. Wan, S. Wan, H. Bi, and L. Sun, "Graphene-based sensors for human health monitoring," *Frontiers Chem.*, vol. 7, p. 399, Jun. 2019.
[210] S. Kabiri Ameri, R. Ho, H. Jang, L. Tao, Y. Wang, L. Wang, D. M. Schnyer, D. Akinwande, and N. Lu, "Graphene electronic tattoo sensors," *ACS Nano*, vol. 11, no. 8, pp. 7634–7641, Aug. 2017.
[211] P. Cordier, F. Tournilhac, C. Soulié-Ziakovic, and L. Leibler, "Self-healing and thermoreversible rubber from supramolecular assembly," *Nature*, vol. 451, no. 7181, pp. 977–980, Feb. 2008.
[212] B. C.-K. Tee, C. Wang, R. Allen, and Z. Bao, "An electrically and mechanically self-healing composite with pressure- and flexion-sensitive properties for electronic skin applications," *Nature Nanotechnol.*, vol. 7, no. 12, pp. 825–832, Dec. 2012.
[213] Y. Yang, B. Zhu, D. Yin, J. Wei, Z. Wang, R. Xiong, J. Shi, Z. Liu, and Q. Lei, "Flexible self-healing nanocomposites for recoverable motion sensor," *Nano Energy*, vol. 17, pp. 1–9, Oct. 2015.
[214] A. J. Bandodkar, I. Jeerapan, and J. Wang, "Wearable chemical sensors: Present challenges and future prospects," *ACS Sensors*, vol. 1, no. 5, pp. 464–482, May 2016.
[215] A. J. Bandodkar, V. Mohan, C. S. López, J. Ramírez, and J. Wang, "Self-healing inks for autonomous repair of printable electrochemical devices," *Adv. Electron. Mater.*, vol. 1, no. 12, Dec. 2015, Art. no. 1500289.
[216] A. Rizwan, A. Zoha, R. Zhang, W. Ahmad, K. Arshad, N. A. Ali, A. Alomainy, M. A. Imran, and Q. H. Abbasi, "A review on the role of nano-communication in future healthcare systems: A big data analytics perspective," *IEEE Access*, vol. 6, pp. 41903–41920, 2018.
[217] A. Z. Shirazi, S. M. Mazinani, and S. K. Eghbal, "Protocol stack for nano networks," in *Proc. Int. Symp. Comput., Consum. Control*. Taichung, Taiwan: IEEE, Jun. 2012, pp. 849–853.
[218] C. Doukas and I. Maglogiannis, "Managing wearable sensor data through cloud computing," in *Proc. IEEE 3rd Int. Conf. Cloud Comput. Technol. Sci.* Athen, Greece: IEEE, Nov. 2011, pp. 440–445.
[219] C. Liu, C. Yang, X. Zhang, and J. Chen, "External integrity verification for outsourced big data in cloud and IoT: A big picture," *Future Gener. Comput. Syst.*, vol. 49, pp. 58–67, Aug. 2015.
[220] C. Zhang, C. Li, and J. Zhang, "A secure privacy-preserving data aggregation model in wearable wireless sensor networks," *J. Electr. Comput. Eng.*, vol. 2015, pp. 1–9, Jan. 2015.
[221] C. Lin, P. Wang, H. Song, Y. Zhou, Q. Liu, and G. Wu, "A differential privacy protection scheme for sensitive big data in body sensor networks," *Ann. Telecommun.*, vol. 71, nos. 9–10, pp. 465–475, Oct. 2016.
[222] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," *Nano Commun. Netw.*, vol. 3, no. 3, pp. 151–160, Sep. 2012.
[223] S. Dhawan and A. Saini, "Secure data transmission techniques based on DNA cryptography," *Int. J. Emerg. Technol. Comput. Appl. Sci.*, vol. 2, no. 1, pp. 95–100, Aug./Nov. 2012.
[224] G. Cui, L. Qin, Y. Wang, and X. Zhang, "An encryption scheme using DNA technology," in *Proc. 3rd Int. Conf. Bio-Inspired Comput., Theories Appl.*, Sep. 2008, pp. 37–42.
[225] M. Rusia and R. H. Makwana, "Review on DNA based encryption algorithm for text and image data," *Int. J. Eng. Res. Technol.*, vol. 3, no. 1, pp. 3182–3186, 2014.
[226] Y. Zhang and L. B. Fu, "Research on DNA cryptography," in *Applied Cryptography and Network Security*, vol. 357. Berlin, Germany: Springer, 2012, pp. 10–5772.
[227] G. Jacob, "DNA based cryptography: An overview and analysis," *Int. J. Emerg. Sci.*, vol. 3, no. 1, p. 36, 2013.

[228] G. Jacob and A. Murugan, "An encryption scheme with DNA technology and JPEG Zigzag coding for secure transmission of images," 2013, *arXiv:1305.1270*. [Online]. Available: http://arxiv.org/abs/1305.1270
[229] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 4, pp. 394–400, Jan. 2008.
[230] A. Gehani, T. LaBean, and J. Reif, "DNA-based cryptography," in *Aspects of Molecular Computing*. Berlin, Germany: Springer, 2003, pp. 167–188.
[231] K. Malasri and L. Wang, "Design and implementation of a SecureWireless mote-based medical sensor network," *Sensors*, vol. 9, no. 8, pp. 6273–6297, Aug. 2009.
[232] S. C. Seo, D.-G. Han, and S. Hong, "TinyECCK16: An efficient field multiplication algorithm on 16-bit environment and its application to Tmote Sky sensor motes," *IEICE Trans. Inf. Syst.*, vol. E92-D, no. 5, pp. 918–928, 2009.
[233] K. Malasri and L. Wang, "SNAP: An architecture for secure medical sensor networks," in *Proc. 2nd IEEE Workshop Wireless Mesh Netw.* Reston, VA, USA: IEEE, 2006, pp. 160–162.
[234] T. M. Fernández-Caramés, "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6457–6480, Jul. 2020.
[235] F. Dressler and O. Akan, "Bio-inspired networking: From theory to practice," *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 176–183, Nov. 2010.
[236] F. Dressler and O. B. Akan, "A survey on bio-inspired networking," *Comput. Netw.*, vol. 54, no. 6, pp. 881–900, Apr. 2010.
[237] U. Rauf, "A taxonomy of bio-inspired cyber security approaches: Existing techniques and future directions," *Arabian J. Sci. Eng.*, vol. 43, no. 12, pp. 6693–6708, Dec. 2018.
[238] F. Dressler, "Bio-inspired mechanisms for efficient and adaptive network security mechanisms," in *Service Management and Self-Organization in IP-Based Networks* (Dagstuhl Seminar Proceedings), M. Bossardt, G. Carle, D. Hutchison, H. de Meer, and B. Plattner, Eds. no. 04411. Dagstuhl, Germany: Internationales Begegnungs-und Forschungszentrum für Informatik (IBFI), 2005, pp. 1–6.
[239] E. B. Noeparast and T. Banirostam, "A cognitive model of immune system for increasing security in distributed systems," in *Proc. 14th Int. Conf. Comput. Modeling Simulation (UKSim)*. Cambridge, UK: IEEE, Mar. 2012, pp. 181–186.
[240] E. W. Fulp, H. D. Gage, D. J. John, M. R. McNiece, W. H. Turkett, and X. Zhou, "An evolutionary strategy for resilient cyber defense," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 1–6.
[241] S. Bitam, S. Zeadally, and A. Mellouk, "Bio-inspired cybersecurity for wireless sensor networks," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 68–74, Jun. 2016.

**SIDRA ZAFAR** received the B.S. degree in software engineering from International Islamic University Islamabad, Pakistan, and the M.S. degree in computer science from Lahore College for Women University (LCWU), Lahore, Pakistan, in 2012, where she is currently pursuing the Ph.D. degree. She has presented her work at the international conference. Her research interests include the Internet of Nano Things, nano communication networks, security in nanonetworks, and access control.

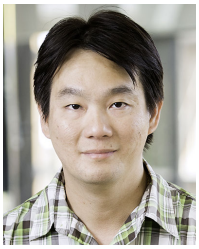
**MOHSIN NAZIR** received the Ph.D. degree from the Asian Institute of Technology (AIT), Thailand, in 2011. He has been working with Lahore College for Women University, as an Associate Professor, since 2012. His research interests include cooperative cognitive wireless communications, game theory, evolutionary game theory, graph theory, smart energy grids, nano communications, cloud computing, QoS, and 4G networks. He is a member of various renowned research societies.

**TAIMUR BAKHSHI** received the B.Sc. degree in electronic engineering in Pakistan, the M.Sc. degree (Hons.) in network systems engineering from the University of Plymouth, U.K., and the Ph.D. degree in computer science from the Department of Computing and Mathematics, University of Plymouth, with a focus on software defined networking. Prior to starting his academic career, he worked for more than five years in IT incident management and network engineering roles for BlackBerry Ltd., and Orange S. A. (France Telecom). He currently holds an associate fellowship position with the Higher Education Academy (HEA), U.K. His present research interests include software defined networking, network measurements, Internet traffic classification, and systems security. He is a professional member of the British Computer Society (BCS) and the Institute of Electrical and Electronic Engineers (IEEE).

**HASAN ALI KHATTAK** (Senior Member, IEEE) received the B.C.S. degree in computer science from the University of Peshawar, Peshawar, Pakistan, in 2006, the master's degree in information engineering from the Politecnico di Torino, Torino, Italy, in 2011, and the Ph.D. degree in electrical and computer engineering from the Politecnico di Bari, Bari, Italy, in April 2015. He has been serving as an Associate Professor with the School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Pakistan, since October 2020. His current research interests include future Internet architectures, such as the Web of Things and leveraging data sciences, and social engineering for future smart cities.

**SARMADULLAH KHAN** received the M.Sc. and Ph.D. degrees in electronics and telecommunication engineering from the Politecnico di Torino, Italy, in 2009 and 2013, respectively. He was an Assistant Professor with the CECOS University of IT and Emerging Science, Peshawar, Pakistan, from 2013 to 2017. He is currently a Lecturer with De Montfort University, U.K. He is also the Program Leader of M.Sc. cyber technology and its pathways. His current research interests include the Internet of Things security, content centric networks security, cryptographic key establishment and management, and wireless sensor networks security. He is a member of academic board of studies, curriculum revision committee, program management board, and school management group. He is also a Guest Editor of two special issues in the journal of *Wireless Communications and Mobile Computing*.

**MUHAMMAD BILAL** (Senior Member, IEEE) received the B.Sc. degree in computer systems engineering from the University of Engineering and Technology, Peshawar, Pakistan, in 2008, the M.S. degree in computer engineering from Chosun University, Gwangju, South Korea, in 2012, and the Ph.D. degree in information and communication network engineering from the School of Electronics and Telecommunications Research Institute (ETRI), Korea University of Science and Technology, in 2017. He is currently an Assistant Professor with the Division of Computer and Electronic Systems Engineering, Hankuk Academy of Foreign Studies, Yongin, South Korea. Prior to joining Hankuk Academy of Foreign Studies, he was a Postdoctoral Research Fellow with the Smart Quantum Communication Center, Korea University, Seoul, South Korea, in 2017. His research interests include design and analysis of network protocols, network architecture, network security, the IoT, named data networking, blockchain, cryptology, and neural networks. He is also an Editor of IEEE Future Directions Ethics and Policy in Technology Newsletter and IEEE Internet Policy Newsletter.



**KIM-KWANG RAYMOND CHOO** (Senior Member, IEEE) received the Ph.D. degree in information security from the Queensland University of Technology, Australia, in 2006. He currently holds the cloud technology endowed professorship position at The University of Texas at San Antonio (UTSA). He was a recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), the British Computer Society's 2019 Wilkes Award Runner-up, the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, the Outstanding Associate Editor of 2018 for IEEE Access, the 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, the Fulbright Scholarship, in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award, in 2008. He received best paper awards from IEEE Systems Journal, in 2021; *IEEE Consumer Electronics Magazine*, in 2020; *EURASIP Journal on Wireless Communications and Networking*, in 2019; IEEE TrustCom, in 2018; and *Computer Security–ESORICS 2015*. He received the Korea Information Processing Society's *Journal of Information Processing Systems* Outstanding Research Award (Most-cited Paper), in 2020; and the Survey Paper Award (Gold), in 2019; the IEEE Blockchain 2019 Outstanding Paper Award; and the Best Student Paper Awards from ACISP 2005 and Inscrypt 2019. He is also the Founding Co-Editor-in-Chief of *Distributed Ledger Technologies: Research & Practice* (ACM), and Founding Chair of IEEE Technology and Engineering Management Society's Technical Committee on Blockchain and Distributed Ledger Technologies.

**KYUNG-SUP KWAK** (Life Senior Member, IEEE) received the Ph.D. degree from the University of California. He was with Hughes Network Systems and IBM Network Analysis Center, USA. He was with Inha University, South Korea, as a Professor. He was also the Dean of the Graduate School of Information Technology and Telecommunications and the Director of the UWB Wireless Communications Research Center. In 2008, he was an Inha Fellow Professor (IFP). He is currently an Inha Hanlim Fellow Professor. His research interests include UWB radio systems, wireless body area networks, and nano and molecular communications. He received the official commendations for achievements of UWB Radio Technology R/D from the Korean President, in 2009. He was the President of the Korean Institute of Communication Sciences (KICS), in 2006, and the Korea Institute of Intelligent Transport Systems (KITS), in 2009.

**ANEEQA SABAH** is currently working as an Assistant professor in physics with LCWU. She has been Awarded for the Overseas Scholarship for the Ph.D. degree in the field of Nanotechnology by the Higher Education Commission (HEC), Pakistan. It was a successful project. She has been supervising the several projects on the B.S., M.S., and Ph.D. level, based on nano fabrication, nano films and membranes, quantum dots, hybrid materials, spectroscopy, composites, and metal doped sensing. She has published many research articles in high impact factor journals, such as *The Journal of Physical Chemistry A* and ACS, and involved in participating and organizing seminar and conferences in respective departments. Her expertise is nano synthesis, self-assembly and organization, colloids, one dimensional nano materials, green chemistry, and quantum dots.



View publication stats