available online at: https://alkadhum-col.edu.iq/ijst/index.php/JACEAS

2023, р.р 27-37



Journal of Imam Al Kadhum College for Engineering and Applied Sciences (JKCEAS)



Applications of the Internet of Nano Things in Health Care

Ruaa S. kammel^{1*}, Dania K. Hafedh²

¹ Department of Computer Techniques Engineering, Imam Alkadhum College (IKC), Baghdad, Iraq,

ruaa_s_k@alkadhum-col.edu.iq

² Department of Computer Techniques Engineering, Imam Alkadhum College (IKC), Baghdad, Iraq, <u>dania2000khaled@gmail.com</u>

Received: 1/9/2022

Accepted: 1/10/2022

Abstract

The Internet of Nano Things (IoNT) is a relatively new addition to the Internet of Things (IoT). The IoNT refers to the connectivity of nanodevices and nanosensors, and next-generation standards based on the IoT have been established to connect many nanomachines with current communications systems via the Internet. In communication networks, nanoscale applications provide a new edge. Because of the novel features resulting from nanotechnology's benefits, IoNT opened the door to a slew of new applications in a range of fields. This study provides an overview of the IoNT technique, including its implementation, objectives, general implications, and most significant problems, as well as the differences between IoT and IoNT. The architecture of the IoNT in smart health care, as well as the most essential technologies used in nano communication networks, have been recognized, along with an assessment of each technology's merits.

Keywords: Internet of Nano Things (IoNT); architecture of IoNT; health care applications; IoNT applicatons.

1. Introduction

The increased linking of everyday life applications with smart systems resulted in the emergence of the Internet of Nano Things (IoNT), whose massive expansion, which included various public and private fields, resulted in the introduction of a new communication network model based on nanotechnology. Most critical difficulties can now be overcome using this technology, and applications such as reading data from portable sensors are now available [1]. The most important factors in the advancement of IoNT technology are low-cost processing capabilities in comparison to massive storage capacities, as well as smart antennas and smart Radio Frequency Identification (RFID) technology [2]. Together using local wireless connections, as a result, a new notion known as the Internet of Everything has emerged (IoE) [3]. The Internet of Bio-Nano Things (IoBNT) are based on bio-nano objects, which are defined as the unique identifier of a basic structural feature part that describes the function and connection in biological settings [4]. The popularity of (IoNT) is growing by the day, mainly using current and new mobile communications technologies. The IoNT may connect with any item in our environment via wireless connections [5]. According to recent research, the level of studies in the IoNT field has been quite

^{*} corresponding author

limited in recent years, as shown in the graph of Fig 1, a low rate of production throughout this period, and the necessity to stimulate interest in this area [6].

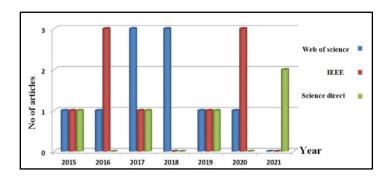


Fig. 1. The volume of IoNT publications through the major browsers between 2015 and 2021 [6].

2. Literature Reviews

Several IoNT technology gates were created to gain access to one or more nanonets while ensuring accuracy and reliability. The intended IoNT healthcare applications and their requirements are recognized, as are the fundamental health care facility chances [7]. While studying in-body nanocommunication, network with the IoNT architecture's body area network via an overview and major requirements to create portals. This studied model creates a new level of security, and the authors assessed the resulting security challenges with processors. Another study looked at the impact of changing environmental conditions on IoNT communication based on molecular contacts, specifically temperature (T) and the relative concentration of physical obstacles (X) [8]. The IoNT-based telemedicine application was examined, and medical data from international publications was obtained, processed, and distributed developed a new approach called the rational data delivery approach (RDDA) to provide an extended network lifetime without affecting other QoL features within the IoNT [9]. A proposal was presented to address the energy problem in the IoNT communication system, which included synchronization of wireless information and nanonetworks that transmit energy in the terahertz (THz) range to ensure improved system performance [10]. The energy problem was also investigated, with the proposal of a system that saves energy by employing only one brief pulse. This system is based on the use of a uniform linear model [11]. The general markov decision process (MDP) model has been presented as a mathematical model that contributes to the development of transportation policy in IoNT technology by addressing some constraints [2]. It will help to lower the cost of this procedure while also minimizing the risk of implant damage inside the body. Wireless nanosensor networks (WNSN) and IoNT routing protocols have been investigated [12]. Which, through its connection with other nanodevices, contributes to the expansion of coverage. A review of this technology has been provided in this paper, as well as an explanation of the IoNT in health care communications architecture. The authors presented an encryption strategy for dealing with the security concerns of IoNT by utilizing security developments in the radio physical layers (PLs), this approach helps to make the system's task easier while also making it safer [13]. A review of IoNT technology has been provided in this paper, as well as an explanation of the IoNT in health care communications architecture.

3. Internet of Nano Things (IoNT)

The establishment of a physical network, made of nanomaterials, that permits the interchange of data through diverse components connecting with each other at the micro level is where nanotechnology and the Internet of Things (IoT) can be merged, the Internet of Nano Things (IoNT) is the name given to this phenomenon. It is not yet at the level of other IoT systems in terms of development, but it is garnering interest from the communication and medical industries. One example is in field-based applications where remote sensing is necessary, or for measuring different sites within a human body. The IoT is a collection of sensor networks, data collectors, and transmitters that deliver data from many entry points into a centralized location via the cloud, this allows the IoT to be self-sufficient, requiring no human input unless the system detects a problem through its analytics and alerts an operator [14]. In essence, the IoNT is a miniature version of these systems, they could send data across the network by using nanosensors as link gateways. Despite their lack of development compared to their IoT counterparts, their

method of collecting signals with sensing element nodes allows them to act for purposes that are unsuitable with other (bulkier) sensing devices [14,15]. Table 1 summarizes the most notable comparisons between IoNT and IoT.

No.	IoNT	ют
1	It concentrates on manufacturing, power plants,	It concentrates on a broad range of applications, ranging
	oil and gas, and other industrial applications [11].	from wearables to robotics and machinery [16].
2	It makes use of vital devices linked by a system that,	Its application begins on a tiny level, there are no existing
	if they fail, could result in its existence or other extreme	circumstances to be concerned about.
	circumstances, necessitating the use of more sensitive and accurate	
	detectors.	
3	It is concerned with tiny systems.	It is concerned with the big networks.
4	It can be controlled from afar.	It allows for simple off-site computing.
5	It may entail collecting in the middle to upper range.	It can only process a limited amount of data at once.
6	To secure sensitive information necessitates a high level of	It necessitates both identification and security.
	security.	
7	It necessitates a set of strict criteria.	It has to meet certain criteria.
8	It has a lengthy lifespan.	It has a rather limited product life cycle.
9	It's extremely dependable.	It's much less dependable.

3.1 IoNT architecture techniques

There are two types of IoNT: the Multimedia Internet of Nanoscale Things (IoMNT) and the Internet of Nanoscale Bio Things (IoNBT). Nanodevices connect to existing communication networks in both cases. The IoNT network architecture is determined by the application domain and its unique characteristics [17]. The features of nanomaterials contained in nanodevices, such as graphene nanoribbon (GNR), are just one planar layer comprised of hydrocarbon chains placed on a hexagonal crystalline, or carbon nanotubes (CNT), play a key role in IoNT design difficulties [17]. A Wi-Fi access point known as a gate gives a precise position of a patient's location or the location of a patient's smartphone [18]. The IoNT architecture combines intra-body nanocommunication networks with body-area networks. The nanodevices are spread in groups in this design, with each group having a group boss who manages the data and sends it to the nano router via a dynamic path that changes depending on the configuration and availability; these nanopaths cleverly connect to the nearest gateway to send data; the nanodevices are then linked together by networks that are physically separated [19].

The main nanodevices based on the IoNT architecture are the processor, communication, sensor, actuation units, and storage units [14]. From the perspective of the individual, house, car, road, or clinic, off-body systems are widespread. These technologies are capable of providing comprehensive health monitoring [14]. The IoNT network's components change depending on the situation. Fig 2 depicts the general IoNT architecture, which combines intra-body nanocommunication systems with body-area networks. In this design, the nanodevices are spread into subgroups, with each team having a unit supervisor that manages the data and transmits it to the nanorouter via a variable route that alters depending on the configuration and accessibility. These nanopaths smartly connect to the adjacent gateway to send data. The nanodevices are then linked together by lines that are technically segregated. However, there are crucial features for the network design of IoNT in diverse applications. These are some of the elements:

• Nano-nodes: are the smallest and simplest nanodevices that perform a variety of functions, such as processing and data transfer over short distances with little memory. Biological sensors embedded in the human body are referred to as nano-nodes in body sensor networks.

• Nano-routers: in comparison to nanonodes, nano-routers have a lot of computing capacity and operate as aggregators of data from nanonodes. Nano-routers are also important for controlling nano-nodes through the exchange of control commands.

• Nano-micro interface devices: these devices collect information from nano-routers and transmit it to the microscale, as well as the other way around. They function as hybrid devices, allowing them to communicate at the

nanoscale using nanocommunication techniques as well as with traditional communication networks using traditional network protocols.

• Gateway: it allows for internet-based remote control of the complete nanothings network. Consider the body sensor network: With the deployment of a gateway, all sensor data from the human body may be accessible by doctors from anywhere in the world over the Internet.

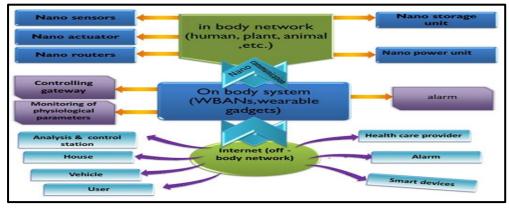


Fig. 2. the IoNT architecture in general [6].

The IoNT is rapidly changing the health care landscape by focusing on how people, devices, and applications are connected and interact with one another, as well as promising health care solutions, resulting in a more revolutionary archetype for health care manufacturing based on a safety model [20]. Rapid advances in information and communication technology (ICT) and the growing number of smart things have enabled a variety of e-health situations (detectors and mobile devices). These health care services include a wealth of information that can be used to gain knowledge, as illustrated in Fig 3. Internet-powered e-health has the potential to improve outcomes, increase efficiency, and reduce health-care costs by integrating information, people, technologies, procedures, and the environment. It is vital to track and record personal data in order to keep track of it.

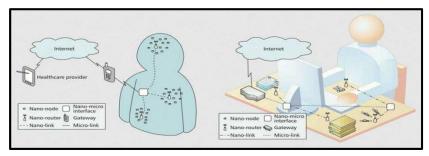


Fig. 3. network architecture for the IoNT [21].

3.2 IoNT applications

IoNT uses the most complex and advanced methodology for data collection when compared to IoT regular architecture and common components, allowing it to expand its base from existing appliances with a wide range of new and innovative appliances. Medical services monitoring and nano-sensor-based body sensors are examples of IoNT applications, as shown in Fig 4 [3].

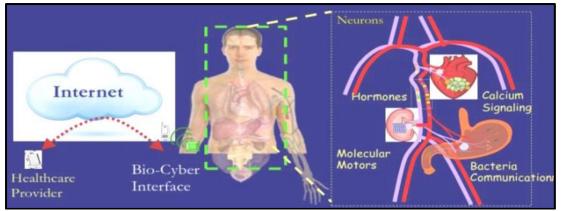


Fig. 4. example of IoNT Applications [3].

IoNT devices will communicate with one another via short-range wireless technologies, including WiFi, RFID, and sensor networks; this is accomplished through the use of nanosensors and nanonetworks to integrate nanosensors into a variety of items. A model of this concept as a medical application demonstrates the use of some instruments that were previously difficult to use due to their massive sensor size; this will enable the acquisition of new medical and environmental data, which could lead to the refinement of existing data, new discoveries, and enhanced medical diagnostics [22]. Each functional task, like actuation or sensing, is carried out in an IoNT, this is accomplished by adding nanodevices that can be linked together using nanonetworks [23]. The concept of nanonetworks in health care applications is illustrated in figure 5. Nanotechnology facilitates the ability to feel and respond, capture data from parts of the body that have previously been accessible because of network size constraints. As a consequence, modern treatment diagnoses and discoveries will help enhance medical technology. As a result, the internet of things will be used not just in the visible world, but also at scales that are unseen to visible light. This will be accomplished through the employment of IoNT and IoBNT.

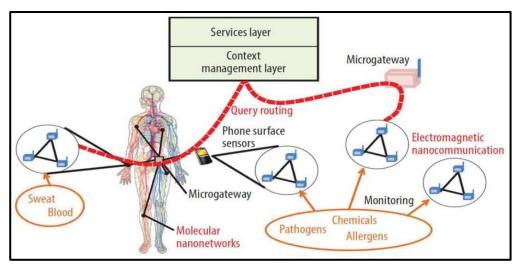


Fig. 5. nanonetworks in health care application [21].

IoNT technology has several prospective applications that researchers have highlighted in various fields based on the advantages of this current technology, which can have a major effect on various fields in the future and can signal IoNT use as shown in Fig 6 [24].

• Biomedical Applications: the most important applications based on IoNT technology are biological applications, which are conceivable due to the size convergence between nanoparticles and living cells, as this technology can simulate living cells.

• Military: as the weapons business develops and diversifies, IoNT technology can perform a wide range of services.

• Industry: industry can profit from IoNT in several ways. Using nanomaterials to detect and interpret the motions of a certain shape in the environment can enhance the accuracy of a device [14].

• Smart Cities: household appliances, monitoring sensors, observation cams, motors, buses, vehicles, and other equipment can all interact and communicate with each other in a smart city [22].

• Oil and gas: using nano-sensor features, IoNT provides a fantastic opportunity to locate underground oil with high accuracy.

• Multimedia: nanotechnology has provided new non-materials for the fabrication of a new generation of small photodetectors and acoustic nano-transducers.

• Functionalized Materials and Fabrics: using IoNT technology, it is possible to develop materials and fabrics with modern features that aid in the development of antibacterial textiles and the production of spot pesticides in the textile industry, such as contributing to the development of antibacterial textiles and the manufacture of spot pesticides.

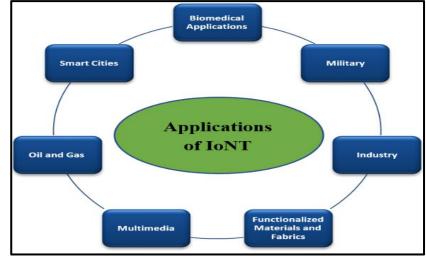


Fig. 6. general applications of IoNT.

3.2.1 Health care applications (IoBNT) in IoNT

The compatibility of IoNT with nanobiosensors in the human body is a problem because these sensors are often created artificially. The artificiality of nanoelectronics may have unfavorable health consequences. To overcome this issue, the notion of an internet of bio-nano things (IoBNT) has been proposed [25]. IoBNT was developed by fusing nanotechnology, IoNT, and synthetic biology to control, change, reengineer, and reuse biological cells in IoT-enabled computing devices [26]. As shown in Fig 7, it entails networking and communication between nanoscale and biological elements, with organic molecules replacing electronics in cells [27].

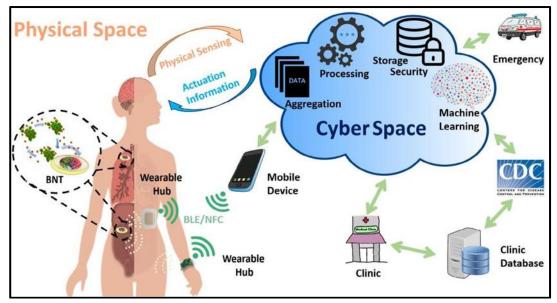


Fig. 7. IoBNT concept [27].

The goal of this figure is to interface directly with cells; this enables more precise detection and, potentially, real-time management of the human body's highly complex processes. Modified cells must perceive, process, and interact with one another, as well as with exterior features that enable distant and endoscopic questioning, according to the IoBNT concept. The first step in putting IoBNT into practice is to create implantable sub-millimeter BNTs that can sense biochemical data inside the body and send that data to a wearable center from outside the body. Not only is this paradigm helpful to personal health, but it is beneficial to the health care system. In the event of an epidemic or pandemic, the continuous monitoring of infections provided by IoBNT sensors is particularly useful. Because IoBNT is already connected to portable systems and wireless analytics platforms, it can be easily adapted for monitoring, locating, and isolating individuals. Some of the most well-known IoBNT applications in healthcare include:

• Bio-hybrid grafts: can be used to replace all individual body systems, neurological systems, and missing cells.

• Immune system support: the body controls various alien and pathogen elements, and nano devices can be used in conjunction with intelligent devices to prevent various infections, the medical business will be transformed, especially in the detection of cancer.

• Health Care Monitoring: nanosensors can be used in health care monitoring applications to measure variables such as temperature, pressure, sugar, and blood fat. These sensors can also be used to identify cancerous and non-cancerous tumors [8]. Furthermore, by detecting the afflicted area and utilizing the myelin sheath, nanosensors can be used to treat nerve cell injury. Although the nerve impulse signal is transmitted by IoNT's microsensors,

• Body Sensor Networks: a network of nanosensors embedded in the body that play a crucial role in collecting and monitoring the organic movement of a patient, as well as other landmarks. BSN provides continuous data on a portable device employing nanoscale sensors that the expert can use to easily get information about the patient's health [23].

• Drug Delivery Systems: nanodevices can be used as regulator implants in the Internet of Bio-Nano Things (IoBNT) to compensate for metabolic illnesses such as diabetes. To support the glucose level processes, smart glucose reservoirs and nanosensors work together. Drug delivery systems that transfer neurotransmitters or specific medications to the neuro system can be used to eliminate the consequences of neurodegenerative illnesses [28].

3.2.2 The benefits of IoNT in health Care

IoNT provides nano-networking between distinct nanobiosensors implanted in or on the body. Individual nanobiosensors work in isolation. IoNT enables networked health care, allowing various disparate devices to collaborate and offer more detailed data. More precise clinical decision-making is aided by combining data from many regions of the body. Through IoNT, the health information gathered by biosensors is made available to stakeholders such as doctors, medical service providers, the patient and his or her relatives, and so on. As a result,

IoNT serves as a universal health care system, allowing for continuous and real-time monitoring of a patient's health state from somewhere and at any time. This not only allows for quick care, but it also allows for the initial discovery and diagnosis of disease. This also ensures that therapy and rehabilitation are cost-efficient, precise, and beneficial for the patient [29]. The key benefits of IoNT in health care are illustrated in Fig 8.

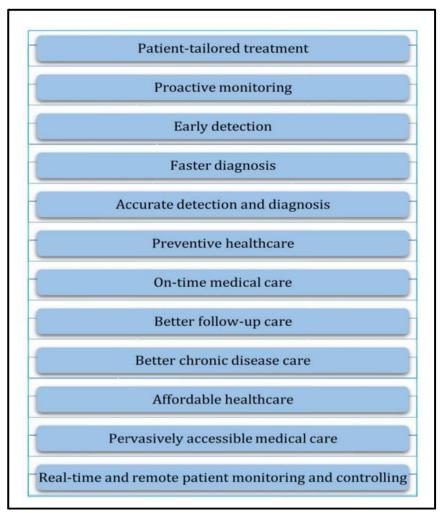


Fig. 8. Advantages of IoNT in health care [30].

Health-related information is particularly sensitive, and it must be properly protected. IoNT necessitates the development of new and adequate security and privacy frameworks and methods to reduce the risk of malicious attacks (e.g., interruption of clinical uses that may cause harm or death due to medicine and radio interaction), as detailed in numerous research papers [31, 32]. Table 2 seeks to summarize the benefits, drawbacks, possibilities, and risks associated with the application of nanoscale and IoNT in health care.

Strengths	Weaknesses
• quicker and more precise analytic procedures; advanced and passable	• There is still a paucity of understanding about how
therapies; painless treatments; and reduced negative effects of drugs and	nanoparticles and nanostructures behave within the
surgical procedures.	human body.
• Quicker, minor, extremely subtle diagnostic and action apparatuses (e.g.,	• Nanoparticles and nanomaterials toxic effects.
nanorobots, nanoneedles, nanotweezers, etc.)	• Health-related data privacy and security concerns.
• The IoNT allows for real-time and distant health and treatment	• Standards and regulations are lacking [34].
monitoring, as well as a significant reduction in health care and medical	
costs [33].	
Opportunities	Threats
Opportunities Nano network security and privacy concerns are not fully addressed. 	Threats Nano network security and privacy concerns are not
Nano network security and privacy concerns are not fully addressed.	Nano network security and privacy concerns are not
 Nano network security and privacy concerns are not fully addressed. Controlling nanotechnologies in medicine and health care is a source of 	 Nano network security and privacy concerns are not fully addressed.
 Nano network security and privacy concerns are not fully addressed. Controlling nanotechnologies in medicine and health care is a source of concern. 	 Nano network security and privacy concerns are not fully addressed. Controlling nanotechnologies in medicine and health
 Nano network security and privacy concerns are not fully addressed. Controlling nanotechnologies in medicine and health care is a source of concern. Due to a lack of suitable mechanisms, nanotechnology and the IoNT 	 Nano network security and privacy concerns are not fully addressed. Controlling nanotechnologies in medicine and health care is a source of concern.
 Nano network security and privacy concerns are not fully addressed. Controlling nanotechnologies in medicine and health care is a source of concern. Due to a lack of suitable mechanisms, nanotechnology and the IoNT 	 Nano network security and privacy concerns are not fully addressed. Controlling nanotechnologies in medicine and health care is a source of concern. Due to a lack of adequate mechanisms, nanotechnology

Table 2. the strengths, weaknesses, opportunities and threats for IoNT applications in health care

3.3 Challenges of IoNT

Because IoNT technology functions at the nanoscale scale, it poses a number of issues that need to be investigated by researchers in order to create answers that will allow this technology to give better services to humanity in a way that is safer and less destructive to societies. One of the issues that has been researched is the connection of body area networks and other extrinsic gates to nanodevices inside the body. The challenge of ensuring high throughput for distributed scheduling algorithms while maintaining low average latency has been addressed, as has the challenge of allowing data to be carried within strict constraints before being released when the next package arrives [7]. Some of these are listed below:

• IoNT security technique: one of the most significant challenges facing IoNT technology is the issue of security and privacy during its operation. Because IoNT technology enters the human body in addition to its work outside of it, the sensitivity of the information transmitted by this technology increases, as does the need for safety to protect lives and property. Because IoNT runs at terahertz frequencies, it necessitates new security measures that are compatible with this technology in order to prevent data theft and user injury. Eavesdropping and data theft, attempts to disrupt therapeutic injection operations, and changing nanocommunication lines or a blocking gateway are among the most serious security threats.

• Privacy: phones, home appliances, and the like are examples of data theft threats that IoNT deals with as a result of its integration with other apps, as this data can be attacked, especially when they are connected to the internet.

• Nanoscale communication: this technology's deployment faces challenges, including those related to the nanoscale size of IoNT devices, which necessitates the redesign and development of new communication models and network concepts compatible with these components.

4. Conclusions

Because of the relative ease of mass deployment and the nanoscale operational mode, the IoNT holds a lot of potential for omnipresent health care. On the other hand, the unique qualities of nanoscale devices must be included in network architecture design, and the challenges of nano-communication paradigms must be addressed in networking protocols. A review of IoNT approaches was studied in this paper. This technique's architecture, communication methodologies, applications, difficulties, and recommendations have also been discussed. Researchers in this field need to give more importance to IoNT technology. It was decided that this technology has a wide range of applications in several fields, as well as numerous issues that need to be addressed and some future

recommendations. The findings reveal that this technology will be extremely valuable in the future development of several scientific and practical sectors.

References

[1] Al-Turjman, F. (2020). Intelligence and security in big 5G-oriented IoNT: an overview. Future Generation Computer Systems, 102, 357-368.

[2] Cruz Alvarado, M. A., & Bazán, P. (2019). Understanding the Internet of Nano Things: overview, trends, and challenges. E-Ciencias de la Información, 9(1), 152-182.

[3] Nayyar, A., Puri, V., & Le, D. N. (2017). Internet of nano things (IoNT): Next evolutionary step in nanotechnology. Nanoscience and Nanotechnology, 7(1), 4-8.

[4] Ali, N. A., Aleyadeh, W., & AbuElkhair, M. (2016, September). Internet of nano-things network models and medical applications. In 2016 International Wireless Communications and Mobile Computing Conference (IWCMC) (pp. 211-215). IEEE.

[5] Atlam, H. F., Alenezi, A., Alharthi, A., Walters, R. J., & Wills, G. B. (2017, June). Integration of cloud computing with internet of things: challenges and open issues. In 2017 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData) (pp. 670-675). IEEE.

[6] Naser, H. A., Lateef, A. T., Bida, F. A., & Zorah, M. (2021). Systematic Review of Internet of Nano Things (IoNT) Technology: Taxonomy, Architecture, Open Challenges, Motivation and Recommendations. Iraqi Journal of Nanotechnology, (2), 7-19.

[7] Dressler, F., & Fischer, S. (2015). Connecting in-body nano communication with body area networks: Challenges and opportunities of the Internet of Nano Things. Nano Communication Networks, 6(2), 29-38.

[8] Jarmakiewicz, J., Parobczak, K., & Maślanka, K. (2016, May). On the Internet of Nano Things in healthcare network. In 2016 International Conference on Military Communications and Information Systems (ICMCIS) (pp. 1-6). IEEE.

[9] Al-Turjman, F. (2019). A rational data delivery framework for disaster-inspired internet of nano-things (IoNT) in practice. Cluster Computing, 22(1), 1751-1763.

[10] Atlam, H. F., Walters, R. J., & Wills, G. B. (2018, August). Internet of nano things: Security issues and applications. In Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing (pp. 71-77).

[11] Rong, Z., Leeson, M. S., Higgins, M. D., & Lu, Y. (2018). Nano-rectenna powered body-centric nano-networks in the terahertz band. Healthcare technology letters, 5(4), 113-117.

[12] Canovas-Carrasco, S., Sandoval, R. M., Garcia-Sanchez, A. J., & Garcia-Haro, J. (2019). Optimal transmission policy derivation for IoNT flow-guided nano-sensor networks. IEEE Internet of Things Journal, 6(2), 2288-2298.

[13] Balghusoon, A. O., & Mahfoudh, S. (2020). Routing protocols for wireless nanosensor networks and internet of nano things: a comprehensive survey. IEEE Access, 8, 200724-200748.

[14] Pramanik, P. K. D., Solanki, A., Debnath, A., Nayyar, A., El-Sappagh, S., & Kwak, K. S. (2020). Advancing modern healthcare with nanotechnology, nanobiosensors, and internet of nano things: Taxonomies, applications, architecture, and challenges. IEEE Access, 8, 65230-65266.

[15] Perwej, Y., Haq, K., Parwej, F., Mumdouh, M., & Hassan, M. (2019). The internet of things (IoT) and its application domains. International Journal of Computer Applications, 182(49), 36-49.

[16] Panigrahi, T., & Hassan, M. (2018, December). Energy efficient event localization and classification for nano IoT. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[17] Perwej, Y., Parwej, F., Hassan, M. M. M., & Akhtar, N. (2019). The internet-of-things (IoT) security: A technological perspective and review. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 5(1), 462-482.

[18] Piro, G., Boggia, G., & Grieco, L. A. (2015). On the design of an energy-harvesting protocol stack for Body Area Nano-NETworks. Nano Communication Networks, 6(2), 74-84.

[19] Youssef, M., Ghanim, F., Imad, N., Alqasim, A., & Shubair, R. (2018). Design of intra-body nano-communication network for future nano-medicine. arXiv preprint arXiv:1810.00186.

[20] Atlam, H., Alenezi, A., Walters, R., & Wills, G. (2017). An overview of risk estimation techniques in risk-based access control for the internet of things. In 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017) (pp. 254-260). INSTICC.

[21] Akyildiz, I. F., & Jornet, J. M. (2010). The internet of nano-things. IEEE Wireless Communications, 17(6), 58-63.

[22] Akkari, N., Wang, P., Jornet, J. M., Fadel, E., Elrefaei, L., Malik, M. G. A., ... & Akyildiz, I. F. (2016). Distributed timely throughput optimal scheduling for the Internet of Nano-Things. IEEE Internet of Things Journal, 3(6), 1202-1212.

[23] Balasubramaniam, S., & Kangasharju, J. (2012). Realizing the internet of nano things: challenges, solutions, and applications. Computer, 46(2), 62-68.

[24] Rutherglen, C., & Burke, P. (2009). Nanoelectromagnetics: Circuit and electromagnetic properties of carbon nanotubes. small, 5(8), 884-906.

[25] Akyildiz, I. F., Pierobon, M., Balasubramaniam, S., & Koucheryavy, Y. (2015). The internet of bio-nano things. IEEE Communications Magazine, 53(3), 32-40.

[26] Almazrouei, E., Shubair, R. M., & Saffre, F. (2018). Internet of nanothings: Concepts and applications. arXiv preprint arXiv:1809.08914.

[27] Akyildiz, I. F., Ghovanloo, M., Guler, U., Ozkaya-Ahmadov, T., Sarioglu, A. F., & Unluturk, B. D. (2020). PANACEA: An internet of bio-nanothings application for early detection and mitigation of infectious diseases. IEEE Access, 8, 140512-140523.

[28] Freitas, R. A. (2006). Pharmacytes: An ideal vehicle for targeted drug delivery. Journal of Nanoscience and Nanotechnology, 6 (9-10), 2769-2775.

[29] Omanović-Mikličanin, E., Maksimović, M., & Vujović, V. (2015). The future of healthcare: nanomedicine and internet of nano things. Folia Medica Facultatis Medicinae Universitatis Saraeviensis, 50(1), 23-28.

[30] Pramanik, P. K. D., Nayyar, A., & Pareek, G. (2019). WBAN: Driving e-healthcare beyond telemedicine to remote health monitoring: Architecture and protocols. In Telemedicine technologies (pp. 89-119). Academic Press.

[31] Ezz El-Din, H., Manjaiah, D.H. (2017). Internet of Nano Things and Industrial Internet of Things. In: Acharjya, D., Geetha, M. (Eds.), Internet of Things: Novel Advances and Envisioned Applications. Studies in Big Data (pp. 109-123). Cham: Springer.

[32] Dressler, F., & Kargl, F. (2012, June). Security in nano communication: Challenges and open research issues. In 2012 IEEE International Conference on Communications (ICC) (pp. 6183-6187). IEEE.

[33] Bhatt, Y., Bhatt, C. (2017). Internet of Things in HealthCare. In: Bhatt, C., Dey, N., Ashour, A. (Eds.), Internet of Things and Big Data Technologies for Next Generation Healthcare. Studies in Big Data (pp. 13–33). Cham: Springer.

[34] Akyildiz, I. F., Jornet, J. M., & Pierobon, M. (2011). Nanonetworks: A new frontier in communications. Communications of the ACM, 54(11), 84-89

[35] Parveen, K., Banse, V., & Ledwani, L. (2016, April). Green synthesis of nanoparticles: their advantages and disadvantages. In AIP conference proceedings (Vol. 1724, No. 1, p. 020048). AIP Publishing LLC.