DOI: https://doi.org/10.46632/daai/2/6/5

Data Analytics and Artificial Intelligence

Vol: 2(6), 2022

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

The Internet of Nano-Things

Yogesh Vishwakarma

University of Mumbai, Mumbai, Maharashtra, India

*Corresponding Author's mail id: yogesh.mit21017@sstcollege.edu.in

Abstract: *The growth of Intelligent environments reveals the interconnectedness of applications and the internet usage. For this reason, known as the Internet of Things (IOT). The expansion of the IOT concept provides access to the Internet of Nano-Things (IONT). A new communication network model based on nano-technology and IOT, in other words, a paradigm with the ability to interconnect nano-scale devices through existing networks. The concept of the Internet of Things Nano emerged from the interconnection of these nano machine with the Internet. Nano-internet of things is a system of Nano-connected devices, objects or organisms that have unique identifiers to transfer data wirelessly to the cloud over a computer or cellular network. Data distribution, caching and energy consumption are among the most important topics in IONT nowadays. The nano-network paradigm can empower consumers to make a difference in their well-being by connecting data to personalized analytics within timely insights. Real-time data can be used in the diversification of Nano-applications in the Internet of Things, from preventive treatment to diagnosis and rehabilitation. This paper intelligently explains the Internet of Nano Things, its architecture, challenges, role of IONT in the global market, IONT applications in various domains. The Internet of Things has provided countless new opportunities to create a powerful industrialized infrastructure and many more. Major applications for IONT communications including healthcare, transportation and logistics, defense and aerospace, media and entertainment, manufacturing, oil and gas, high-speed data transfer and cellular, multimedia, immune system support and other services. Finally, since security is considered as one of the core issues of the IONT system, we provide an in-depth discussion of the Nano-Things market trends on security, communication networks and the Internet.*

Keywords: *The Nano-Technology, Internet of Nano Things (IONT); The Smart Home; Functioning of the, Commination with The internet of Nano-Technology, Security of the Internet of Nano Things.*

1. INTRODUCTION

We are amazed at the technology revolution that has brought us the awesome concept called Internet of Things. With the help of intelligent, we are able to convert our ordinary home into a smart home and control it without physically operating any device just by giving commands. These are smart watches that only track all our physical activities but also alert us when the data exceeds the limit. But, on the technology front, things are, moving fast, so we need more comfort with the help of technology. this is why now the talk of the town is more about the latest technology called INTERNET OF NANO THIINGS (IONT).

2. NANO-TECHNOLOGY

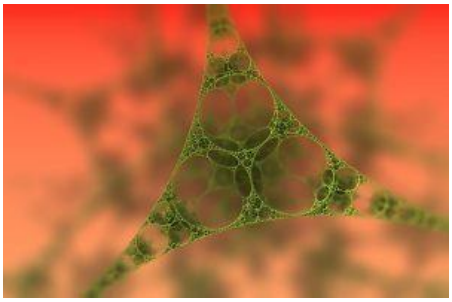

FIGURE 1. Nano technology

Nano-Technology stands for nano particles that can't detected by earlier technologies. For example, we have a sensor to detect various object but it failed in case of nano particle detection. Then come nano-sensors in the picture, which are helping us collect information from the nanoparticles of the microscopic world. In the case of medical science, nano sensors are being used to detect the stage of tumor and cancer. Data accuracy and observation down to the cell level make the nano sensor more reliable. Thus doctors and researchers used this technique to detect diseases more accurately. Nano technology provides intelligent solutions in many sectors such as the biomedical, industrial and military sectors as well as consumer and industrial goods. This is the potential for engineering functional systems at the nano scale – particles at the molecular level. Let's see some of the examples where Nanotechnology is helping us to solve many problems.

- Nano sensors are not only used for the medical research and the automotive world but also help protect our environment. There are nano sensors that let you know the exact level of pollution in the air. Thus helping us to identify the source of pollution and the act on it so as to clearly prevent the menace of clean air.
- Nano sensors have the ability to measure the temperature of living cells. Thus it helps doctors and scientists to make more accurate decisions when treating a patient or researching specific topics.
- There are smoke and gas detectors where nano sensor technology is being used to detect hazardous chemicals and the other fine toxic particles which may not be possible with normal sensors. Thus, by using nano sensors, we can protect our environment as well as ourselves from the danger.
- Nano sensors are being used in the case of DNA testing?. Yes, because of its ability to read cell level information and data accuracy, it is being used in DNA testing to detect similar properties between two cells. Thus, it is helping doctors and scientists to uncover and unsolved mysteries. Furthermore, nano sensors are helping us to collect precise and accurate information from cell level which helps our doctors and scientists to treat dangerous diseases like cancer and tumors.

3. The Internet of Nano Things

The Internet of Nano Things is nothing but the interconnection of nano devices with existing networks. Thus, it create a state of the art revolution in electromagnetic communication fields between nano-scale devices.

FIGURE 2. IONT

A nano machine integrates with nano components to perform multiple functions. It performs the way we connect devices in the case of Internet of Things but the big difference is that it can connect nano components which is not possible with Internet of Things. Although the Nano Internet of Things is still in its early stages, the concept may soon be implemented in the same way as we are implementing the Internet of Things in many application areas. Let us discuss some examples of Internet of Things which are currently helping us in many areas, and how it can be carried forward with the help of Nano Internet of Things to work more precisely.

The Smart Home: One of the most popular applications of the Internet of Things is smart home solutions. A lot of people have already implemented this awesome application to control many useful devices in their home using many useful devices like Smartphone, Amazon Echo, and Thermostat etc. It makes their life easy, they can control their home even sitting at their home from offices or any other place. So, what could be the next possibilities with the Internet of Things Nano? With IONT there are many possibilities that can further enhance this amazing smart home solution. Imagine, you are away from your home and there is a gas leak in your kitchen. This can be dangerous and some electric spark or some other reason may cause a fire. But, with the help of IONT, it can be detected much earlier and you can be alerted to take necessary steps to resolve the issues. Since IONT has the capability to detect nano particles, a simple nano sensor can detect

a gas leak and send you an immediate alert to take necessary action. There are many application areas where the concept of IONT can be applied to further enhance the functionality of the Internet of Things.

FIGURE 3. Smart home

Nano sensors invented with this concept of IONT are currently helping in many useful application areas by sensing nano particles which may not be possible with normal sensors. Let us discuss some examples in case of both humans and animals where nano sensors are being used for the betterment of their lives.

- Nano sensors are being used to track farm animals. Thus the solution to a great concern of farmers is that it is very common that farm animals like cows, pigs, sheep etc. may run away while grazing. Nano sensors are attached to farm animals and are being tracked by a centralized computer system.
- Nano sensor networks are used to track the health of crops and plants. The researcher collects accurate data about the health of plants and crops and recommends necessary action accordingly.
- Viruses that cannot be detected by normal sensors, nano sensors can easily detect them. There are bands that can be used as normal wristbands to inform us when we are exposed to anything contaminated with viruses and bacteria. Thus saving us from falling prey to those deadly little animals.
- We have thermometers, sensors to measure temperature, but nano sensors are a step ahead. Nano sensors have the ability to measure the temperature of living cells. Thus it helps doctors and scientists to make more accurate decisions while treating a patient or doing research.
- Finally, although the Internet of Nano Things is still in the developing stages, the day is not far when it can be applied in many useful application areas to provide extended functionality beyond the Internet of Things we currently have.

How Internet of Nano Things Functioning: Nanotechnology can be combined with IOT, in the creation of a physical network made of nanomaterials that facilitates the exchange of data through various components that communicate with each other at the nano level. In terms of development, it is not yet at the level of other IOT systems, but it attract interest from the communication and medical sectors. One such example is in fieldbased applications where remote sensing is required, or for measuring various points within the human body. We need to first look at the traditional IOT systems that are now being deployed to create smart sensor networks and more automated processes. An IOT is a set of sensor networks, data collectors and transmitters that send data through the cloud from multiple entry points to a centralized location. This enables the IOT to be self-sustaining without the need for human interaction, as long as the system does not alert the operator to a problem, which it finds through its analysis. IONT, in essence, is a smaller version of these systems that employ much smaller sensors and data network hubs to transmit data over long distances. As it stands, IoT systems are not as welldeveloped as their IoT counterparts, but their ability to collect data using such small sensor points makes them useful for applications that are similar to other (bulkier) sensor networks. are not compatible with. There are various components within the IONT network that communicate with each other to transfer data over long distances. Any system, there are many components, and the IONT is no different. There are also two general ways in which these components communicate with each other, and these are through electromagnetic nano-communication (transmitting and receiving electromagnetic waves) and molecular communication (information encoded in molecules). As for components, IONT has four main areas that help facilitate the transfer of information; these are nano nodes, nano-routers, nano-micro interface devices, and gateways. There are four basic components of an IONT system as shown in the figure below. These are called nano nodes, nanorouters, nano-micro interface devices and gateways. The smallest component is the nano node. These are colloquial terms for sensors in traditional IoT networks and are essentially basic nano machines. Due to their small size and small internal memory, the operations they can perform are limited, as well as the distance that they can transmit data. However, multiple nano-nodes can be connected to one or more nano-routers, such that sensors send localized data to a localized hub before sending information over long distances. Nano-routers are much larger than nano nodes, and therefore have much

higher computational power which enables them to collect and aggregate all data from surrounding nano nodes and transmit this data over long distances to nano-routers. Micro interface transmits to the device. A nano node is the simplest and smallest component within the IONT setup and is viewed as a basic nano machine. These tiny nano machines are used to transmit data and perform basic calculations. However, their small size (and energy) limits the distance they can transmit data, and they have very small internal memory. Nevertheless, they can be placed in a specific location and the data can be transmitted to a large nanorouter, which then transmits the data over long distances. Therefore, nano nodes can often be the actual sensor components of the system. Nano nodes pass the data to a nano-router, which is a nano machine with enormous computational power. Because they have a lot of computational power, they act as an aggregator for all the surrounding nano nodes that receive the initial data. They can then control exchange commands between nano nodes and send information to the nano-micro interface devices. These interface devices collect all the data from the nano-router and transmit the data to the micro scale (and vice versa) using a combination of nanocommunication techniques and classical network protocols. The gateway then acts as the controller of the entire system and enables the data to be accessed anywhere via the Internet. Therefore, IOT shows some similarities to how IOT systems work, but the smaller size of the components means that some centers have to be closer together.

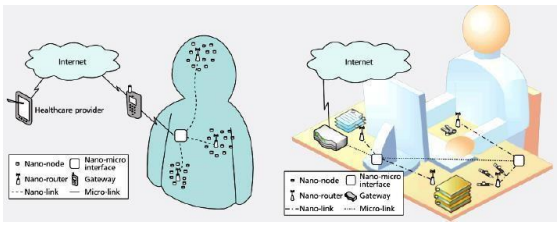

FIGURE 4. Functioning of IONT

The Main Reason of Internet of Nano things: The development of nanotechnology, nano machine, Internet of nano things will have a great impact on the advanced development in almost every field in the near future. The interconnection of nanoscale devices with existing communication networks and eventually the Internet defines a new networking paradigm further called the Nanotechnology Internet of Things.

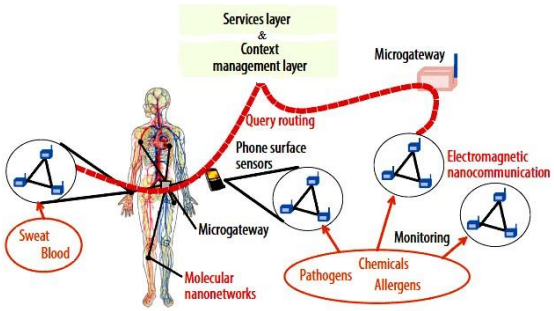

FIGURE 5. The Nano Communication in Internet of Nano Things

IONT is an extension of the Internet of Everything, but where you have the possibility to incorporate nano-sensors into various objects and use nanonetworks. That is, the reason for IONT is its ability to interconnect a variety of devices developed at the nano-scale in communication networks, where it allows data to be collected in hard-to-reach places. The figure shows the interconnection that is established between different devices, such as a nano-sensor via a nano-network, with the objective providing the necessary information within complex-to-reach areas. For example, on-body nano-sensors can provide electrocardiographic and other vital signs, while environmental nano-sensors can collect information about pathogens and allergens in a given area. The term as a nano-network is not a simple extension of the traditional communication network at the nanoscale. They are a whole new communication paradigm, in which most communication processes are inspired by biological systems found in nature.

4. INTERNET OF NANO THINGS SECURITY

The Internet of Nano Things is being incorporated into most of our lives in applications such as phones, home appliances, sensors, vehicles and largescale infrastructure systems. These devices have their own control and monitoring processes digitized and connected to the Internet, which raises a number of security and privacy issues. The integration of body area network systems within body devices and nano machines also creates a new level of security challenges. One of the most important challenges as a result of the growth of the Internet of Things market pertains to the security of the data transmitted over the Internet. For example, in the healthcare sector, a bio-cyber-attack can steal people's personal health information. This information can be used to create new types of viruses to hack nano sensors already deployed in the Internet of Things

Nano. Therefore, security assurance methods should be applied to communication networks in the 4G and 5G eras, especially in the Nano Internet of Things, to prevent such problems, taking into account the nature of the Internet of Nano Things communications. Nano Internet of Things is vulnerable to all kinds of attacks, whether physical or via wireless technologies, given that this type of device does not meet with constant vigilance. Attacks can be to obtain private data through theft of sensors, disrupt controlled applications that use computers, or modify communication links in nano-networks. This is because standard security techniques cannot be applied to nano networks operating in the terahertz band. In order to secure the IONT system, there is a need to develop new security solutions. The author proposed new security methods between nano-communications, in particular the connection between the Nano-Internet of Things and the Nano-Internet of Things. These security aspects are mentioned in nano communication security, security purposes and security mechanisms for IONT systems. They are made up of confidentiality, integrity and availability. When connecting nano communication devices with IoT, we are facing typical sensor network security issues. The range for an attacker, especially the integration of gateway nodes and smart phones, opens up entirely new attack vectors. Furthermore, the use of these networks to collect very private information, from location information to physical data, makes these networks a valuable target for malicious users. Therefore, there is a need for new security and privacy technologies to protect the sensitive data collected by nano sensors.

Aim: In this section evaluating the security of the Internet of Things nanotechnology system, we need to begin with a classical security and risk analysis. In addition, there are innovative and emerging challenges in the nano communication field as well as those related to the coupling of in-body networks with external devices. First assess the estimate of CIA (Availability, Integrity, and Confidentiality) security in these new circumstances. The availability of a network that is secure can be difficult, as attackers may have enough energy to jam radio transmissions or flood a communication channel with large amounts of molecules that destroy regular communication molecules.

Availability: The malicious user must not be able to disrupt or harmfully affect the quality of service or communications provided by the Nano device or the Nano network. In the Internet of Nano Things scenario, the availability of the BAN network, in-body nano communication network and gateway nodes must be maintained under all conditions and circumstances. There is a need for adaptive self-organizing solutions to handle this issue.

Integrity: The content of messages exchanged between a sender and a receiver must be protected against modification by an intruder, without the receiver not being able to track this modification. In Internet of Nano Things systems, integrity checks need to be implemented not only on BAN nodes but also on nano devices and micro gateways. Integrity checks can be performed on each node involved in the exchange of messages between the originator and receiver.

Confidentiality: An attacker should not be able to access the contents of messages exchanged between the sender and receiver. In our context, this means that confidentiality must be ensured not only within body area networks, for example, using encryption techniques such as well-known AES or RSA algorithms, and within in-body nano communication networks, As such, relying on biochemical cryptography, but mainly also when relaying messages using gateway systems connecting the two worlds. As always, encryption and digital signatures require security supporting functionality, starting with cryptographic techniques, but also for authentication as a base functionality.

5. INVASION VECTORS IN INTERNET OF NANO THINGS

An attack vector is a path or means by which an attacker can gain unauthorized access to a computer or network in order to deliver a payload or malicious result. Attack vectors allow attackers to exploit system vulnerabilities, install various types of malware, and launch cyberattacks. Attack vectors can also be exploited to gain access to sensitive data, personally identifiable information (PII) and other sensitive information that can result in a data breach. It tries to exploit vulnerabilities in a device or network. There are many attack vectors associated with the Internet of Things nanotechnology system that need to be controlled by implementing the necessary security measures to mitigate them.

Internet Exposure: Despite the fact that connecting nano devices to the Internet helps to share information with each other and allow for real-time applications, any device that connects to the Internet and intercepts incoming traffic, Eventually falls victim to the attack. Unlike network servers where a firewall can control how a host can be accessed, nano devices are employed with limited compute capabilities and memory and are built without security features that allow it to be accessed from various locations on the Internet. Make it an easy target for the various attacks to come.

Lack of Encryption: Unfortunately, security is often a consideration throughout the development lifecycle of Internet of Things devices. Failure to encrypt sensitive data exchanged between nano devices, whether on a nano device or over a nano network, will lead to a number of security issues, especially when nano devices become part of our bodies. Embedded cryptography such as cryptographic coprocessors, which can address encryption and authentication of nano devices, is needed and securing data on nano devices should be part of any design.

Wearable Malware*:* Wearable devices are developing rapidly in various fields. These devices include smart glasses and headgear, fitness trackers, wearable medical devices, smart watches and smart clothing and accessories. Wearable devices can become attractive targets for malicious software, especially as they use Bluetooth, which uses frequency hopping to allow multiple devices to transmit a signal at the same frequency at the same time.

Denial-of-service: Denial-of-service (DOS) attack is a type of cyber attack in which a malicious actor aims to make a computer or other device unavailable to its intended users by disrupting the normal functioning of the device. It is defined as any event that reduces or eliminates the network's ability to perform the expected function. An attacker tries to influence the availability of a network that may be difficult to protect, as the attackers may have enough energy to jam radio transmissions or fill a communication channel with large amounts of molecules that Regular communication destroys molecules.

6. INTERNET OF NANO THINGS SECURITY MECHANISMS

In this section, we are discussing how to increase the security of IoT systems and also we are considering the following mechanisms to establish secure communication in nano sensor networks.

Key Management: Establishing symmetric keys is called key management. The distribution of security keys is believed to be the core of almost all key management systems. Keys can be distributed either pre-distribution prior to deployment or actively distributed across the sensor network before any data transmission occurs. It is necessary to have the ability to revoke a key when it has been exposed. This problem is still one of the most challenging issues in sensor networks and IONT systems. It is necessary to define standard procedures for generating shared keys and to define how the keys can be revoked when necessary.

Cryptographic Primitives: In the realm of body area networks, we can rely on classical cryptographic solutions such as using symmetric AES or asymmetric RSA algorithms. For body nano communication, however, we need more lightweight solutions such as the proposed biochemical cryptography.

Access Control and Authentication: Authentication is a prerequisite to guarantee the purpose of confidentiality. Every message that wants to be sent to a nanocommunication system must pass through a gateway and be authenticated. Authentication is usually achieved using traditional symmetric or asymmetric cryptography. Biochemical cryptography is a new and still unexplored field that uses biological molecules such as DNA/RNA evidence to encrypt information and protect the confidentiality and integrity of data. Although this cryptography scheme opens up various new application domains, it leads to new issues related to communication systems. Complex molecules can spontaneously react within the system resulting in modifications outside the control of the nano machinery. Therefore, there is a need to better understand the biochemical processes involved in the system.

Secure Localization: In IONT, many applications will need to know the location of the nano-sensors to perform specific functions. Some applications that use nano communication require the localization of nano machines to complete their operation. Differences in demands between classical sensor networks, using other coordinate systems, and nano devices make it difficult to generate an absolute position with nanoscale resolution, but relative positioning may be more relevant. This is directly tied to security to allow only nearby nano machines to communicate and prevent remote attackers from interfering.

Intrusion Detection: Due to some of the problems that classical cryptography methods can present, it is necessary to put in place the necessary systems to detect and respond to attacks. Indicated that the strategy for denial of service attacks involves implementing an intrusion detection system in the entry node of the nano-communication system and is failsafe. Some attacks generally cannot be handled by cryptography. For example, denial-of-service attacks that try to disrupt system availability in nano communications networks can be difficult to defend against. This is because attackers may have the energy needed to jam a radio transmission or fill a communication channel with massive amounts of molecules that destroy regular communication molecules. An intrusion detection system can be used to handle this issue by detecting the attack and triggering the system to go into fail-safe mode. Therefore, it is important to establish new intrusion detection systems that are capable of efficiently detecting and responding to attacks in nanonetworks.

Performance and Scalability: Last but not least, the resulting system performance is an important aspect to consider. Security and privacy in nanocommunication systems present significant challenges with respect to the performance and scalability of participating nodes. IONT securities will create issues of extreme performance and scalability. Nano machines that perform nanotechnology will have severe resource limitations that are unmatched in current communication systems. Although the performance of cryptographic algorithms has been evaluated in sensor networks, these results cannot be directly applied to the nanodomain because of the different processes of information processing. In addition, energy consumption is a more serious issue as communication systems such as nano-tube based radios require significant power due to the cryptographic payloads they carry. Therefore, the performance of communication protocols and cryptographic techniques must be taken into account when developing practical applications.

7. LITERATURE REIVEW

In the U.S., several IONT technology gateways were designed to gain access to one or more nanonets to ensure accurate processing and reliability. IONT health care applications intended with requirements are also recognized as fundamental health care facilitation opportunities. The in-body nano communication network was studied with An overview and key requirements for designing gateway body area network of IONT architecture by IONT architecture. studied it The model creates a new level of security where the authors assess the resulting security challenges with the processor. another The study examined the effects of some changing environmental conditions and their impact on IONT communications Based on molecular interactions, i.e. temperature (T) and relative concentration of physical constraints (X). when The conductivity (Pconn) of the nano-network was examined, it is noted that Pconn was less affected when the transformation occurred. occur in T and X while increasing T has a positive effect on Pconn, where interference occurs in received signal. The analysis was done in the IONT based telemedicine application and the medical information contained in it was analyzed International publications received, processed and distributed. The authors propose the eNeutral (electronicneutral) model for monitoring the energy factor via IONT, which detects and introduces signals about the event that depend on the amount of energy generated by the events. As a result, the data will be Based on the energy received from the incident a control should be uploaded to the location. A New Approach Based in Nano Grid IONT which minimizes energy consumption within the grid is an advanced Energy Efficient Algorithm (E3A) which was Preface A new approach called a Rational Data Distribution Approach (RDDA) was designed to provide Extended network lifetime without affecting other QoI features within IONT. was presented in a motion to address Energy problem in IONT communication system, this proposal includes synchronization of wireless information and Nano-networks that transmit energy in the Terahertz (THz) range to ensure better system performance. Examined the applications, challenges, security objectives, attack cycles and security challenges of the IONT network

8. METHODOLOGY

This is done through a qualitative methodology involving cutting-edge research and analysis of IONT trends. Bibliographies related to research topics are searched, reviewed and evaluated. The above allows to establish the state of the art, definitions, characteristics and possibilities of IONT. At the same time, it enables IONT to create a range of criteria for analyzing trends and challenges. Kitchenham's work (Kitchenham, 2004 was considered for the selection of bibliographic material, where several works were established, such as research questions, keywords, search strings, inclusion and exclusion criteria, and selected articles.)

9. RESULT ANALYSIS

"Global Internet of Things Nanotechnology Market: Industry Analysis, Market Size, Share, Trends, Application Analysis, Growth & Forecast, 2021-2026" provides an in depth and in depth evaluation of the Global Internet of Things Nano-technology market. The Internet of Nano Things (IONT) is an interconnected system of nano devices that are used to transfer data over a network. It consists of small, interconnected sensors, processors, networking components and control equipment that are accessed via highspeed Internet and communications networks. IONT is embedded in Internetconnected consumer electronics for collecting, processing and sharing data. As a result, it finds wide applications in various industries such as healthcare, transportation, defense, aerospace, manufacturing, energy and retail. The global Internet of Nano Things (IONT) market is primarily driven by the growing need for smart and high-speed data processing systems across industries. Compared to the metal wires used traditionally, the optical wires used in IONT systems connect and transmit data between processes at higher speeds, which is highly beneficial in applications such as gaming. Moreover, integration of connected devices with cloud computing solutions to move, store and access large amounts of data, is fueling the growth of the market.

10. CONCLUSION

This work examined a systematic review into IONT techniques. In addition, a review and survey, architecture, The communication techniques, applications, challenges and recommendations related to this technology are presented. The field of study described in Scientific Engine Cab can be described as follows: Science Direct, IEEE and Web of Science (WOS) database. The research deadline was achieved within years (2015–2021). The results showed that there are There were only 27 articles in IONT technologies during these engines, 13 articles about reviews and surveys and 14 in these articles. were involved Articles on which IONT architecture based Nano Sensors, Gateways and Servers. IONT technology needs more attention researchers in this field. It was concluded that there are wide application areas for this technology in

various fields, and There are also a number of challenges that require more attention than some future recommendations. result shown That this technology is very useful in developing many scientific and applied fields in the future. The current development of communication equipment and wireless network technologies is leading to a new era of Internet and telecommunications. Various "things", which include not only communication equipment, but also every other physical object on the planet, would also be connected to the Internet, and controlled via wireless networks. The Internet of Nano Things paradigm will take the IoT to a new level, where devices that will be connected to the Internet will focus on nano devices built from nano devices and components. These nano devices will communicate with a micro-device, which in turn will communicate with the Internet. Scientists are currently beginning to scale sensors down in size from millimeters or microns to the nanometer scale, small enough to circulate within living bodies and mix directly into building materials. This nanotechnology is an important first step towards an Internet of Things that could take medicine, energy efficiency and many other fields to a whole new dimension. The combination of nano-sensors and nano devices with the Internet has regularly set the stage for the development of the next modernization that deals with different types of data, from heterogeneous networks such as nano-links, nano micro interfaces and body sensor networks to a high degree of communication. Supports speed. Which leads to the "Internet of Nano Things". The main objective of this paper was to provide an overview by discussing the communication types and network architecture of the Internet of Nano Things system, and the communication challenges as well as the various applications and challenges of the IONT system. We have also examined Internet of Nano Things security mechanism, Attack vectors in Internet of Nano things, Security purpose. The development of nanotechnology and the Internet of Things Nano are expected to have a huge impact on advanced developments in every field.

REFERENCES

[1]. Cruz Alvarado, M.A., & Bazan(2019). E-Ciencias de la Informacion,
[2]. Balghusoon, A.O., & Mahfoudh, S. (2020). IEEE Access, 8, 200724-200748
[3]. Al-Turjman, F. (2020). Intelligence and security in big 5G-oriented IONT
[4]. Raut, P., & Sarwade, N. (2016, March). In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WIS PNET).
[5]. Jarmakiewicz, J., Parobczak, K., & Maślanka, K. (2016, May). IEEE.
[6]. Hassan, N., Chou, C. T., & Hassan, M. (2019). NEUTRAL IONT: Energyneutral event monitoring for Internet of Nano things. IEEE Internet of Things Journal.
[7]. Al-Turjman, F.(2017). Mobile Networks and Applications.
[8]. Al-Turjman, F.(2019). Cluster Computing.
[9]. Rong, Z., Leeson, M.S., Higgins, M.D., & Lu, Y.(2017).
[10]. Atlam, H.F., Walters, R.J., & Wills, G.B. (2018, August). Internet of Nano things: Security issues and applications.
[11]. Rong, Z., Leeson, M. S., Higgins, M.D., & Lu, Y.(2018). Nano-rectenna powered body-centric Nano-networks in the terahertz band. Healthcare technology letters.
[12]. Panigrahi, T., & Hassan, M.(2018), December). In 2018 IEEE Global Communications Conference (GLOBECOM) IEEE.
[13]. Canovas-Carrasco, S., Sandoval, R.M., Garcia-Sanchez, A. J., & Garcia-Haro, J.(2019). IEEE Internet of Things Journal.
[14]. Ali, N.A., Aleyadeh, W., & AbuElkhair, M. (2016, September). Internet of Nano-things network models and medical applications.