The internet of nano things (IoNT) existing state and future Prospects

Nikhat Akhtar, Yusuf Perwej

GSC Advanced Research and Reviews, 2020, 05(02), 131–150

Available online at GSC Online Press Directory

GSC Advanced Research and Reviews

e-ISSN: 2582-4597, CODEN (USA): GARRC2

Journal homepage: https://www.gsconlinepress.com/journals/gscarr

(RESEARCH ARTICLE)

The internet of nano things (IoNT) existing state and future Prospects

Nikhat Akhtar [1,*] and Yusuf Perwej [2]

[1] *Research Scholar (Ph.D), Department of Computer Science & Engineering, Babu Banarasi Das University, Lucknow, India.*
[2] *Associate Professor, Department of Computer Science & Engineering, India.*

Publication history**:** Received on 16 November 2020; revised on 25 November 2020; accepted on 28 November 2020

Article DOI: https://doi.org/10.30574/gscarr.2020.5.2.0110

Abstract

The increase of intelligent environments suggests the interconnectivity of applications and the use of the Internet. For this reason, arise what is known as the Internet of Things (IoT). The expansion of the IoT concept gives access to the Internet of Nano Things (IoNT). A new communication networks paradigm based on nano technology and IoT, in other words, a paradigm with the capacity to interconnect nano-scale devices through existing networks. From the interconnection of these nano machines with the Internet emerged the concept of Internet of Nano Things (IoNT). The Internet of Nano-Things (IoNT) is a system of nano connected devices, objects, or organisms that have unique identifiers to transfer data over a computer or cellular network wirelessly to the Cloud. The data delivery, caching, and energy consumption are among the most significant topics in the IoNT nowadays. The nano-networks paradigm can empower the consumers to make a difference to their well-being by connecting data to personalized analysis within timely insights. The real-time data can be used in a diversification of nano-applications in the Internet of Nano-Things (IoNT), from preventive treatment to diagnostics and rehabilitation. In this paper intelligibly explains the Internet of Nano Things (IoNT), its architecture, challenges, explains the role of IoNT in global market, IoNT applications in various domains. Internet of things has provided countless new opportunity to create a powerful industrialized structure and many more. The key applications for IoNT communication including healthcare, transportation and logistics, defense and aerospace, media and entertainment, manufacturing, oil and gas, high speed data transfer & cellular, multimedia, immune system support and others services. In the end, since security is considered to be one of the main issues of the IoNT system, we provide an in-depth discussion on security, communication network and Internet of Nano Things (IoNT) market trends.

Keywords: Internet Of Nano Things (IoNT); Nanoscale Devices; Nano-Bioscience; Sensors; Internet Of Things (IoT); Internet Of Bio-Nano Things (IoBNT); Body Sensor Network (BSN).

1. Introduction

The arrival of the internet of things [1] has transformed the day to day functionality of each life's intensely. The Internet is a highly connected global network which promises to connect physical and digital devices. Several IoT applications have been implemented and deployed in the modern years [2]. The Internet of things (IoT) extends the objective of the internet to many devices and objects from different domains by interconnecting them. Internet of Things (IoT) the new dawn technology [3] that describes how data, people, and interconnected physical objects act based on communicated information, and big data [4] analytics have been adopted by diverse domains for varying purposes. The Internet of Things (IoT) and big data are massive, complex ideas. While interrelated, they're also distinct. The IoT consists of

*Corresponding author: Nikhat Akhtar and E-mail - dr.nikhatakhtar@gmail.com
Research Scholar (Ph.D), Department of Computer Science & Engineering, Babu Banarasi Das University, Lucknow, India .

millions of devices that collect and communicate information, but big data [5] encompasses a much wider landscape. The big data [6] and IoT are distinctive ideas, but they depend on each other for ultimate success. The IoT will hugely expand the amount of data on hand for evaluation by all methods of organizations. However, there are large limitations that must be overcome earlier rather than later before expertise advantages are thoroughly realized. The IoT and big data are certainly intimately related: billions of internet-connected 'things' will, by definition, generate giant amounts of data [7].The Internet of Things (IoT), big data, and Internet of Nano Things (IoNT) are the most-talked-about technology topics in recent years [8]. The main building block of Internet of Nano things (IoNT) is nanotechnology. Nanotechnology [9] (science on the scale of single atoms and molecules) has been called the second Industrial Revolution because of the special properties of materials at the nanoscale. The IoNT involves a large number of nanosensors that used to provide more precise and detailed information about a particular object to enable a better understanding of object behavior. IoNT adds a new scale in IoT incorporating nano-sensors in the devices, which in turn allows it to connect and communicate through the nanotechnology network with internet. The IoNT is embedded with nanotechnology (a technology which is deployed in desired devices within the nanotechnology radius), which helps in seamless transmission and communication of data within a given range of operations. This vision and model has been greatly evolving with respect to the number and types of things that are being connected, and in the technologies for collecting, processing, and sharing. The IoNT infrastructure [10] allows different combinations of nano cameras, nano phones, nano things &objects, nano-sensor network technologies, and many more.

The IoNT is increasing fast, prominently improving the mighty IoT. In IoNT infrastructure, these "nano things" will realize and explore each other and learn to take advantage of each other's data by sharing resources and dramatically enhancing the scope and dependability of the resulting services. The concept of the IoNT is introduced as a type of IoT where nano-devices whose dimensions may range from 1 to 100 nm [9] are interconnected with classical networks leading to new networking paradigms. Internet of Nano Things (IoNT) communications can be structured [11] by integrating nano devices and a number of other technologies such as IoT, Sensors Network, Cloud Computing, Big data analytics etc. This new networking paradigm will have a great impact in almost every field of our society, ranging from healthcare to homeland security or environmental protection.

The rest of the paper is organized as follows: Section 2 provides the IoNT related work; about Internet of Nano Things (IoNT) presented in Section 3; Section 4 how Internet of Nano Things (IoNT) functioning; Section 5 the main reason of Internet of Nano Things (IoNT); Section 6 Internet of Nano Things (IoNT)communication network; Section 7 Internet of Nano Things (IoNT) security; Section 8 Internet of Nano Things (IoNT)market trends; Section 9 Internet of Nano Things (IoNT)applications; Section 10 open research Internet of Nano Things (IoNT)challenges and Section 11 is the conclusion.

2. Related Work

The Internet of nano things is a newly emerging technology that is arriving faster than ever and holds the promise of solving many of the world's most pressing challenges. It performs the way we connect devices in case of Internet of Things but the major difference is it can connect the nano components which is not possible with Internet of Things. Thus, it creates a state of the art revolution in electromagnetic communication areas among nano scale devices. In this section, we are discuss the Internet of Nano Things relate works. Ian F. Akyildiz et al. focuses on electromagnetic communication in nanoscale devices by drawing attention towards channel modeling, information encoding and networking protocols for nano-devices based on IoNT. The Information and Communication society (ICT) should provide some new solutions with regard to communication in nanoscale devices and nano networks [10]. A. Nayyar et al. discuss Nan machine is characterized as the fundamental useful unit incorporated by means of nano-components to perform essential tasks like detecting or inciting. Nano-machines can be additionally utilized as establishment for improvement of nano-bots, nano-processors, nano-clocks, and nano-memory. Aside from dealing with examining on different application field and improvement of Nanotechnology based IoNT gadgets , new security and protection systems should be looked into concerning the information being gathered by nano sensors[12]. The Kulakowski et al. [13] focused on Nano-communications via Forster resonance energy transfer (FRET), which was found to be a technique with a very high signal propagation speed and discussed how to route signals through Nano-networks. They introduced five new routing mechanisms, based on biological properties of specific molecules and experimentally validated one of these mechanisms. K. Agarwal et al. [14] the increase in internet users, there is need for more bandwidth. This issue can be solved by using a frequency band called as Terahertz band. It provides very large amount of channel capacity which makes massive bandwidth available for very short ranges (>1m). Ali et al. [15] outlined the different network models of Internet of Nano-things (IoNT) and the architectural requirements for implementation. They highlighted the main applications of IoNT and the significant challenges faced in implementing this technology in healthcare. They also discussed the communication and networking aspects of IoNT examining two paradigms, layer-based and non-layer-based models including the comprised layers in the layered model. Hemdan Ezz El-Din et al. [16] order to provide in-

depth knowledge about Internet of Nano Things (IoNT) and Industrial Internet of Things (IIoT) technologies, the researchers provided various fundamental concepts, architecture, communication classifications, communication issues, applications, benefits, security and future research directions. Kuscu et al. [17] provided a detailed architectural view of Nano communication focused on its fundamental principles and design requirements by surveying theoretical and experimental ideas. They gave an overview of networking opportunities offered by the intrinsic capabilities of fluorophores under the concept of Internet of Molecular Things. Bassam Al-Shargabiet al. [18] IoT operational model based on how they are interconnected and operated, the Internet Architecture Board (IAB) classifies them into IoT Device-to- Device model, IoT Device-to-Cloud model, IoT Device-to-Gateway Model, IoT Back-End-Sharing Data model. An explored analysis for the major opportunities and challenges faced in implementation of IoT technology was introduced. The growth of the Internet of Nano Things (IoNT) primarily focuses on improving processing capabilities, providing larger storage capacity at lower costs and increasing the role of communication terminals. The Yusuf Perwej et al. IoNT infrastructure can be deployed in various eco-systems such as electro-magnetic waves, RedTacton [19], Wi-Fi, Li-Fi [20], radio frequency identification (RFID) and nano antenna. Andrew Whitmore et al. [21] in this paper the present scenario of IoT, technologies supporting IoT , its applications and challenges, recent advances and development through an in-depth review has been presented. The literature was classified into six major categories: technology, applications, challenges, business models, future directions and overview & survey. Mahdi. H. Miraz et al. in this paper Internet of Things (loT), Internet of Everything (loE) and Internet of Nano Things (loNT) are briefly studied and various future applications of these technologies was also presented by authors [22]. Stelzner et al. [23] were looking at the combination of in-body Nano-communication with the Internet of Things (IoT) especially Body Area Networks (BAN) and the resulting research challenges in the Internet of Nano-Things (IoNT). Moreover, they provided a concept for Function Centric Networking presented an approach to deal with these challenges by addressing specific groups of interchangeable and replaceable Nano-machines. Several communication paradigms can be used in Nano-networks depending on the technology used to manufacture the Nano-machines and the targeted application. Josep Miquel Jornet et al. discuss the latest techniques used in the development of nano things and major research challenges in the recognition of the IoMNT [24]. The future research trends and major challenges are defined in terms of multimedia data and signal processing, propagation modeling for communication amongst nano things in the terahertz band, physical layer solutions for terahertz band communication and protocols for the IoMNT. The researchers also proposed novel medium access control techniques, addressing schemes, neighbor discovery and routing mechanisms, a novel QoS aware cross-layer communication module, and novel security solutions for the IoMNT. Falko Dressler et al. [25] examined the challenges and opportunities of connecting Body Area Networks and other outer gateways with in body nano-devices. A novel network architecture supporting the application requirements was derived and in particular simulation-based performance evaluation and security issues was also been identified. Najah Abu Ali et al. presented different network models of IoNT and the architectural requirements [26] for implementing this technology in healthcare applications such as drug delivery and disease detection. The nano networks protocol stack was categorized into two main categories, first Layer-based and second non-layer based models. And finally a comparison between the two models along with the advantages and disadvantages of both was provided.

2.1. About Internet of Nano Things (IoNT)

The Internet of Nano Things (IoNT) is a convergent point where nanotechnology, the Internet of Things (IoT) and Industry 4.0 meet. The premise of the IoNT is pretty simple; it is essentially a nanoscale version of the IoT. These areas also converge within sensors that can be used in conventional IoT systems [27], but the IoNT is the manifestation of small-scale IoT systems that is ideal solution for remote environmental monitoring and medical applications. The IoNT involves a [11] large number of nanosensors that used to provide more precise and detailed information about a particular object to enable a better understanding of object behavior.

The first concept of IoNT was proposed by Ian Akyildiz and Josep Jornet [10] a paper entitled “The Internet of Nano-Things” in 2010. Describing the term of IoNT as the interconnection of nanoscale devices with existing communication networks and ultimately the Internet defines a new networking paradigm that is further referred to as the Internet of Nano Things. IoNT is the new evolution that blends IoT with nanotechnology. The Internet of nano things is based on synthetic biology and nanotechnology tools that allow the engineering of biological embedded computing devices opportunities. Nanosensors have become one of the main research fields in nanoscience due to having effective solutions in medicine, agriculture, environment, and computing systems [28]. These nanosensors could be interconnected with the existing wireless communication systems, which can produce a new domain that is called internet of nano-things (IoNTs). Normally, nanosensors can be classified into the following types, physical (mechanical, acoustical, thermal and radiation, optical, and magnetic), chemical (atomic and molecular energies), and biological (antibody & antigen interaction, DNA interaction, enzymatic interaction). Approaches for the fabrication and integration of nanosensors shown in figure 1.

The real-time data can be used in a variety of nano-applications in the Internet of Nano-Things (IoNT), from preventive treatment to diagnostics and rehabilitation. IoNT introduces significant challenges as well as opportunities for wearable sensor-based big data analysis research. Traditional algorithms do not offer flexibility to handle such large volumes of diverse data, and this creates a need for proper mechanisms for data analysis to be able to keep up with the managing, processing, and response requirements along with the data reliability. IoNT uses two broad areas of communication firstly the Terahertz Electromagnetic Nano-Communication [29], which is regarded as transmission and receiving of electromagnetic radiation from components, and secondly the Molecular Communication, which is regarded as transmission and receiving of information encoded in molecules. IoNT infrastructure can be implemented by introducing nano devices with other popular technologies like big data, wireless sensor network, cloud computing, and grid computing.

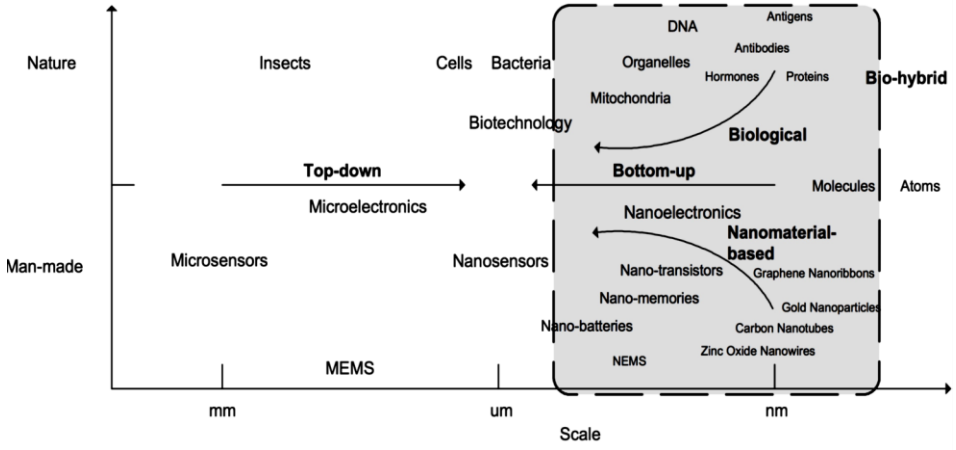

Figure 1 The Outlook for the Fabrication and Integration of Nanosensors

The interconnection of nano machines with existing communication networks such as Internet requires the development of new network architectures. The development and widespread adoption of IoNT relies on processing capabilities, large storage at low costs, smart antennas, and smart RFID tag technology. The IoNT has given birth of new domains like Internet of Bio-Nano Things (IoBNT) [8] and Internet of Multimedia-Nano Things (IoMNT) [24] which can add novel developments in healthcare and multimedia arenas. Many nanosensors have also been made from non-biological materials, such as carbon nanotubes, that can both sense and signal, acting as wireless nano antennas. Because they are so small, nanosensors can collect information from millions of different points. External devices can then integrate the data to generate incredibly detailed maps showing the slightest changes in light, vibration, electrical currents, magnetic fields, chemical concentrations and other environmental conditions. The IoNT could provide much more detailed, inexpensive, and up-to-date pictures of our cities, homes, factories even our bodies. Today traffic lights, wearables, or surveillance cameras are getting connected to the Internet [30]. Next up billions of nanosensors harvesting huge amounts of real-time information and beaming it up to the cloud. IoT with nano-machines have attracted much attention as one of the new research areas.

3. How Internet of Nano Things (IoNT) Functioning

The Nanotechnology can be combined with the IoT is in the creation of a physical network, composed of nanomaterials that facilitates the exchange of data through different components communicating with each other at the nano level. This is known as the Internet of Nano Things (IoNT) [31]. In terms of development, it is not yet at the level of other IoT systems, but it is attracting interest from the communication and medical sectors. One such example is in field-based applications, where remote sensing is required, or for measuring different points within a human body. We need to first view at the conventional IoT systems that are now being put in place to create smarter sensor networks and more automated processes. The IoT is a collective of sensors networks, data collectors, and transmitters that send data from multiple entry points through the cloud into a centralized location. This enables the IoT [2] to be self-sufficient, without the need for human interaction, unless the system alerts an operator to a problem, which it finds through its analyses. The IoNT, in essence, is a miniaturized version of these systems which employ very small sensors and data network hubs to transmit data over long distances. As it stands, IoNT systems are not as well-developed as their IoT counterparts, but their ability to gather data using such small sensor [3] points makes them useful for applications that are not compatible with other (bulkier) sensor networks. There are various components within the IoNT network which communicate with each other to transfer the data over long distances.

The any system, there are multiple components, and the IoNT [11] is no different. There are also two common ways that these components communicate with each other, and these are through electromagnetic nano-communication (transmission and receiving of electromagnetic waves) and molecular communication (information encoded in molecules). As for the components themselves, there are four main areas of the IoNT that help to facilitate the transfer of information these are nano nodes, nano-routers, nano-micro interface devices, and gateways. There are four basic components to an IoNT system shown in figure 2. These are called the nano nodes, nano-routers, nano-micro interface devices, and gateways. The smallest component is the nano node [32]. These are colloquial to sensors in conventional IoT networks [2] and are essentially basic nano machines. Because of their small size and small internal memory, the operations that they can perform are limited, as is the distance that they can transmit data. However, many nano nodes can be connected to one or more nano-routers much like where sensors transmit the localized data to a localized hub before sending the information over long distances. Nano-routers are much larger than the nano nodes, and therefore possess a much higher computational power that enables them to collect and aggregate all the data from the surrounding nano nodes and transmit this data over long distances to the nano-micro interface device. A Nano node is the simplest and smallest component within the IoNT [33] setup and is seen as a basic nano machine. These small nano machines are used to transmit data and perform basic computations. However, their small size (and energy) limits the distance that they can transmit data, and they possess a very small internal memory. Nevertheless, they can be placed in a specific location and transmit data to a larger nano-router, which then transmits the data over longer distances. Therefore, the nano nodes can often be the actual sensor component of the system. The nano nodes pass the data on to the nano-router, which is a nano machine with a much larger computational power. Because they possess a much higher computational power, they act as an aggregator for all the surrounding nano nodes that obtain the initial data. They can then control the exchange commands between the nano nodes and send the information to the nano-micro interface device. These interface devices aggregate all the data from the nano-routers and transmit the data [34] to the micro scale (and vice versa) using a combination of nano-communication techniques and classical network protocols. The gateway then acts as the controller of the whole system and enables the data to be accessed anywhere via the internet. So, the IoNT [35] does show some similarities with how IoT systems operate, but the small size of the components means that some of the hubs need to be closer together.

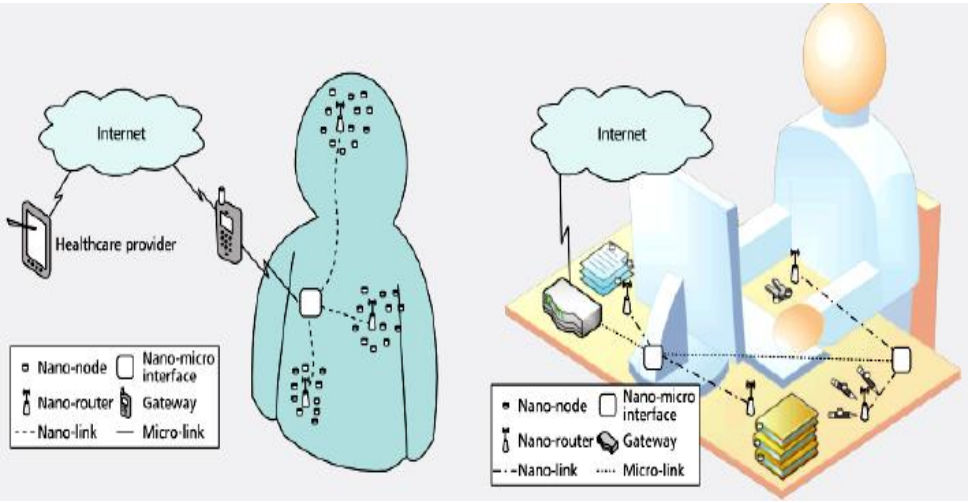

Figure 2 The Functioning of Internet of Nano Things (IoNT)

4. The Main Reason of Internet of Nano Things (IoNT)

The development of Nanotechnologies, nano machines, Internet of Nano Things (IoNT) [36] will have a great impact on advanced development in almost every field in near future. The interconnection of nanoscale devices with existing communication networks and ultimately the Internet defines a new networking paradigm that is further referred to as the Internet of Nano Things [10].

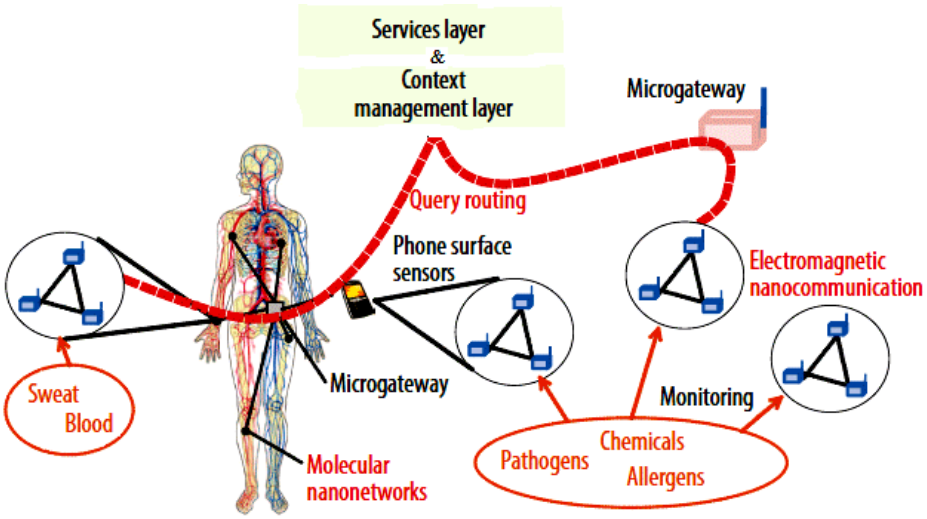

Figure 3 The Nano Communication in Internet of Nano Things

The IoNT is an extension of the Internet of everything [30], but where you have the possibility of incorporating nano-sensors in various objects and using nano-networks. That is, the reasonof IoNT consists of the capacity to interconnect diverse types of devices developed at a nano-scale in a communication network, where it allows the collection of data in places with difficult access [37]. The figure 3 show the interconnection which is established between different devices, as are nanosensors through nano-networks, with the aim provides essential information within complex-to-access areas. For example, on-body nano-sensors could provide electrocardiographic and other vital signals, while environmental nano-sensors could collect information about pathogens and allergens in a given area [35]. The term as nano-networks are not a simple extension of traditional communication networks at the nano-scale. They are a complete new communication paradigm, in which most of the communication processes are inspired by biological systems found in nature [28].

5. The Area of Internet of Nano Things (IoNT)

The Internet of Nano Things (IoNT) contains two areas firstly the Internet of the Nano-Things Multimedia (IoMNT)and secondly the Internet of the Bio-Nano Things (IoBNT) [38], also, the architecture of the nano devices can be different, depending on the capabilities that it provides nano technology. The perspective of multimedia nano-things concludes that nano components have to be integrated into a single device [39]. The interconnection of pervasively deployed multimedia nano-devices with existing communication networks and ultimately the Internet defines a truly cyber physical system which we further refer to as the Internet of Multimedia Nano-Things (IoMNT). The IoMNT is not only compliant with the envisioned applications of the IoT [40], but it also enables more advanced applications in diverse fields. In figure 4, a single device is made up of different nano components (nano cameras, nano-phones, nano-antenna, etc.). Additionally, this device must be tiny of at least a few cubic micrometers [10].

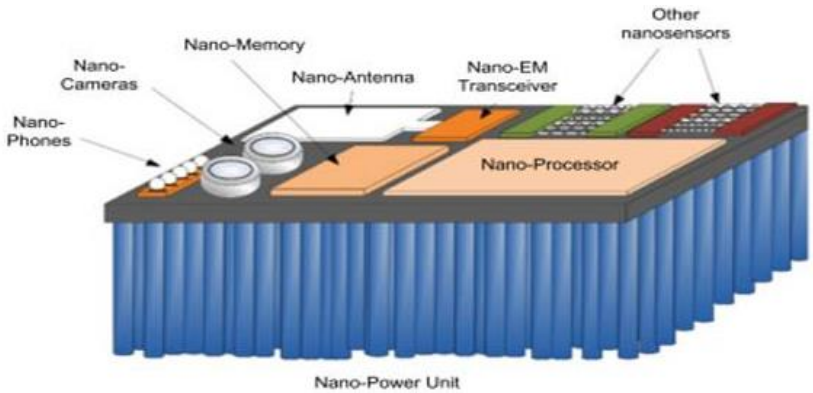

Figure 4 TheArchitecture of Multimedia Nano Things

In the Internet of the Nano Things Multimedia (IoMNT) architecture contain a Nano Cameras photo-detector designed at nano-scale which is of great importance in telecommunications. It allows the detection of signals and acquisition of optical images [41] and Nano-Phones Consist of ultrasonic transducers with nanoscale dimensions [42].In the Scalar nano sensors are able to devices of a new generation of sensors. A nano sensor is not just a tiny sensor, but a device that makes use of the novel properties of nanomaterials to identify and measure new types of events in the nanoscale and Nano processor is high performance transistors. They are smaller and can work at high frequencies. The Nano memories are indicated that these memories are not yet ready and available for the nano devices. Nano-materials [9] and new manufacturing processes are considered as the starting point for their development, using single-atom memories, where each bit of information requires only one atom and power nano systems type of batteries requires new models or techniques that allow energy storage in a very different way than conventional batteries. Again, nano antennas and nano transceivers use of nano materials has generated that many investigations can be made and with this the possibility of manufacturing nano-antennas [9].These antennas are much more compact than the traditional antennas, that is based on graphene and have the chance of working on the frequency of the Terahertz band. The capabilities of multimedia, processing, data storage, energy, of the nano devices, will not always be the same and this capacity vary according to their size [43].

The secondly the Internet of the Bio-Nano Things (IoBNT) areas has the perspective on biological structures. The Internet of the Bio-Nano Things (IoBNT) is defined as uniquely identifiable basic structural and functional units that operate and interact within the biological [8] environment [37]. The stemming from biological cells [44], and enabled by synthetic biology and nanotechnology. In nature, the exchange of information between cells is based on the synthesis, transformation, emission, propagation, and reception of molecules [9] through biochemical and physical processes [10]. Bio-Nano Things are expected to perform tasks and functionalities typical of the embedded computing devices in the IoT, such as sensing, processing, actuation, and interaction with each other. In figure 5 shows how the comparison of elements by a biological cell [44] with the features or components that make up an electronic device is carried out [8]. For instance, nucleus of the cell with the control unit and the cytoplasm with the memory. In the Internet of the Bio-Nano Things (IoBNT) architecture the Control Unit can be considered as the control unit of the cell [28]. The genetic instructions are those that are packaged in the DNA molecules of the cells [37] and memory unit contains the values of the embedded system data, would correspond to the chemical content of the cytoplasm, i.e. the interior of the cell [44], comprised of molecules synthesized by the cell as a result of DNA instructions [37].In the processing unit concerns the molecular machinery that, rough DNA molecules, generates other molecules with types and concentrations dependent on the instructions are given[8] and Power Unit corresponds to the deposit in the cell of the molecule Adenosine Triphosphate (ATP), which is synthesized by the cell from energy provided by an external environment and provides power so that the biochemical reactions of the cell can be generated [37].Again, transceivers are falls on the chains of chemical reactions, through these the cells [9] exchange information molecules as well as sensing and actuation consist of the ability of the cell to recognize external molecules or physical stimuli [37].

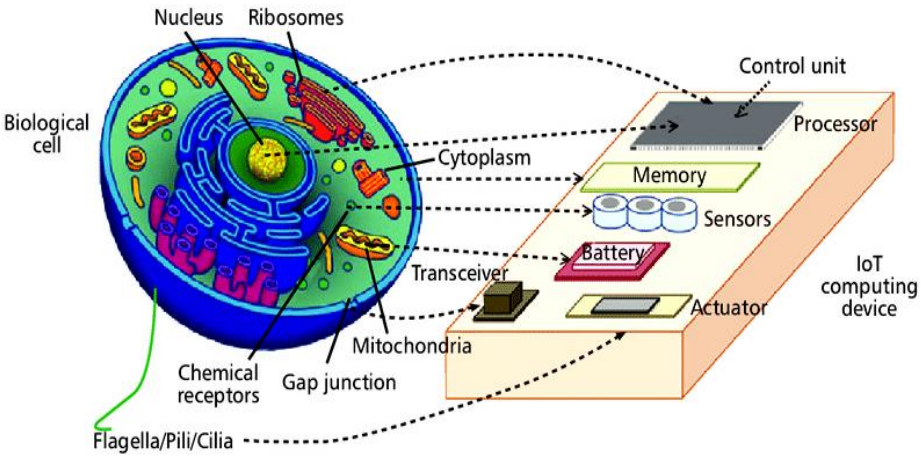

Figure 5 TheConceptual Elements of a Biological Cell and IoT Components

6. Internet of Nano Things (IoNT) Communication Network

The Internet of Nano Things (IoNT)is defined as an interconnection of nanoscale devices with the current communication technologies and the Internet [45]. The IoNT should be capable of interconnecting billions of nanosensors and nano devices through the Internet, interacting with each other in a distributed manner. Terahertz

(THz) band communication is utilized through new developments in areas such as spectrum management and antenna design to obtain data from various objects [46]. The IoNT paradigm is characterized by a very large number of nano devices, technologies, and protocols. It is really important to take into account various properties for the IoNT, namely availability, scalability, interoperability, flexibility, and reliability. The IoNT defines a paradigm where all types of nano devices (e.g. nanosensors, nano actuators, etc.) are connected to the nano networks and are able to interact with each other in real time. In nano networks, the gateway [47] must integrate data from different nano devices (e.g. nano sensors). However, due to the timing difference in data propagation between nano sensors, this can lead to long delays for data before reaching the sink node. Therefore, a time-delayed data fusion method should be applied at the gateway for the processing of data before they are transmitted over the Internet.

6.1. Conventional Communication vs Molecular Communication

In conventional communication, the information is encoded in electromagnetic, acoustic, or optical signals. But in nano-network based on molecular communication, the information is encoded by means of molecules. The propagation speed of signal in conventional communication is much faster than the propagation speed of molecules in molecular nano-networks. In molecular communication, the information molecules physically move from the transmitter to the receiver, therefore, the environmental condition such as temperature can affect the propagation of the information molecules. The noise in conventional communication is additive noise, which is defined as an undesired signal overlapped with the information signals. But there are only two types of noise in molecular communication. First, it is additive noise that also occurs in conventional communication. This means another source release same molecules which are used to encode the message, therefore, the receiver may sense an incorrect concentration level. The second noise is undesired interaction occurring between information molecules and environmental molecules such as medium molecules. The conventional communication can transmit the text, voice, and video over medium but in molecular communication, the message is a molecule. There are chemical processes in molecular communication. Therefore, their power consumption is low, while conventional communication consumes electrical power for their communication processes [28] that is obtained from internal or external sources such as batteries or electro-magnetic induction

6.2. Communication Models in Internet of Nano Things (IoNT)

The communication in nanoscale can be classified in molecular communication and nano electromagnetic communication [48]. The molecular communication is defined as the transmission and reception of information encoded in molecules, while transmission and reception of electromagnetic (EM) radiation from components based on nanomaterials defines nano-electromagnetic communication. It is of great importance to study the communication nature in very short range, since it is functioning at the nanoscale. In the IoNT communication paradigm, the routing protocol should be coupled to the MAC layer through a cross-layer design [2]. The residual energy and current load of the IoNT nodes will be utilized to identify and bypass critical links. Therefore, the network lifetime can be effectively prolonged by preserving residual energy and increasing network throughput, which can be achieved through load balancing.

Traditional nano networks spend energy in almost all processes. They spend energy while making data transmissions and data sensing as well as data processing. There have been a few attempts toward [49] achieving energy efficiency in such networks via wireless multi-hop networking such as and [50]. However, such schemes are only applicable in static wireless networks and are impractical in multi-hop nanoscale wireless networks with random topologies. Routing algorithms for the IoNT can be classified to cluster-based algorithms vs. cognitive-based algorithms. In the cluster-based algorithms packet transmission from the source to the cluster-head or nano controller can be direct or multi-hop based on the probability of saving energy through transmission, optimizing throughput, and minimizing nanosensors' load. In the cognitive-based algorithms [51] was proposed for data delivery in nanoscale networks where nano routers forward the collected data to cognitive relay nodes for acting and making decisions based on the network conditions.

6.3. The Forming of Network Connections of Various Nano Scale Devices

In this section, we are discussing thepreliminary ideas for the forming of network connections of various nano scale devices. In channel sharing develop impulse-based communications [36]. We think of asynchronous MAC protocols, in which a nano node willing to send a packet can just transmit it and wait for some type of acknowledgment. The implement addressing schemes that capture and exploit the hierarchy of the network. Investigate strategies for the discovery of neighbours that exploit the high directivity of the terahertz antennas to determine the relative location and orientation between the nano-objects simultaneously [39]. A communication system based on impulses must be defined and assume that the nano-nodes know the distance between them. For example, different nodes at the same distance from the nano-router will have the same ID. The neighbours of these nodes, who might not have heard the nano-router, will take a higher ID and broadcast it. Therefore, other nodes will have higher IDs. [29]. a hierarchical network structure,

it is not necessary to notify the entire network of the existence of a new nano node; it would only be required to inform the nearest nano-router or nano-micro interface [29]. End-to-end reliability in nano networks and the IoNT has to be guaranteed both for the messages going from a remote command centre to the nano- nodes, as well as for the packets coming from the nano machines to a common sink [29].

6.4. The Nanoscale Communication Challenges

The Internet of Nano-Things requires redesign and develops new communication paradigms, and networking concepts that will be compatible for nanoscale machines. Many communication challenges appear in the physical layer of nano machines to the nano networking protocols. In this sectionwe are discussing themain challenges from communication respective [10]. In the channel modelling terahertz band spans the frequencies between 100 GHz and 10 THz is still unlicensed band. It has major limitations for short and medium range communications [52], but it is applicable for nano network applications as discussed aforementioned, therefore the channel modelling for this band in the very short range should be investigated. The Jornet et al. investigates the properties of the Terahertz band in terms of path-loss, noise, and bandwidth and channel capacity as described below [53]. The absorption loss depends on the type of the molecules and its concentration along the path. Different resonance frequency associated to different types of molecules where the absorption at each resonance spreads over a range of frequencies. As a consequence, the Terahertz channel will suffer from high frequency selectivity, multi-path propagation, and scattering from the nano particles in the field which affect the signal strength at the receiver. The main source of the ambient noise in the Terahertz band is the molecular noise. The molecular absorption introduces noise along with the attenuation. This type of noise occurs only when transmitting signal through the channel. Additionally, equivalent noise temperature is introduced around the frequencies where the molecular absorption is considered high. The molecular absorption determines the transmission bandwidth in terahertz channel. Therefore, the molecular composition of the medium and the total transmission path constrain the available bandwidth [54]. The available bandwidth for a very short range is ranging from a few hundreds of gigahertz to almost ten Terahertz (almost the entire band).Therefore, the channel capacity of electromagnetic nano networks in the Terahertz band is predicted to be in the order of a few terabits per second.

7. Internet of Nano Things (IoNT) Security

Internet of Nano Things is being incorporated into most applications of our life such as phones, household appliances, sensors, vehicles, and large-scale infrastructure systems. These devices have their control and monitoring procedures digitized and connected to the Internet, which raises many security and privacy issues [55].The integration of Body Area Networks systems within body devices and nano machines also creates a completely new level of security related challenges. One of the most important challenges as a result of the growth of the Internet of Nano Things market is related to the security of data communicated over the Internet. For example, in the healthcare domain, a bio-cyber-attack can steal people's personal health related information. This information can be used to create new types of viruses to hack into already-deployed nanosensors in the Internet of Nano Things. Therefore, security assurance methods should be applied to communication networks in the 4 G and 5G era, especially in the Internet of Nano Things, in order to prevent such problems, considering the nature of Internet of Nano Things communications carefully. The Internet of Nano Things is vulnerable to all types of attacks, either physical or through wireless technologies, given that this type of device does not meet with constant vigilance [56].The attacks can occur to acquire private data through the theft of sensors, interrupt applications controlled utilizing computers, or modify the communication links in the nano-networks. This is because standard security techniques cannot be applied to nano networks that operate in the terahertz band. To secure the IoNT system, there is a need to develop new security solutions [57]. The author proposed [56] new security methods among nano-communications, especially the connections between Internet of Nano Things and Internet of Nano Things. These security aspects mentioned are nano communication security, security objectives, and security mechanisms for IoNT systems. The security objectives are a series of concepts that guarantee the security of communication systems. They are made up of confidentiality, integrity, and availability. When combining nano communication devices with IoT, we are facing typical sensor network security issues. The range for an attacker, especially gateway nodes and the integration of smart phones [58] opens up completely new attack vectors. Furthermore, the use of these networks for collecting very private information ranging from location information to physiological data makes these networks a valuable target for malicious users. Therefore, new security and privacy techniques are required to protect sensitive data collected by nanosensors.

7.1. Internet of Nano Things (IoNT) Security Aim

In this section evaluating the security of Internet of Nano Things systems, we need to start with a classical security and risk analysis. Further-more, novel and emerging challenges in the nano communication domain [59] as well as related to the coupling of In-Body Networks with external devices is necessary. Firstly assess the estimate CIA (Availability, Integrity, and Confidentiality) security aims in these new circumstances [60].

7.1.1. Availability

A malicious user must not be capable of disrupting or harmfully affecting communication or quality of service provided by either nano devices or nano networks. In the Internet of Nano Things scenario, availability of the BAN network, in-body nano communication network, and gateway nodes should be maintained under all situations and conditions. Adaptive self organizing solutions are needed to handle this issue.

7.1.2. Integrity

The content of messages exchanged between a sender and a receiver should be protected against modification by an intruder without the receiver being able to track this modification [56]. In the Internet of Nano Things system, integrity checks need to be applied not only on BAN nodes but also on the nano devices and micro gateway. The integrity checks can be carried out at each node involved in the message exchange between the originator and the receiver [61].

7.1.3. Confidentiality

An attacker should not be able to access the content of messages exchanged between a sender and a receiver. In our context, this means that confidentiality need not only be ensured within the Body Area Network, e.g., using encryption techniques such as the well known AES or RSA algorithms [62], and within the In-Body Nano Communication network, e.g., relying on biochemical cryptography, but primarily also when relaying messages using a gateway system interconnecting both worlds. As usual, security helper functionality is needed starting with cryptographic techniques for encryption and digital signatures but also for authentication as a base functionality.

7.2. Invasion Vectors in Internet of Nano Things (IoNT)

An invasion vector is a path or means by which an attacker can gain unauthorized access to a computer or network to deliver a payload or malicious outcome. Attack vectors allow attackers to exploit system vulnerabilities, install different types of malware, and launch cyber attacks. Attack vectors can also be exploited to gain access to sensitive data, personally identifiable information (PII) and other sensitive information that would result in a data breach. It tries to exploit the vulnerabilities in a device or a network [63].There are several invasion vectors associated with the Internet of Nano Things system that need to be handled by implementing the required security measures to reduce against.

7.2.1. Internet Exposure

In spite of the fact that connecting nano devices to the Internet helps to share information with each other and allow real-time applications, any device which connects to the Internet and accepts incoming traffic eventually comes under attack. Unlike the network server where a firewall can control how the host can be accessed, nano devices are employed with limited computation capabilities and memory and without built in security features that make it an easy target to various attacks coming from different locations over the Internet.

7.2.2. Lack of Encryption

Unluckily, security is often an afterthought in the development lifecycle of Internet of Nano Things devices. Encryption is missing from most nano devices due to their small size and limited computation capabilities. Failure to encrypt sensitive data exchanged between nano devices, whether on nano device itself or on nano networks will lead to several security issues especially when nano devices become part of our bodies. Embedded cryptography such as crypto graphic co-processors, which can address encryption and authentication of nano devices, is required and securing data of nano devices should be part of any design.

7.2.3. Wearable Malware

There is a rapid growth of wearable devices in different fields [64]. These devices include smart glasses and headgear, fitness trackers, wearable medical devices, smart watches, and smart clothing and accessories. Wearable's devices might become attractive targets for malicious software especially they use Bluetooth [65], which uses frequency hopping whereby many devices can transmit a signal across the same frequency at the same time [66]. This increases the chances of signal interception by attackers and theft of sensitive information from these unencrypted feeds.

7.2.4. Denial-of-service

A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. This is defined as any event that diminishes or eliminates the capacity of a network to perform its expected function [67]. An attacker tries to affect

the availability of a network that might be difficult to protect, as attackers might have sufficient energy to jam radio transmission or flood the communication channel with large amounts of molecules that destroy regular communication molecules.

7.3. Internet of Nano Things (IoNT) Security Mechanisms

In this section, we are discussing the how to increase the security of IoT systems as well as we are consider the following mechanisms to establish secure communications in nano sensor networks.

7.3.1. Key Management

The establishment of symmetric keys is called key management [68]. Distributing security keys is considered to be the root of nearly all key management systems. Keys can be distributed either by key pre-distribution before the deployment or pro-active in a sensor network before any data transmission occurs. It is essential to have the ability to revoke a key when it has been disclosed [65]. This issue is still one of the most challenging issues in sensor networks and IoNT systems. It is necessary to define standard procedures to create shared keys and define how keys can be revoked when necessary.

7.3.2. Cryptographic Primitives

In the scope of Body Area Networks, we can rely on classical cryptographic solutions such as using the symmetric AES or the asymmetric RSA algorithms. For in Body Nano Communication, however, we need more lightweight solutions such as the biochemical cryptography proposed [69].

7.3.3. Access Control and Authentication

Authentication is a prerequisite to guarantee the objective of confidentiality. Each of the messages that want to be sent to a nano-communication system must go through a gateway and be authenticated. Authentication is typically achieved using traditional symmetric or asymmetric cryptography. Biochemical cryptography is a new and still unexplored field which uses biological molecules like DNA/RNA evidence to encrypt information and protect the confidentiality and integrity of data [70]. Although this cryptography scheme opens various novel application domains, it leads to new issues related to the communication system. The complex molecules can spontaneously respond within the system which results in modifications out of the control of the nano machinery. Therefore, the biochemical processes involved in the system need to be better understood.

7.3.4. Secure Localization

In IoNT, many of the applications will need to know the location of the nano-sensors to perform specific jobs. Some applications that use nano communication need the localization of nano machines to complete their operations. The difference in demands between classical sensor networks, using other coordinate systems, and nano devices make generating an absolute positioning with nanoscale resolution difficult to realize, but relative positioning might be more relevant. This links directly to security to permit only nearby nano machines to communicate and prevent remote attackers from interfering [71].

7.3.5. Intrusion Detection

Due to some problems that classical cryptography methods could present, it is essential to make the necessary arrangements to detect and react to attacks. In indicated that a strategy to counteract a denial of service attacks consists of implementing an intrusion detection system in the entry node to the nano-communication system and that it is fail-safe. Some attacks typically cannot be handled by cryptography. For instance, denial-of-service attacks that try to disrupt the availability of a system might be difficult to protect against in a nano communication network. This is because attackers might have the necessary energy to jam radio transmission or flood the communication channel with huge amounts of molecules that destroy regular communication molecules. An intrusion detection system can be used to handle this issue by detecting the attack and trigger the system to go into a fail-safe mode [72]. Therefore, it is critical to establish new intrusion detection systems that are able to detect and react to attacks efficiently in nano networks.

7.3.6. Performance and Scalability

Last but not least, the resulting system performance is an important aspect to be considered. The security and privacy in the nano-communication systems present significant challenges regarding the performance and scalability of the participating nodes. IoNT securities will create enormous performance and scalability issues. There will be severe resource limitations in nano machines that make nano communication which is unmatched in current communication

systems. Although the performance of cryptographic algorithms has been assessed in the sensor network, these results cannot be directly applied to the nano domain due to different procedures of information processing [70]. In addition, energy consumption is another serious issue since communication systems like nano-tube based radios require significant power because of the cryptographic payloads they create [72]. Therefore, the performance of communication protocols and cryptographic techniques should be taken into consideration when developing practical applications.

8. Internet of Nano Things (IoNT) Market Trends

The global internet of nano things market can be characterized by the relatively new series of nano-scale devices and the systems that are built using them. His global internet of nano things market thus implies a market dedicated to providing interconnectivity between nano-scale systems for better data direction, collection, and processing. This also allows a smoother transition for sharing the data with the various end users. Current uses of the global internet of nano things market include those in the industries of retail, media and entertainment, energy and utilities, transportation and logistics, manufacturing, and healthcare. The IoNT comprises of nano scale network of different physical objects that exchange information among each other using nano communication. As per the recent research, IoNT market is expected to grow from around USD 5 billion in 2016 to USD 10 billion by 2020shown in figure 6, at an estimated rate of more than 24.12% for the current forecast period of 2016 to 2025 [73].IoNT infrastructure can get deployed by mixing of nano devices and several other technologies like IoT, sensors network, cloud computing, and big data analytics among others. The IoNT infrastructure depends on the area of operation and required bandwidth required by specific application. The enhancement and adoption of IoNT depends on processing capabilities, large storage at low costs, and smart RFID tag technology.

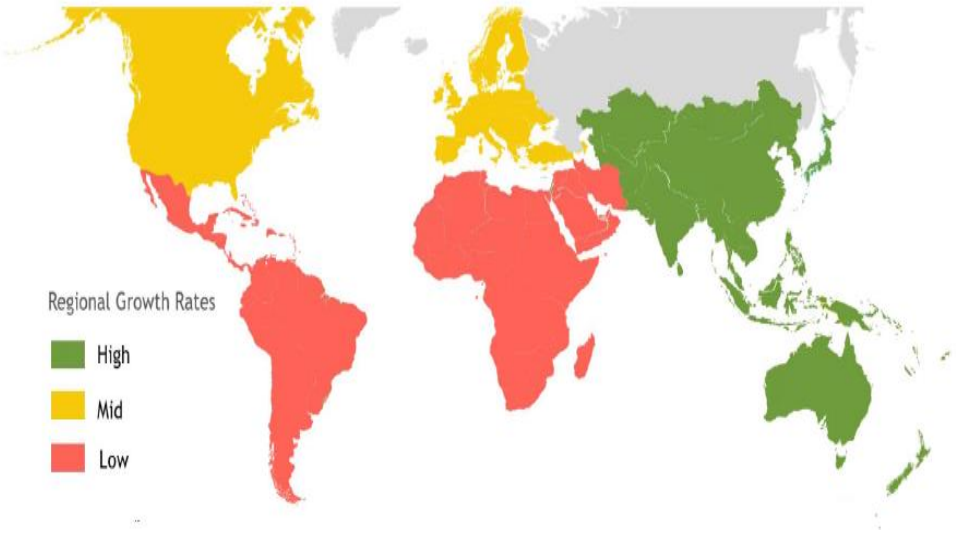

Figure 6 The Market Growth Rate Internet of Nano Things (IoNT) by Region (2020 - 2025)

A primary driver concerning the global internet of nano things market is the growing rate of demand for ubiquitous connectivity. As the number of connected devices and computer devices increase, the need for better interconnectivity drives the internet of things concept and consequently, the IoNT market. The global internet of nano things market has allowed companies to greatly improve their rate of data transfer between systems and to lower the level of complexity within different communications systems. Moreover, government's support for the development of IoNT technology for healthcare has further increased the demand and awareness of IoNT [61]. However, the growth of the IoNT market faces a few challenges due to privacy and security issues. Since critical data is communicated between devices over the internet, concerns related to security of the data have risen. Another factor which hinders the growth of IoNT market is the huge capital investment required for the development of nano technology. The players associated with the global internet of nano things are likely to be focused in regions that hold a greater scope of use of IoT and IoNT, i.e. developed economies from North America and Europe. A greater contingency of players in the global IoNT market are present in these regions, while developing economies have only been showing greater interest in the market in very recent times. Immense growth opportunities of the IoNT market have been identified through its applications in various sectors such as healthcare, transportation, logistics, manufacturing, media, entertainment, and retail. With technological advancements in the IoNT, the scope of IoNT and its applications is [35] on the rise. Major companies are conducting research on nanotechnology and constantly developing nano systems with wider scope of applications. Some of the

major players in the IoNT market are Intel Corporation, Cisco Systems Inc., Qualcomm Incorporated, Juniper Networks, and IBM Corporation in U.S., Schneider Electric, and Alcatel-Lucent S.A. in France, and SAP S.E. and Siemens AG in Germany among others.

9. Internet of Nano Things (IoNT) Applications

There is no doubt that Internet of Nano Things (IoNT)will make a gigantic impact on the nanotechnology businesses. The possibilities offered by the new techniques for the collection of fine-grained information by IoNT allow to increase the existing applications and to venture into new fields in contrast with IoT [74]. Internet of Nano things has countless applications such as Oil and Gas, Armed, Farming, Smart Cities, Healthcare and many more etc. In this section, we are discussing the various applications of IoNT which can improve the nanotechnology benefits in many fields [75].

9.1. Fertilizers and Pesticides Delivery in Agriculture

Nano technology has the potential to bring important changes in agricultural industry. Some of these challenges include the increasing threats to agricultural production and risks of plant related diseases. The agricultural sector will benefit greatly from Nano-technology tools to detect diseases in a rapid manner, improve the ability of plants to absorb nutrients and promote molecular treatment of diseases.

9.2. Drug Delivery Systems

Nano devices in Internet of Bio-Nano Things (IoBNT) can be used as regulator implants that could compensate metabolism diseases such as diabetes. Smart glucose reservoirs and nanosensors collaborate to support the glucose level mechanisms. The effects of neurodegenerative diseases can be eliminated using drug delivery system to deliver neuro transmitters or specific drugs to neurosystem [76].

9.3. Environmental Monitoring

Nano sensors are used in environmental monitoring through deployment in public locations like bus stops, airports, hotels, etc. and real time monitoring of traffic and temperature. In smart factories or farms, nano devices could monitor temperature, humidity, and air quality. IoNT used in precision farming applications leading to efficient environment monitoring, crop growth and even animal monitoring. It is being used to monitor and track the farm animals.

9.4. Smart Cities

Implementation of a smart city provides an interaction and communication with the home appliances, monitoring sensors, observation cameras, actuators, buses, cars, and others. The roadmap for the smart urban is contingent on topographical surroundings and persons routines. The communication technologies can be used by anyone, regardless of their financial situations. Execution of smart cities has previously been done with the assist of Internet of Things. We can use nano sensor to monitor and recognize the location of litter discovered in the air in high absorption and trigger nano sensors to clean up that exact position. Moreover, with the assist of the innumerable amount of nano sensors, we can use to collect an enormous quantity of information in real time to improve the quality of life and offer new facilities and applications [77].

9.5. Animals and Biodiversity Control

Several animal species can be controlled by nano networks in natural environments. Nano networks could develop pheromones or messages to trigger certain animal's behaviors. Therefore, controlling the location of certain animal species in particular environment would be possible.

9.6. High Speed Data Transfer & Cellular

In telecommunication domain, IoNT incorporated electromagnetic wave nature properties for Pico and Fem to cells based networking over Terahertz band (0.1THz –10THz), for correspondence among sensors. Due to matters of fact that, THz based frequencies have higher capacity and transmission rate available, it can exchange rapid information and can be made conceivable by incorporating Nano gadgets in the cutting edge cell systems and military related applications [78].

9.7. Biomedical applications

The nanoscale is the natural domain of molecules, proteins, DNA, organelles and the major components of living cells. As a result, a very large number of applications of nano networks is in the biomedical field. For example, nano material-

based biological nanosensors [79] can be deployed over (*e.g.*, tattoo-like) or even inside the human body (*e.g.*, a pill or intramuscular injection) to monitor glucose, sodium, and cholesterol, to detect the presence of infectious agents [80], or to identify specific types of cancer. A wireless interface between these nano machines and a micro device, such as a cell phone or medical equipment, could be used to collect data and to forward it to a healthcare provider. Better health monitoring and treatment frameworks which consolidate chemical and biological nanosensors, nano cameras with extremely high-resolution powers and ultrasonic nano phones for catching diseases like cancer in their initial phases and treatment of various other ailments. Another example is that of parents who wish to keep a check on their child's addictive drug use. They can do so by installing particular nanosensors inside the body of their child. These sensors will provide valuable objective data regarding the time and contexts of drug use. Nanosensors are better in this situation because visible range sensors deployed outside bodies could be taken off.

9.8. Functionalized Materials and Fabrics

New advanced materials and fabrics can be manufactured by using nano networks in order to improve certain functionalities. There are developed products such as antimicrobial and stain-repeller textiles using nano functionalized materials [81]. Nano actuators communicate with nanosensors in order to control the reaction which will improve the airflow in advanced smart fabric.

9.9. Oil and Gas

By using the nano sensor we can increase the repossession rate of the oil. Nano sensor can travel through the holes of the rock and benefit us to discover the oil bounded to the rocks. However, there is a cross well imaging and seismic tool which has more impact to this area, but the firmness provided by them is very low. In Internet of Nano things, nano sensor cooperates and interconnects with each other by molecular communication. Furthermore, the collection of information can be transported in actual time using the neighboring gateway. Due to which the oil position can be efficiently plotted without needing an exact magnetic source and receiver.

9.10. Industrial and Consumer Goods Applications

The applications of nanotechnology in the development of new industrial and consumer goods range from flexible and stretchable electronic devices [82] to new functionalized nanomaterials for self cleaning anti-microbial textiles. In addition, the integration of nano machines with communication capabilities in every single object will allow the interconnection of almost everything in our daily life, from cooking utensils to every element in our working place.

9.11. Multimedia

It focuses on the construction of devices such as photo-detectors and acoustic nano-transducers to produce multimedia content with high Resolution [83]. The nano-multimedia systems have their focus in various fields such as health, biological attacks, forensic science, and industrial process control. Increasing resolution and accuracy of visual and acoustic information is not an easy task, but with nano-cameras and nano-phones, this issue can be handled by enabling higher computational and storing capacities, higher quality image and audio sensing capabilities, and higher energy efficiency

9.12. Military and Defense Applications

Advanced nuclear, biological and chemical (NBC) defenses, and sophisticated damage detection systems for civil structures, soldiers' armor and military vehicles, are two examples of the military applications enabled by nano networks. For example, a network of nanosensors can be used to detect harmful chemicals and biological weapons with unprecedented accuracy and timeliness, in very different scenarios, from the battle-field (*e.g.*, deployed from an unmanned vehicle and imperceptible by the human eye) to airport lobbies or a conference room (*e.g.*, contained within the wall paint.

9.13. Food Packaging

About intelligent packaging the exploration in nanotechnology field has risen steeply over the previous period and there are several corporations which are focusing in the creation of new forms of nano sized substance. However, one industry which is flow to catch on to this is the food industry and this is not surprising as the public reference for natural food products has historically inhibited the implementation of emerging food technologies and indisputably the most active area of food nano science investigation and expansion is wrapping. After introducing nano material compounds like SiO_2, TiO_2 and $KMnO_4$ the food packaging sealing can be enhanced greatly.

9.14. Body Sensor Network (BSN)

This comprises of in body nano sensors playing a crucial role in collecting and monitoring patient's biological activities. The nano sensors being used in BSN to provide real time data on a wearable device. They can be placed in the body and a gateway to communicate with Internet.

9.15. Immune system support

IoBNT can be utilized to support the immune system to identify and control foreign and pathogen elements in the human body. Several nano devices such as sensors and actuators collaborate with each other in macro, micro, and nano systems to protect organism against diseases. Implementing nano devices can advance the medical field by utilizing theses nano devices to predict, detect, and eliminate certain procedures based on localization of malicious agents and cells, such as cancer cells [84]. This will minimize the risk of developing such disease and provide treatments less aggressive and invasive compared to the existing ones.

10. Open Research Internet of Nano Things (IoNT) Challenges

The Internet of Nano Things technology can face the many challenges during implementation. The first important challenge nano devices collect large volumes of confidential data, concerns regarding privacy and security need to be addressed. Users of Internet of Nano Things infrastructure need to be informed regarding who has access to their data and how their data will be used. Also, the collected data needs to be stored in a secure location with encryption and state-of-the-art cyber security protocols. If left unsecured, cyber criminals can illegally access this confidential data. In the case of a cyber-security attack, users may want to know who could be held responsible and which mitigation strategies can be executed. Hence, IoNT developers need to consider these issues before the mass production and utilization of IoNT devices.

There are still many challenges and open research issues that need to be taken into account regarding the performance improvements of the IoNT. One of them is terahertz band channel modeling. The IoNT needs to transmit very large amounts of data in a timely and reliable manner. Therefore, the impact of molecular absorption on the path loss and noise should be accurately analyzed. This will help to locate the best transmission window in terms of achievable information rates and channel capacity. Moreover, the impact of multi-path propagation on the capacity and achievable information rates should be accurately investigated. Nano-devices addressing scheme as Nano-devices have limited energy and computational processing, addresses with reasonable size are needed to consume less processing power. Moreover, the address domain shall be adequate to support the expected enormous number of fabricated Nano-machines. IPv4 provides 32-bit address space of four billion addresses; however it is not even enough to give each person on earth a unique identifier. By addressing Internet of things usingIPv6 concept, there is no need to fear that there will not be enough IP addresses for things. IPv6 is providing 128-bit addresses, this makes the address needs of IoNT will be sufficient. The real question is whether ''everything'' needs its own IP address. The answer of this question is no, because in today's Internet, things are mostly servers and switches, firewalls, routers, laptops, phones and tablets with IP to IP connectivity. When we start talking about refrigerators, clothing, thermostats, light bulbs and Nano devices & machines, they do not need to be directly on the Internet with an IP address [85].Another important challenge is related to the MAC protocol. The terahertz band supports very high bit rates and has a specific relation between the available transmission window, the bandwidth for each window, and the transmission distance. Therefore, research into transmission schemes would be beneficial in order to develop novel transmission techniques using the relation between the transmission bandwidth and the transmission distance. The MAC protocol should also guarantee that the transmitter and receiver are properly aligned before the transmission of the data packet.

The compatibility is a major challenge in developing medical nano sensors. Developers have to ensure that these nano sensors will not have any side effects on a patient's body as well as support uninterrupted connectivity with wearable devices. For this purpose, designers and developers may have to find and research a wide range of materials that can be compatible with the human body. However, finding such materials will require extensive testing, making the entire process time-consuming as well as error-prone. Nano-network system scalability is the capability of a system to handle a growing number of tasks. A system is considered to be scalable, if it is capable of increasing its total output under an increased load when resources are added. A Nano-network system is considered scalable, when its performance improves after adding additional Nano devices with additional computational functions. A Nano-network system will be suitably efficient and practical, when it applied to large situations (e.g., a large input data set, a large number of outputs or a large number of participating Nano-machines &devices). If the system fails when a quantity increases, it will not be a scalable system. Fully integration between Nano-machines has not been built to date. As a result, many of the developed solutions cannot be experimentally validated. However, very advanced emulation tools are available for the partial validation of analytical models [86].Nano-network system computational complexity theory introduces a

mathematical model of computation to study the problems of a Nano-network system and quantify the amount of resources needed to solve them such as time, storage, and the amount of communication. More precisely, computational complexity theory tries to classify problems that can or cannot be solved with appropriately restricted resources

11. Conclusion

The current development of communication devices and wireless network technologies continues to advance the new era of the Internet and telecommunications. The various "things", which include not only communication devices, but also every other physical object on the planet, are also going to be connected to the Internet, and controlled through wireless networks. The Internet of Nano Things (IoNT) paradigm will take IoT to a new level, where devices that will be connected to the Internet will be focused on nano devices that are constructed from nanomaterials and components. These nano devices will communicate to a micro-device, which in turn communicates to the Internet. Currently the scientists have started shrinking sensors from millimeters or microns in size to the nanometer scale, small enough to circulate within living bodies and to mix directly into construction materials. This is a crucial first step toward an Internet of Nano Things (IoNT) that could take medicine, energy efficiency and many other sectors to a whole new dimension. The combination of nano sensors and nano devices with Internet have form the forum for the development of next modernization regular that deals with various types of data, supports high speed of communication from heterogeneous network such as Nano link, Nano micro interface and Body Sensor Network, which leads to "Internet of Nano Things" (IoNT). The main purpose of this paper was to provide an overview of the Internet of Nano Things (IoNT) system by highlighting its communication types and network architecture, and ccommunications challenges as well as various applications and challenges of the IoNT system have discussed. We have also investigated the Internet of Nano Things (IoNT) security mechanisms, invasion vectors in Internet of Nano Things (IoNT), security aim. The evolution of Nanotechnologies and Internet of Nano things (IoNT) is expected to have immense impact on advanced development in every field.

Compliance with ethical standards

Acknowledgments

This research paper is made possible through the assistance and support from almost everyone. The author would like to thank the reviewers anonymous for their constructive comments. First and foremost, we would like to thank GOD for his unconditional guidance and wisdom as we do my research. Finally, we would like to thank my colleagues for his more support and encouragement for giving us this research.

Disclosure of conflict of interest

All authors declare that there is no conflict of interest regarding the publication of this paper.

References

[1] Yusuf Perwej, Majzoob K. Omer, Osama E. Sheta, Hani Ali M. Harb, Mohmed S. Adrees, "The Future of Internet of Things (IoT) and Its Empowering Technology", International Journal of Engineering Science and Computing (IJESC), 2019; ISSN : 2321- 3361:Volume 9, Issue No.3:Pages 20192– 20203.

[2] Yusuf Perwej, Kashiful Haq, Firoj Parwej, M. M. Mohamed Hassan, "The Internet of Things (IoT) and its Application Domains", International Journal of Computer Applications (IJCA), USA, 2019; Vol. 182, No.49:PP. 36-49. DOI: 10.5120/ijca2019918763

[3] Yusuf Perwej, Firoj Parwej, Mumdouh Mirghani Mohamed Hassan, Nikhat Akhtar, "The Internet-of-Things (IoT) Security: A Technological Perspective and Review", International Journal of Scientific Research in Computer Science Engineering and Information Technology (IJSRCSEIT), 2019; Volume 5, Issue 1: Pages 462-482. DOI: 10.32628/CSEIT195193

[4] Yusuf Perwej, "An Experiential Study of the Big Data," International Transaction of Electrical and Computer Engineers System (ITECES), USA, ISSN (Print): 2373-1273 ISSN (Online): 2373-1281, Science and Education Publishing March 2017; Vol. 4, No. 1:page 14-25, DOI: 10.12691/iteces-4-1-3

[5] Nikhat Akhtar, Firoj Parwej, Yusuf Perwej, "A Perusal of Big Data Classification and Hadoop Technology," International Transaction of Electrical and Computer Engineers System (ITECES), USA, ISSN (Print): 2373-1273 ISSN (Online): 2373-1281, May 2017; Vol. 4, No. 1:page 26-38, DOI:10.12691/iteces-4-1-4

[6] Yusuf Perwej, "The Hadoop Security in Big Data: A Technological Viewpoint and Analysis", International Journal of Scientific Research in Computer Science and Engineering (IJSRCSE), 2019; Vol. 7, Issue 3: Pages 1- 14. DOI:10.26438/ijsrcse/v7i3.1014

[7] Firoj Parwej, Nikhat Akhtar, Yusuf Perwej, "A Close-Up View About Spark in Big Data Jurisdiction", International Journal of Engineering Research and Application (IJERA), 2018; Vol. 8, Issue 1:(Part -I1):Page 26-41. DOI: 10.9790/9622-0801022641

[8] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, "The internet of bio-nano things," IEEE Commun. Mag., 2015; vol. 53, no. 3:pp. 32–40.

[9] Nazia Tabassum, "An Empirical Exploration of the Nanotechnology", International Journal of Advanced Research (IJAR), ISSN 2320-5407,July 2020;Volume 8, Issue 7:Page 885-915. DOI: 10.21474/IJAR01/11352

[10] Akyildiz, I. F., & Jornet, J. M.,"The Internet of Nano Things (IoNT)", IEEE Wireless Communications,2010;vol. 17(6):PP. 58-63.

[11] I. F. Akyildiz, J. M. Jornet, and M. Pierobon. "Nano networks: A new frontier in communications," Communications of the ACM,2011;vol. 54, no. 11:pp. 84–89.

[12] AnandNayyar, VikramPuri, Dac-Nhuong Le (LêĐắcNhường), "Internet of Nano Things(IoNT): Next Evolutionary Step in Nanotechnology", Nanoscience and Nanotechnology,2017; 7(1):4-8, DOI: 10.5923/j.nn.20170701.02

[13] P. Kulakowski, K. Solarczyk, K. Wojcik, "Routing in fret-based nanonetworks", IEEE Commun. Mag.2017;Vol. 55 (9):pp. 218–224

[14] Karan Agarwal, Kunal Agarwal, Shalini Agarwal. "Evolution of Internet of Nano Things(IoNT)", International Journal of Engineering Technology Science and Research, ISSN2394 – 3386,2017; Volume 4, Issue 7

[15] N.A. Ali, W. Aleyadeh, M. AbuElkhair, "Internet of nano-things network models and medical applications", in: Wireless Communications and Mobile Computing Conference (IWCMC), International, IEEE, ,2016; pp. 211–215

[16] Hemdan Ezz El-Din, D. H. Manjaiah, "Internet of Nano Things and Industrial Internet of Things", Internet of Things: Novel Advances and Envisioned Applications, https://doi.org/10.1007/978-3-319-53472-5_5

[17] M. Kuscu, O.B. Akan. "The Internet of molecular things based on fret", IEEE Internet Things J.2016; 3 (1):pp. 4–17.

[18] Bassam Al-Shargabi, Omar Sabri,2017. "Internet of Things: an Exploration Study of Opportunities and Challenges", ICEMIS, 978-1-5090-6778-7/17

[19] Yusuf Perwej. "A Literature Review of the Human Body as a Communication Medium using RedTacton", Communications on Applied Electronics (CAE),ISSN : 2394-4714, Foundation of Computer Science FCS, USA, April 2016; Vol. 9, No.4:Page 7 – 17. DOI: 10.5120/cae2016652161

[20] Yusuf Perwej, "The Next Generation of Wireless Communication Using Li-Fi (Light Fidelity) Technology", Journal of Computer Networks (JCN), USA, ISSN (Print): 2372-4749 ISSN (Online): 2372-4757, Science and Education Publishing, June 2017; Vol. 4, No. 1:Page 20-29. DOI: 10.12691/jcn-4-1-3

[21] Andrew Whitmore, Anurag Agarwal, Li Da Xu, "The Internet of Things A survey of topics and trends",InfSyst Front, DOI: 10.1007/s10796-014-9489-2

[22] Mahdi H. Miraz, Maaruf Ali, Peter S. Excell, Rich Picking. "A Review on Internet of Things (loT), Internet of Everything (IoE) and Internet ofNano Things (IoNT)", Internet Technologies and Applications (ITA), IEEE, DOI: 10.1109/ITechA.2015.73173982015

[23] M. Stelzner, F. Dressler, S. Fischer, "Function centric networking: an approach for addressing in in-body nano networks", in: Proceedings of the 3rd ACM International Conference on Nanoscale Computing and Communication, ACM, 2016;pp. 38.

[24] Josep Miquel Jornet , Ian F. Akyildiz, "The Internet of Multimedia Nano-Things", Nano Communication Networks,2012;vol. 3, no. 4:pp. 242–251, doi:10.1016/j.nancom.2012.10.001

[25] Falko Dressler, Stefan Fischer, "Connecting in-body nano communication with bodyarea networks: Challenges and opportunities of the Internet of Nano Things", Nano Communication Networks, 2015

[26] Najah Abu Ali, Wesam Aleyadeh, Mervat Abu Elkhair, "Internet of Nano-Things Network Models and Medical Applications", 978-1-5090-0304-4/16, 2016 IEEE

[27] Yusuf Perwej, Mahmoud Ahmed Abou Ghaly, Bedine Kerim and Hani Ali Mahmoud Harb. "An Extended Review on Internet of Things (IoT) and its Promising Applications", Communications on Applied Electronics (CAE), Foundation of Computer Science FCS, New York, USA, 2019; Volume 9, Number 26: Pages 8– 22. DOI: 10.5120/cae2019652812

[28] I. F. Akyildiz, F. Brunetti, and C. Blazquez, "Nano networks: A New Communication Paradigm", ComputerNetworks (Elsevier) J.Aug. 2008; vol. 52, no. 12:pp. 2260–79

[29] I. F. Akyildiz and J. M. Jornet, "Electromagnetic Wireless Nano sensor Networks", Nano Communication Networks (Elsevier) J.,2010; vol. 1, no. 1:pp. 3–19.

[30] Firoj Parwej, Nikhat Akhtar, Yusuf Perwej, "An Empirical Analysis of Web of Things (WoT)", International Journal of Advanced Research in Computer Science (IJARCS), ISSN: 0976-5697,2019; Volume 10, No. 3:Pages 32-40.DOI: 10.26483/ijarcs.v10i3.6434

[31] K. Agarwal, K. Agarwal, and S. Agarwal, "Evolution of Internet of Nano Things (IoNT)," Int. J. Eng. Technol. Sci. Res.,2017; vol. 4, no. 7:pp. 274–277

[32] G. Miller, M. Kearnes, "Nanotechnology, Ubiquitous Computing and the Internet of Things: Challenges to Rights to Privacy and Data Protection", Draft Report to the Council of Europe, 2012

[33] Miraz, M.H.; Ali, M.; Excell, P.; Picking, R. "A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)", In Proceedings of the Fifth International IEEE Conference on Internet Technologies and Applications (ITA 15), Wrexham, UK, 8–11 September 2015; pp. 219–224

[34] Yusuf Perwej, Bedine Kerim, Mohmed Sirelkhtem Adrees, Osama E. Sheta, "An Empirical Exploration of the Yarn in Big Data", International Journal of Applied Information Systems (IJAIS), ISSN : 2249-0868 , Foundation of Computer Science FCS, New York, USA, 2017; Volume 12 , No.9:Page 19-29. DOI: 10.5120/ijais2017451730

[35] Balasubramaniam, S. Kangasharju, J. "Realizing the Internet of Nano Things: Challenges, Solutions, and Applications",Computer, 2013; 46:pp. 62–68.

[36] Ali, N.A.; Abu-Elkheir, M. "Internet of Nano-Things Healthcare Applications: Requirements, Opportunities, and Challenges", Proceedings of 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob' 2015), Abu Dhabi, UAE, October 2015;pp. 19–21,

[37] Akyildiz, I.F.; Pierobon, M.; Balasubramaniam, S.; Koucheryavy, Y., "The Internet of Bio-Nano Things", IEEE Commun. Mag.,2015; 53:pp. 32–40.

[38] El-din, H., & Manjaiah, D.," Internet of Nano Things and Industrial Internet of Things", In D. P. Acharjya & M. Kalaiselvi Geetha (Eds.), Internet of Things: Novel Advances and Envisioned Applications, Berlin, Germany: Springer ,2015; Vol. 25:pp. 109–123, 2017

[39] Jornet, J., & Akyildiz, I. F.," The internet of multimedia Nano-Things", Nano Communication Networks,2012; vol. 3(4), pp. 242–251

[40] L. Atzori, A. Iera, G. Morabito, "The Internet of things: a survey", Computer Networks,2010; 54:pp.2787–2805

[41] Liu, B., Lai, Y., & Ho, S.-T. " High Spatial Resolution Photo detectors Based on Nanoscale Three-Dimensional Structures", IEEE Photonics TechnologyLetters,*2010*; *22*(12):929–931

[42] Smith, R., Arca, A., Chen, X., Marques, L., Clark, M., Aylott, J., & Somekh, M.," Design and fabrication of nanoscale ultrasonic transducers, Journal of Physics: Conference Series,2012; 353(1)

[43] Jornet, J., & Akyildiz, I. F. ,"The internet of multimedia Nano-Things", Nano Communication Networks,2012a;vol. 3(4):pp. 242–251

[44] Yusuf Perwej, Firoj Parwej, "A Neuroplasticity (Brain Plasticity) Approach to Use in Artificial Neural Network", International Journal of Scientific & Engineering Research (IJSER), France, ISSN 2229 – 5518, 2012; Vol.3, Issue 6:Pages 1- 9. DOI: 10.13140/2.1.1693.2808

[45] Akyildiz I.F., Nie S., Lin S.C., Chandrasekaran M. 5G roadmap: 10 key enabling technologies. Computer Networks, 2016; 106:17–48

[46] T. Nakano, T. Suda, M. Moore, R. Egashira, A. Enomoto and K. Arima, Molecular Communication for Nanomachines Using Intercellular Calcium Signaling, 5th IEEE Conf. on Nanotechnology,2005; Vol. 2:pp. 478-481

[47] D. Kilinc and O. B. Akan, "Receiver design for molecular communication", *IEEE Journal On Selected Areas in* Communications/Supplement Part 2, December 2013; vol. 31, no. 12,

[48] D. N. Kinsumuna, D. T. Altilar and D. Demiray, "A signal transmission model for diffusion based molecular communication nano networks", Joint International Mechanical Electronic and Information Technology Conference, 2015; pp. 1008-1011.

[49] Jornet J.M., Akyildiz I.F. Channel modelling and capacity analysis for electromagnetic wireless nano networks in the terahertz band. IEEE Transactions on WirelessCommunications,2011; 10(10):3211–3221.

[50] Pierobon M., Jornet J.M., Akkari N., Almasri S., Akyildiz I.F. A routing framework for energy harvesting wireless nanosensor networks in the terahertz band. Wireless Networks,2014; 20(5):1169–1183.

[51] Al-Turjman F. A cognitive routing protocol for bio-inspired networking in the Internet of nano-things (IoNT). Mobile Networks and Applications,2017; 1–15

[52] R. Piesiewicz, T. Kleine-Ostmann, N. Krumbholz, D. Mittleman,M. Koch, J. Schoebei, and T. Kurner, "Short-range ultra-broadbandterahertz communications: Concepts and perspectives," IEEE Antennas and Propagation Magazine,2007; vol. 49, no. 6:pp. 24–39.

[53] J. M. Jornet and I. F. Akyildiz, "Channel capacity of electromagnetic nano networks in the terahertz band," in Communications (ICC), 2010IEEE International Conference on. IEEE, 2019; pp. 1–6.

[54] Jan-Christoph Brumm, Gerhard Bauch," Channel Capacity and Optimum Transmission Bandwidth of In-Body Ultra Wideband Communication Links", 11th International ITG Conference on Systems, Communications and Coding, Germany.2017

[55] H. F. Atlam, at.al."Developing an adaptive Risk-based access control model for the Internet of Things," IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), IEEE Smart Data (SmartData), 2017; pp. 655–661.

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

[57] O. M. E. and M. M., "The Future of Healthcare: Nanomedicine and Internet of Nano Things," Folia Medica -Fac. Med. Univ. Saraeviensis, 2015; vol. 50, no. 1:pp. 23–28

[58] Yusuf Perwej, Firoj Parwej, Nikhat Akhtar, "A Posteriori Perusal of Mobile Computing", International Journal of Computer Applications Technology and Research (IJCATR), ATS (Association of Technology and Science), ISSN 2319–8656 (Online),2014; Vol.3, Issue 9:Pages 569 - 578, DOI: 10.7753/IJCATR0309.1008

[59] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an Adaptive Risk-based Access Control Model for the Internet of Things," I.J. Comput. Netw. Inf. Secure., no. January,2018; pp. 26–35,

[60] F. Dressler and S. Fischer, "Connecting in-body nano communication with body area networks: Challenges and opportunities of the Internet of Nano Things," Nano Commun. Netw.2015; vol. 6, no. 2:pp. 29–38.

[61] N. A. Ali and A. Ain, "Internet of Nano-Things Healthcare Applications: Requirements, Opportunities, and Challenges," in 2015 the First International Workshop on Advances in Body-Centric Wireless Communications and Networks and Their Applications, 2015;pp. 9–14.

[62] Yusuf Perwej, Kashiful Haq, Firoj Perwej ,"Block ciphering in KSA, A major breakthrough in cryptography analysis in wireless networks", International Transactions in Mathematical Sciences and Computer, India, ISSN-0974-5068, July-December 2009;Volume 2, No. 2:Pages 369-385.

[63] M. L. Hale and S. Hanson, "A Testbed and Process for Analyzing Attack Vectors and Vulnerabilities in Hybrid Mobile Apps Connected to Restful Web Services," Proc. 2015 IEEE World Congr. Serv. Serv. 2015; pp. 181–188.

[64] H. Chen et al., "Wearable and robust turbo electric nano generator based on crumpled gold films," Nano Energy, 2018;vol. 46, no. January: pp. 73–80.

[65] Yusuf Perwej, Kashiful Haq, Uruj Jaleel, Sharad Saxena, "Some drastic improvements found in the analysis of routing protocol for the Bluetooth technology using scatternet" International Conference on Computing, Communications and Information Technology Applications (CCITA-2010), Ubiquitous Computing and Communication Journal (UBICC) Seoul, South Korea, ISSN Online 1992-8424, ISSN Print 1994-4608,2010; Volume CCITA-2010, Number 5:pages 86-95.

[66] R. Bouhenguel, I. Mahgoub, and I. Mohammad, "Bluetooth security in wearable computing applications," Int.Symp. High Capacit. Opt. Networks Enabling Technol. HONET 2008; pp. 182–186.

[67] F. Dressler and F. Kargl,"Towards security in nano communication: Challenges and opportunities," Nano Commun. Netw., 2012; vol. 3, no. 3:pp. 151–160.

[68] Gandino, F., Celozzi, C., & Rebaudengo, M." A Key Management Scheme for Mobile Wireless Sensor Networks", Applied Sciences,2017; 7(5):490.

[69] F. Dressler, F. Kargl, "Towards Security in Nano-communication: Challenges and Opportunities", Elsevier Nano Communication Networks2012; 3 (3):pp. 151-160.

[70] F. Dressler and F. Kargl, "Towards security in nano communication: Challenges and opportunities," Nano Commun. Netw.,2012 vol. 3, no. 3:pp. 151–160.

[71] S. Brands and D. Chaum, "Distance-Bounding Protocols," in Advances in Cryptology - EUROCRYPT "93, Workshop on the Theory and Application of of Cryptographic Techniques, Vol. LNCS 765, Lofthus, Norway, 1994; pp. 344–359.

[72] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks",IEEE 27th Conf. Comput. Commun.,2008; pp. 1238– 1246,.

[73] https://www.mordorintelligence.com/industry-reports/internet-of-nano-things-market

[74] Najah AA, Wesam A, Mervat Abu E Internet of nano-things network models and medical applications. IEEE Wireless Commun 2016; 211–215

[75] P. Kethineni, "Applications of Internet of Nano Things: A survey," 2017 2nd International Conference for Convergence in Technology (I2CT),2017;pp. 371--375,

[76] R. A. Freitas, "Pharmacytes: An ideal vehicle for targeted drug delivery," Journal of Nanoscience and Nanotechnology,2006; vol. 6, no. 9-10:pp. 2769–2775.

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

[78] Lee SW, Mao C, Flynn CE, Belcher AM Ordering of quantum dots using genetically engineered viruses. Science 2002; 296:892-5

[79] C. R. Yonzon, D. A. Stuart, X. Zhang, A. D. McFarland, C/ L. Haynes, and R. P. Van Duyne. Towards advanced chemical and biological nanosensors-an overview. Talanta,2005; 67(3):438–448,

[80] P. Tallury, A. Malhotra, L. M. Byrne, and S. Santra. "Nano bio imaging and sensing of infectious diseases", Advanced Drug Delivery Reviews, 2010; 62(4-5):424–437.

[81] S. Ravindra, Y. M. Mohan, N. N. Reddy, and K. M. Raju, "Fabrication of antibacterial cotton fibres loaded with silver nanoparticles via "green approach"," Colloids and Surfaces A: Physicochemical and EngineeringAspects,2010; vol. 367, no. 1:pp. 31–40.

[82] J.A. Rogers. "Materials and mechanics for stretchable electronics-from electronic eye cameras to conformal brain monitors", In International Solid-State Sensors, Actuators and Microsystems Conference, June 2009; pages 1602–1603.

[83] El-din, H., & Manjaiah, D. "Internet of Nano Things and Industrial Internet of Things", In D. P. Acharjya & M. Kalaiselvi Geetha (Eds.), Internet of Things: Novel Advances and Envisioned Applications, Berlin, Germany: Springer,2017;Vol. 25, pp. 109–123.

[84] C.-J. Chen, Y. Haik, and J. Chatterjee, "Development of nanotechnology for biomedical applications," in Conference, Emerging Information Technology 2005; IEEE, pp. 4-12

[85] A. Jafarey, The internet of things and ip address needs 2015 [cited 15.11.17]. URL http://www.networkcomputing.com/networking/internet-things-ip-address-needs/1170065007.

[86] J.M. Jornet Montana, 2013. "Fundamentals of Electromagnetic Nano networks in the Terahertz Band", (Ph.D. thesis), Georgia Institute of Technology.