PROGRESSIVE ATTRIBUTES OF INTERNET OF NANO-THINGS (IONT)

Abstract

Numerous advances have been created during the life span of human beings and utilized to progress every individual's life. These breakthroughs will proceed to influence the longer term of mankind. Such innovations have molded who we are presently and are display in each zone fundamental for human survival, counting transportation, healthcare, and farming. Since its conception, nanotechnology has advertised progressed and viable arrangements for a few healthcare, mechanical, rural, and military employments. Nanotechnology has started the progress of infinitesimal components called Nano-machines, which are made up of requested bunches of particles and accomplish foreordained capacities. The "Internet of Nano Things" (IoNT) standard was developed as a result of the interfacing of Nano sensors and Nano gadgets with the Web. The essential objective of this work is to grant a comprehensive outline of the Internet of Nano Things (IoNT)—its design, application spaces, and challenges in arranges to teach scholastics approximately the IoNT standard and empower them to receive it in an assortment of areas within the close future for fast arrangement whereas overcoming current impediments.

Keywords: Nanotechnology, Internet of Nano-Things, Biosensors, Internet of Bio Nano-Things, Body Sensor Network, Key Management, Cryptography Advancements.

Authors

Debolina Neogi
B. Tech Student
Department of Electronics and Communication Engineering
Guru Nanak Institute of Technology
Sodepur, India
neogidebolina@gmail.com

Debalina Basu
B. Tech Student
Department of Electronics and Communication Engineering
Guru Nanak Institute of Technology
Sodepur, India
debalinab1102@gmail.com

Ananya Banerjee
B. Tech Student
Department of Electronics and Communication Engineering
Guru Nanak Institute of Technology
Sodepur, India
ananyabanerjee1233@gmail.com

Riddhi Mitra
B. Tech Student
Department of Electronics and Communication Engineering
Guru Nanak Institute of Technology
Sodepur, India
riddhimitra2703@gmail.com

Dr. Soumik Podder
Assistant Professor
School of Computer Science and Artificial Intelligence
SR University, Warangal, Telangana,
Indiananotechsoumik@gmail.com

I. INTRODUCTION

The following insurgency in computing is clearly exterior the domain of the conventional desktop. The Internet of Things (IoT) is considered as unused insurgency that's gaining immense ubiquity within the world of advanced remote communication. The Internet of Things (IoT) is the spine of different objects such as RFID (Radio Recurrence Distinguishing proof), sensors, actuators, portable innovation, NFC (Close Field Communication), smartphones, tablets, etc., which have a one of a kind presence relating and collaboration with each other to realize craved objectives. The concept of IoT, which may be a reality nowadays, was proposed by Ashton in 1999 and alludes to the unused concept of RFID in connection to its utility within the supply chain. IoT is picking up notoriety day by day by coordination all objects to communicate through implanted systems, making it a arrange of exceedingly dispersed gadgets that associated with individuals and indeed gadgets in both ways. The concept of IoT contains an awesome effect on different perspectives of everyone's life, since the quick advancement prepare of industry and analysts is in different areas such as e-health, e-agriculture, electronic industry, keen cities and e-cities, e-Military etc. The Internet of Things (IoT) creates a parcel of information that must be proficiently put away, handled and displayed - since numerous other computing advances, such as cloud computing, give such utilities through a virtual foundation that coordinating checking gadgets, information storage and information analytics apparatuses and customer-specific information conveyance models. With the developing drift of 4G systems, LTE and WiMAX, the IoT vision is additionally advancing.

The Internet of Things (IoT) requires a bound together understanding of the circumstance of clients and gadgets, Computer program Models and Unavoidable Systems for Representing Relevant Data and high-performance information analytics apparatuses that describe smart innovation. The Web of Things without a doubt revolutionized the utilize of Internet-to-device communication, where gadgets, sensors and objects communicate with each other and exchange information, and moreover made a few other areas such as remote body sensor systems (WBANs), Web. Nano innovation and Internet of Nano Things (IoNT) all lead to one bound together phrasing, Internet of Everything (IoE). The essential definition of nanotechnology is "Nanotechnology is the plan of useful frameworks at the atomic scale. In its unique meaning, "nanotechnology" alludes to the anticipated capacity to construct objects from the ground up using techniques and instruments that are being created nowadays to create total, high-performance items. Nanotechnology has given different high-quality arrangements for numerous genuine application regions such as biotechnology, biomedicine, industry, agribusiness, military applications, since it creates gadgets at a scale of one to a few hundred nanometers. Nano machine is the spine for the change of nanotechnology.

A Nano machine is characterized as a fundamental utilitarian unit coordinates with Nano components to perform fundamental assignments such as detecting or incitation. Compelling participation and coordination between Nano machines grows the complexity and usefulness of applications. In brief, the integration of Nano scale gadgets into traditional communication systems, which are vanishing with the high-speed Internet, has led to a unused advancement called "Internet of Nano-Things (IoNT)". With the presentation of the Internet of Nanotechnology (IoNT), there has too been a tenfold increase in Nano communications investigate, which points to form unused guidelines for Nano gadgets that can build communication with each other and ought to moreover be conveyed in various applications. The Internet of Nano-Things (IoNT) comprises of scaled down sensors

interconnected by Nano-networks to get information almost objects. The Internet of Nano things, on the other hand, opens new doors for logical investigate within the field of Nano sensors, Nano communications and Nano gadgets. Ian Akyildiz and Josep Jornet proposed the concept of "Internet of Nano Things (IoNT) within the Internet of Nano Things" and displayed a modern organizing worldview and state-of-the-art electromagnetic communication between Nano scale gadgets additionally displayed important research points within the channel. Modeling, information encoding and Nano organize conventions and the proposed "Nano - Internet of Things".

II. NANOTECHNOLOGY AND ITS ARCHITECTURE

1. **Emergence of Nanotechnology:** By manipulating atoms and molecules at the Nano scale, which is defined as having one or more dimensions of the order of 100 nanometers, nanotechnology refers to the discipline of science and engineering that is focused on developing, producing, and using structures, devices, and systems. Nano machines serve as the basis ofNanotechnology.

2. **Overview of Nano Machines:** A Nano-machine is defined as "An Artificial Eutectic mechanical device that depends on components that are nanometer in size." A Nano-machine is, in the simplest terms possible, "A mechanical device that performs a useful function using components of nanometer-scale and defined molecular structure, including both artificial Nano-machines and naturally occurring devices found in biological systems."

   Nano-Machine Architecture Nano machines consist of one or more components that are integrated to varying degrees. The components make up a Nano machine are as follows:

   - **Control Unit:** The control unit is the heart and central anxious framework of the Nano machineand carries out all the enlightening to total the specified assignment. The control unit moreover controls all other parts of the Nano machineconjointly acts as a capacity gadget that stores all the information of the Nano machine for clients to utilize.

   - **Communication Unit:** This device sends and receives information at the Nano level.

   - **Reproduction Unit:** The Reproduction Unit makes each part of the Nano machine using external elements and effectively accumulates them to form the Nano machine.

   - **Power unit:** It powers all elements of the Nano machine. It collects vitality from different outside sources such as temperature, light, etc. for advance utilization and dissemination. Sensors and Actuators. Sensors and actuators act as a bridge between the Nano machine and the environment. Different sensors such as temperature, chemicals, presses, engine, etc. are usedin Nano machines.

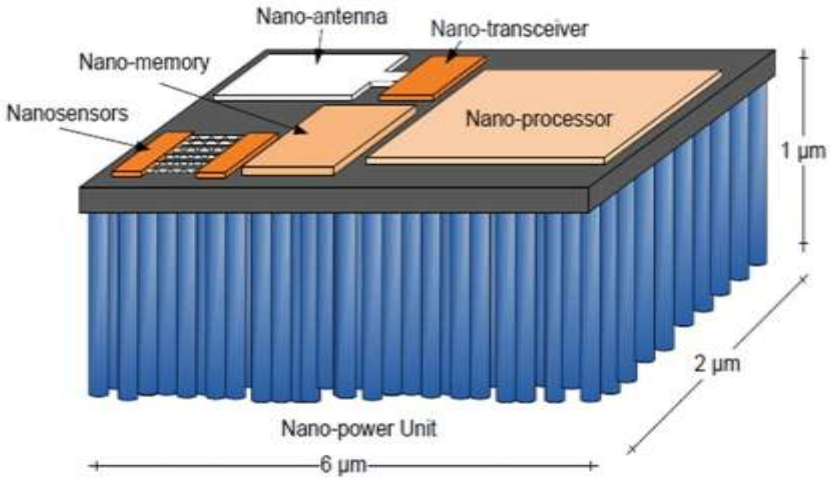

Figure 1: Nano Machine Hardware Architecture

III. EMERGENCE OF INTERNET OF NANO-THINGS

In his popular discourse "There's a Full Room at the Foot" in December 1959, Nobel Laureate in material science "Richard Feynman" displayed the thought of nanotechnology. The most reason of efficient and compact advances within the future. The term "Nanotechnology" was to begin with utilized by N. Taniguchi to portray how materials are handled, isolated, solidified and formed using as it were a single iota or atom. The most rule of the advancement and utilize of nanotechnology is the lessening and generation of objects on a scale of 1-100 nanometers. Mihail Roco of US National Nanotechnology recognized four improvements in nanotechnology.

Agreeing to Roco, the current time is inactive nanostructures that are thematerials outlined to perform a single errand. The moment stage includes "dynamic nanostructures" for multitasking, which incorporates the improvement of exceedingly productive sensors, actuators and medicate conveyance gadgets. The third era incorporates "Highlight Nano frameworks" comprising of thousands of intuitively components. Briefly, nanotechnology can be characterized as “engineering in smaller than expected – the imagined ability to construct things from the ground up utilizing apparatuses and procedures to form culminate and exceedingly progressed items. Nowadays, nanotechnology is driving to a transformation in Nano manufacturing that has critical suggestions for real-time financial, social, natural and military applications. Nano devices, IoT, sensor systems, cloud computing and huge information examination can be utilized to actualize the IoNT engineering.

The Internet of Nano Things (IoNT) has produced a few modern spaces, such as the Internet of Bio-Nano Things (IoBNT) and the Internet of Mixed media Nano Things (IoMNT), which can offer assistance, make and selection of progressed innovation in media and excitement and healthcare. The IoMNT plan incorporates Nano cameras and photo detectors, mostly utilized in broadcast communications, built at the Nano scale. The worldwide IoNT showcase is developing due to the improvement of Nano machines with communication capabilities and the integration of Nano machines with miniaturized scale- and macro-devices. In reality, Nano machines are little gadgets that have a wide extend of applications, such as sedate conveyance, nourishment control, and natural observing.

Concurring to a later advertise ponder, the worldwide IoT showcase estimate will reach USD 46.09 billion by 2028 with an income CAGR of 22.1% amid the estimate period. The major drivers for the income development of the worldwide IoNT showcase incorporate expanding government subsidizing for nanotechnology advancement, expanding number of perilous infections, and expanding private sector speculation. The worldwide IoNT showcase estimate is anticipated to develop to US dollars. 46.09 billion. In 2028, with an income CAGR of 22.1% amid the estimate period concurring to current showcase inquire about. Expanded government financing for the advancement of nanotechnology, expanding predominance of a few major maladies, and developing venture from the private segment are the major components in the market.

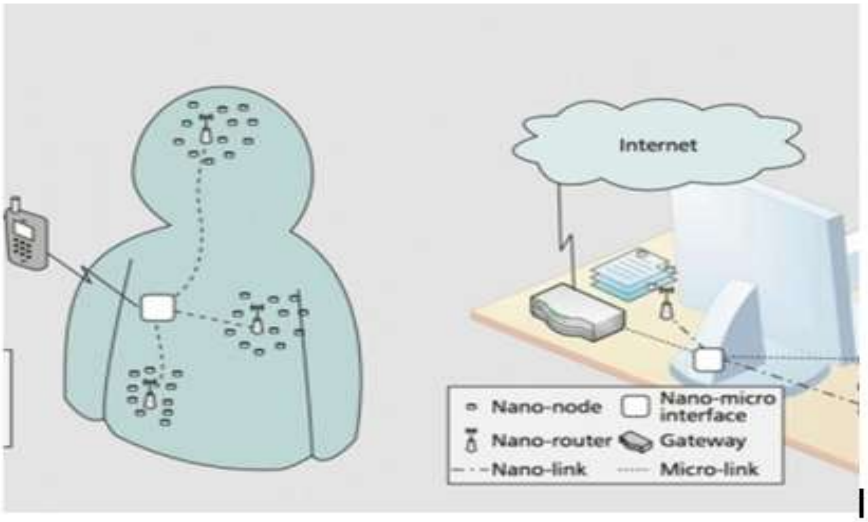

Figure 2: Typical Architecture of IoNT

IV. NETWORK ARCHITECTURE OF INTERNET OF NANO-THINGS

IoNT is gaining traction quickly in various sectors. The following elements make up the Internet of Nano Things architecture:

1. **Nano-Nodes:** The tiniest and simplest Nano machines, known as Nano-nodes, are thought to accomplish various activities, including processing, data transfer across short distances, and memory-constrained storage. Biological sensors installed in the human body are regarded as Nano-nodes in body sensor networks.

2. **Nano-Routers:** Nano-Routers operate as aggregators of data arriving from Nano-nodes and have far more computing capability than Nano nodes. Nano-routers are essential for exchanging control commands with Nano-nodes to control them.

3. **Nano-Micro Interface Devices:** Devices called Nano-micro interfaces aggregate information from Nano-routers and convey it to the micro scale, and the converse is also true. They function as hybrid devices that can transferinformation to standard communication networks using classical network protocols as well as Nano scale communication techniques.

4. **Gateway:** It makes it possible to remotely control the complete network of Nano objects from the Internet. Consider the Body Sensor Network as an example. Through the usage of a gateway, all sensor data from the human body may be accessible by doctors over the Internet from any location.

V. APPLICATION OF IoNT IN VARIOUS FIELDS

Based on the development of technology, researchers have discovered a number of IoNT applications that might be used in a variety of disciplines and have a big impact in the future. The Internet of Things (IoT) has almost reached all of the sectors that the IoT is used in at the time this article is being written. Following is a quick summary of the IoNT's applications in each of the identified domains:

1. IoNT in 5G Communication

- **Introduction:** The enriching resources in the field of Nanotechnology based applicationslead to development of the Internet of Nano-Things (IoNT) which has changed how people utilize the Internet recently. Recent advances in nanotechnology and the design of Nano scale components (such as Nano-sensors, Nano-antenna, Nano-routers, Nano-interfaces, etc.) have sparked the development of a new Nano-networking paradigm and given rise to a new class of applications and services in a variety of fields and industries, including health and agriculture. IoNT is described as the connectivity of Nano scale devices with the Internet and the most recent communication technologies. Through recent advancements in fields like spectrum management and antenna design, terahertz band communication is used to collect data from diverse objects. The culmination of all these advancements is the identification of fresh applications. On-body Nano-sensors can gather electrocardiographic data and other similar significant signals, while environmental Nano-sensors can provide information on allergies and pathogens in a specific setting. It would be considerably simpler to monitor and precisely diagnose a patient's ailments by merging this information with IoNT. A huge number of Nano-devices, gateways, and Internet connection protocols define the IoNT paradigm. In many sectors, it can reduce the expense and complexity of data processing. But it's crucial to consider crucial IoNT characteristics like security, privacy, dependability, secrecy, and interoperability in the new paradigms.

- **Iont Market Opportunity in 5G/Big Data Era**: In the upcoming years, it is estimated that the number of linked devices will expand quickly. Intelligent communication paradigms are needed to enable effective interaction amongst various devices. To serve the increasingly expanding big data project, these intelligent paradigms can process data of various volumes and complexities effectively. Keep in mind that the six dimensions known as the "6 Vs" are what define big data the most.

- **Iont Architecture in 5 G/Big Data:** Understanding the IoNT architecture gives us a strong understanding of the necessary security functionalities. Nano-nodes are the end points, such as Nano-actuators and Nano-sensors that are capable of carrying out basic processing and computation functions.

- **Iont Design Factors:** The fifth generation mobile phone network (5G) is expected to enter the market soon. One of the most important defined goals is communication anywhere, anytime between anyone and anything. This section presents the key design factors of the IoNT paradigm that significantly affect performance in terms of security, energy efficiency and quality of service (QoS).

- **Intelligence and IoNT:** The instrumented and interconnected paradigms of IoNT make the best use of information obtained from sensors and systems of different scales when an intelligent approach is used. In each IoNT paradigm, it is typical to observe the use of artificial intelligence (AI), especially machine learning (ML)techniques, providing citizens with the best lifestyle to improve the use of available network resources in addition to using the Machine Learning method in optimization.

- **Iont Physical Layer & 5G/Big Data:** Nano mechanical, acoustic, electromagnetic, and chemical or molecular communication can be used in Nano network communication. A comparison with existing communication technologies can be seen in Table 3. Physical signaling occurs at the terahertz (THz) level. Therefore, special modulation techniques are required due to the required antenna sizes. On the other hand, the use of graphene-based plasmonic materials in antennas to overcome signal difficulties is being investigated.

- **Iont Communication Technologies:** In this section, we highlight the various secure communication techniques in the aforementioned IoT architecture. Based on the communication component/device, these technologies can be divided into:
  - Nano sensor to Nano sensor/interface.
  - Internet Communication Technologies User Interface.

- **Restrictions in Secured IoNT:** Each secure IoNT paradigm has several constraints that can be classified as primary and secondary constraints. Key constraints are the most important constraints that must be met to effectively achieve a secure IoT paradigm. Energy consumption is one of the most important constraints that must be met for a secure IoT implementation. In IoNT, the full energy of a Nano device is usually sufficient to send at most one packet.

- **Assessment & Tools:** The emerging 5G/Big-Data project not only deals with massive amounts of manipulated data, but also its use. With the help of IoNT, any object or device, even Nano scale, can be connected to the Internet and thus generate huge amounts of data. That is why advanced evaluation methods and benchmarking tools are extremely important in this era.

2. **Nano Sensors and the Internet of Things:** Analysts have started contracting sensors from millimeters or microns down to the nanometer scale, little sufficient to circulate interior living bodies and mix specifically into building materials. Typically a vital to begin with step towards Nano-objects (IoNT), which can bring pharmaceutical, vitality proficiency and numerous other areas to a entirety unused measurement. A few of the foremost progressed Nano sensors to date have been made utilizing manufactured science apparatuses to build single-celled living beings such as microbes. The objective is to

create basic bio computers that use DNA and proteins to recognize specific chemical targets, store many bits of data, and after that report their status by changing color or sending a few other effortlessly distinguishable flag. Cambridge, Mass.-based startup Synlogic looks for to commercialize computer-accessible strains of probiotic microscopic organisms for the treatment of uncommon metabolic disarranges.

In expansion to pharmaceutical, such cellular Nano sensors may too discover numerous employments in horticulture and the pharmaceutical industry. Numerous Nano sensors are moreover made of non-biological materials, such as carbon nanotubes, which can both sense and flag, acting as wireless Nano antennas. Since Nano sensors are so little, they can collect information from millions of diverse focuses. Outside gadgets can at that point coordinated the information to form fantastically gritty maps that appear indeed the littlest changes in light, vibrations, electrical streams, attractive areas, chemical concentrations and other natural conditions. The move from shrewd Nano sensors to IoT appears unavoidable, but imperative challenges remain to be overcome. One specialized jump is coordination of all the essential components into a self-powered Nano device to identify the changes and send the signal to the web. Other deterrents incorporate the complex issues of protection and security. Any Nano device presented into the body intentioned or incidentally can be harmful or cause resistant responses. The innovation may too empower undesirable following.

The primary applications may be able to maintain a strategic distance from the most troublesome issues by joining Nano sensors into less difficult, less hazardous life forms, such as plants and non-infectious microorganisms utilized in mechanical handling. When it arrives, IoT may give distant more point by point, available and up-to-date pictures of our cities, homes, production lines – indeed our bodies. Nowadays, activity lights, versatile gadgets or observation cameras interface to the Web. Another: Billions of Nano sensors collect enormous sums of real-time information and send it to the cloud.

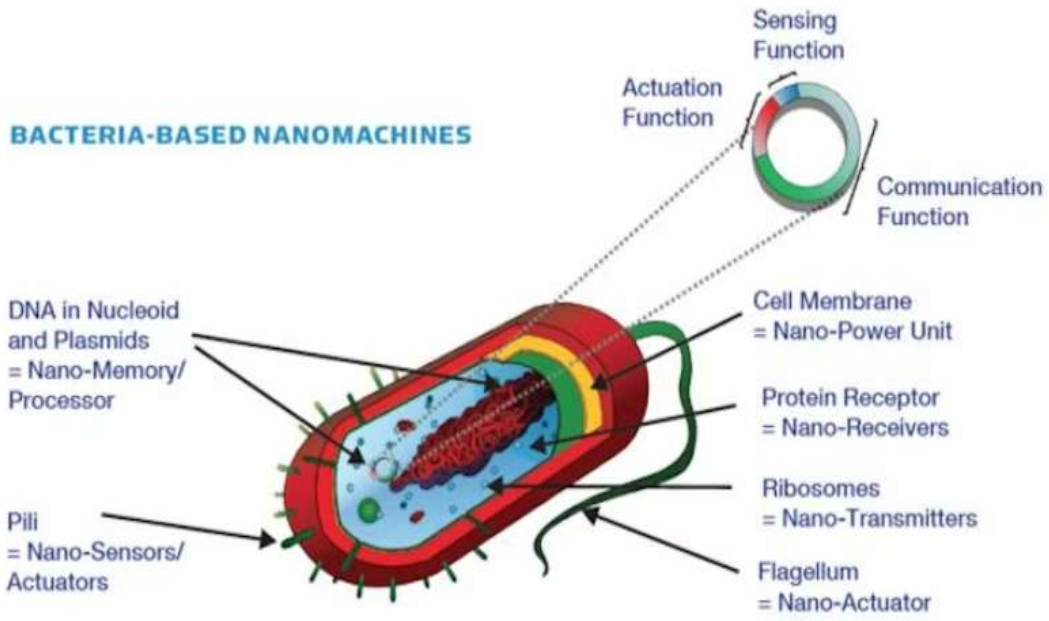

Figure 3: Bacteria-based Nano Sensors

3. **Iont in Developing Smart Cities:** The execution of a keen city empowers interaction and interaction with domestic applications through the checking of different perspectives related to the urban environment utilize shrewd sensors, reconnaissance cameras, drives, vehicles and much more advanced gadgets within the hands of city tenants, which encourages superior city administration to like presently keen cities are already built up with the aid of IoT where Nano sensors are utilized to track and identify the area of airborne flotsam and jetsam with tall receptiveness ranges and actuate the Nano sensors to clear the range. IoT features a collection capability real-time data that can at that point be utilized to progress open services, services, framework and much more within the setting of a shrewd city. In differentiate, with the assistance of IoNT with the arrangements, city partners can accumulate real-time data to move forward lodging level of natives living within the city.

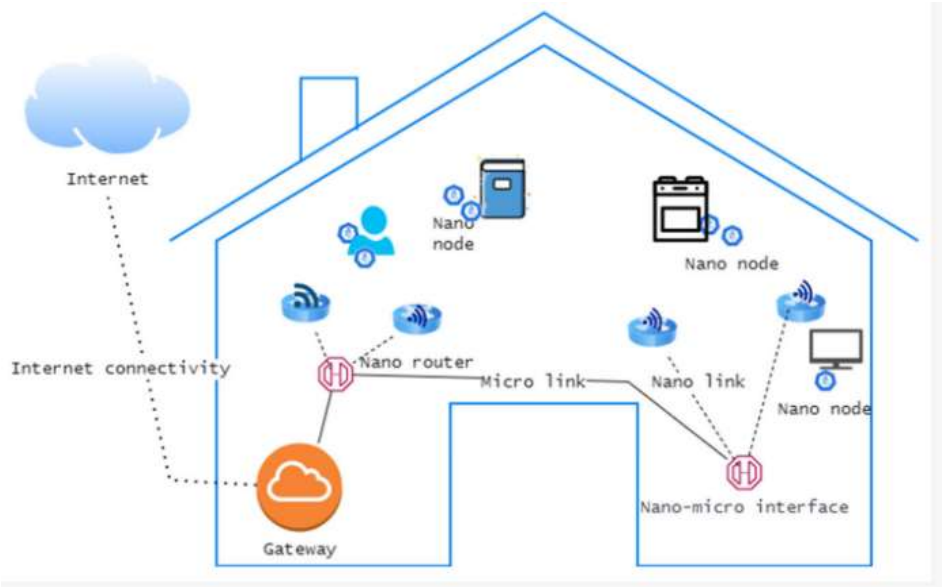

Figure 4: Network Architecture in a Smart Home of a Smart City

4. **IoNT in Agriculture:** The agricultural food production of the world is currently under threat from a numerous factors, including unpredictable climate change, pests, and diseases despite the numerous efforts made to address these threats in order to feed the expanding global population. The necessity for smart farming solutions has already been highlighted by this, with the IoT serving as its primary supporting technology. In this context, the IoNT is currently coupled with smart agriculture in various different ways. For instance, Nano sensors are used to track crop growth, water use, and soil conditions, as well as to improve resource management and cut waste. Typically, facilities may monitor crop health, soil quality, and moisture levels using Nano sensors. In general, facilities can use Nano sensors to continuously monitor soil quality, crop health, and moisture levels. Additionally cheers to the IoNT, farmers may now gather a wealth of data that will help them optimize their procedures and raise yields. Nano sensors are also used to monitor the feed given to agricultural animals, such as cattle, track the whereabouts of those animals, and keep a careful check on their health. Additionally**,** in order to monitor underlying diseases in animals and improve their overall health, Nano scale biosensors are injected within the animals. These injected sensors provide unmatched access to data on the dietary and medical requirements of farm animals.

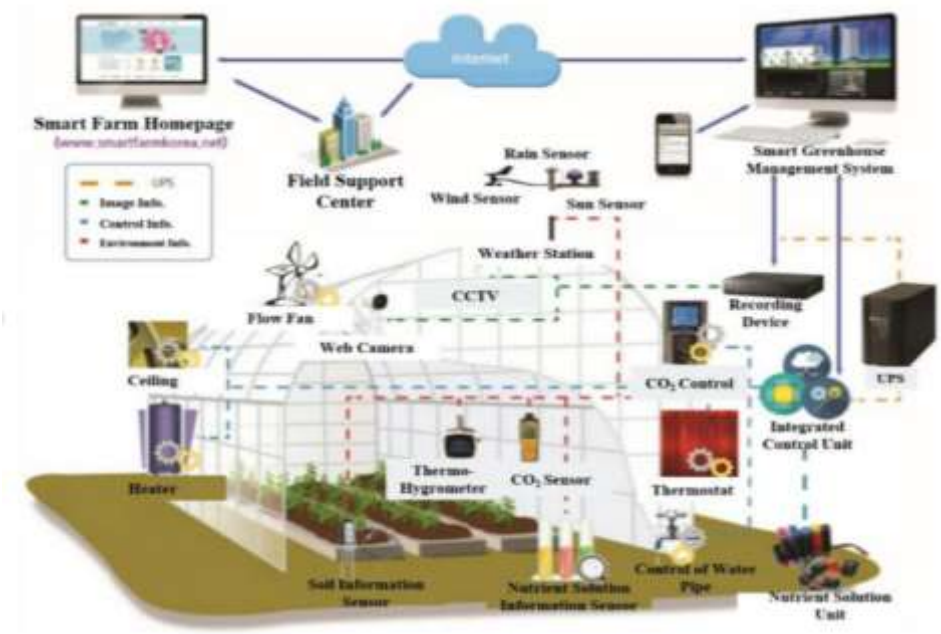

Figure 5: Typical Design of IoNT in Smart Farming

5. **IoNT in Oil and Gas Industry:** Owing to the intrinsic properties of Nano sensors, the IoNT provides practical methods to accurately locate subterranean oil. Since it requires on a robust magnetic field and a receiver inside a specific system to transport Nano composites to the appropriate area, the usual method for locating oil is less successful than this. Finding oil linked to the rocks is made easier because to Nano sensors' capacity to successfully pass through rock holes. Although their stiffness level requires improving, several seismic and cross-well imaging technologies have a more notable impact in this field. In contrast, molecular communication enables Nano sensors to cooperate and interact, and the data they collect can be sent in real time by using a nearby gateway. Therefore, it is not necessary to plot the location of the oil using a precise magnetic source and receiver.

6. **Iont in Facilitating the Military:** Biological and chemical weapons have emerged as practical alternatives as military techniques have developed over time to deal greater damage with fewer resources. The Internet of Nano-Things (IoNT) can employ Nano sensors in the military to identify biological and chemical threats by detecting the presence of chemical compounds in concentrations of even just one molecule. Nano sensors can also find minute faults in fabrics, rockets, vehicles, bridges, and other civil engineering projects. Other IoNT components in the military include Nano-Drones which are utilized for surveillance operations and transporting explosives for military forces.

7. **IoNT in Environment Monitoring:** Nano sensors are employed to detect and monitor environmental factors, such as weather patterns, soil conditions, and the quality of the air and water. Resource management could be improved, the environment could be preserved, and climate change's consequences could be lessened with the aid of this information. In the framework of a smart city, IoNT systems are utilized to track current environmental conditions and produce alerts or replies in accordance with underlying circumstances**.**

8. **IoNT for Smart Packaging:** Relating to smart packaging Over the past several years, there has been a sharp increase in the amount of research being done in the subject of nanotechnology. Several businesses are now concentrating on developing novel types of Nano scale materials. The food industry is one sector that is beginning to take notice of this, which is not surprising given that the public's preference for natural food products has historically prevented the adoption of cutting-edge food technologies. Indeed, wrapping is the field of food Nano science that is currently experiencing the most expansion and research. The sealing of food packaging can be significantly improved by adding nanomaterial compounds like SiO2, TiO2, and KMnO4.

9. **IoNT in Administering Transports:** The effectiveness and security of transport networks are increased appreciations to the IoNT. Nano sensors, for instance, are employed to optimize routes for traffic or to spot and avoid accidents.

10. **IoNT in Healthcare and Telemedicine:** Healthcare is an area where IoT solutions are widely used in recent times compared to all other areas. Nanotechnology in the form of Nano medicine, Nano implants, Nano biosensors and the Internet of Nano-Things (IoNT) can bring revolutionary advances in medicine and healthcare.

Body Sensor Network (BSN) is an application of IoNT in the field of healthcare. It uses various sensors implanted in the human body to obtain relevant observations and diagnostically valuable information that is otherwise beyond the reach of traditional diagnostic methods. IoNT provides a Nano-network between different Nano-biosensors. Through IoNT, health information detected by biosensors is available to doctors, medical service providers, the patient and his relatives, etc. Thus, IoT actually provides a ubiquitous health system that enables continuous and real-time monitoring about the patient's health anywhere and anytime. This not only allows for immediate attention, but also allows for early detection and diagnosis of the disease. It also ensures cost-effective, accurate and efficient patient-tailored treatment and rehabilitation.

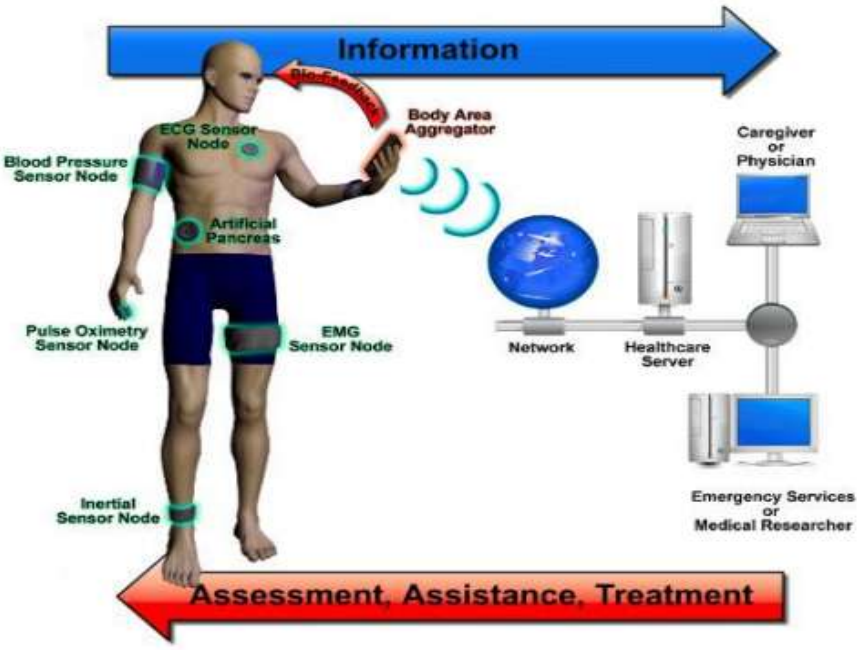

Figure 6: Real Time Health Monitoring via Nano Sensors

- **Working Principle of Body Sensor Network based on IoNT:** Doctors won't have to manually measure patients anymore if IoNT makes a breakthrough in healthcare. Instead, they will be capable of monitoring patients in real time. A typical healthcare IoNT solution, as seen in the Figure 7, consists of many Nano sensors that may broadcast the sensory data they have gathered to an external device, like a smartphone or internet gateway, enabling healthcare personnel to continuously monitor underlying patient data to conditions. Components of IoNT architecture in healthcare systems are

  - **Nano-Nodes/Nano Biosensors:** The Nano Bio sensors are capable of reception of various body parameters of the patient. Biological sensors installed in the human body are regarded as Nano-nodes in body sensor networks.
  - **Nano-Routers:** Nano-routers are essential for exchanging control commands with Nano-nodes to control them.
  - **Nano-Micro interface devices:** Devices called Nano-micro interfaces aggregate information from Nano-routers and convey it to the micro scale.
  - **Gateway:** The gateway devices in IoNT are usually a smartphone, tablets, PDAs or other wireless communication enabled handheld devices. Nano-micro interface communicates with gateway devices to send data and receive commands from the remote healthcare provider.

The real-time data regarding the patient's various body parameters get recepted by the Nano Biosensors implanted in the patient's body and are aggregated in the Nano nodes that transmits the data by the Nano routers to Nano micro interface devices from where the data gets broadcasted or stored in the various gateway devices. Accessing the gateway devices, the healthcare providers and the patient's caregivers can get the access of the patients health related data. Hence, this enlightens the contribution of IoNT towards the healthcare domain.

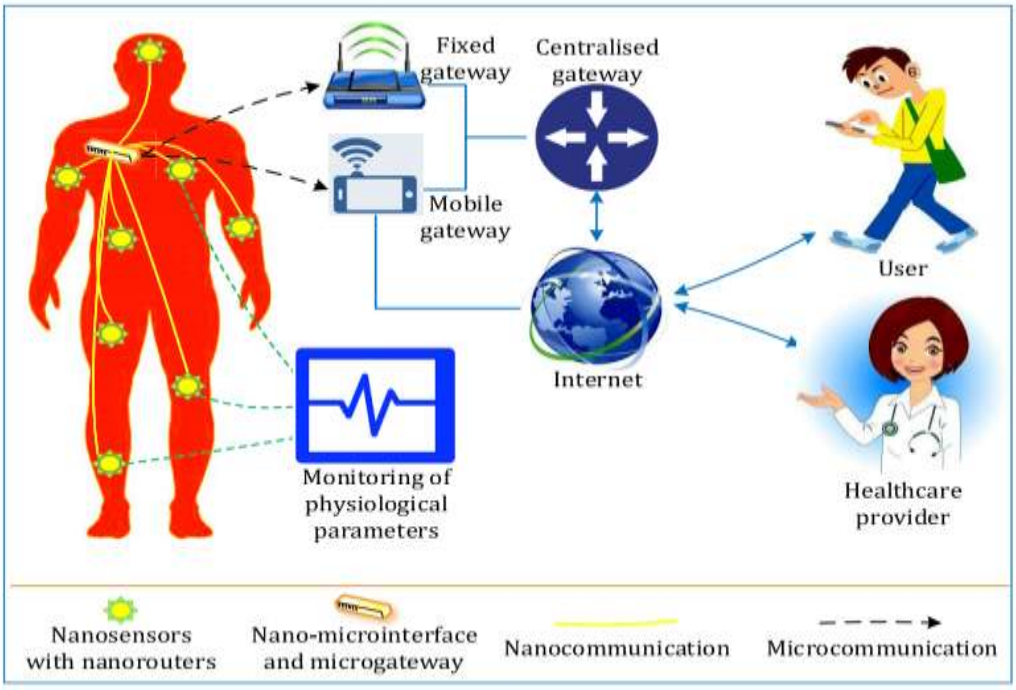

Figure 7: Application of IoNT in Healthcare

The monitoring of a specific human organ is provided by a healthcare system powered by nanotechnology. A smart drug distribution system also uses this kind of healthcare system. The Nano gadgets can be placed inside the human body or outside. There are a various kinds of Nanotechnology based products in the market that can be worn as clothing or even monitored via mobile devices.

IoNT is divided into the following three major Nano networks depending on where a Nano-medical device is implanted on or within the body:

- **Off-body systems:** Off-body networks are implemented in a person's environment like their house, car, street, or hospital. Besides supporting applications for ambient living, these networks can offer general health and environmental monitoring services.
- **On-body systems:** Body area networks and wearable technology are examples of on-body networks. These technologies allow for the mass customization of health monitoring and alarm apps and bring medical services closer to the patient's home or other private location.
- **Intra-body systems**: It is anticipated that intra-body networks would be installed at various points inside the human body, either as networked Nano devices or connected, implanted smart monitoring devices.

The Internet of Bio-Nano Things (IoBNT) is a space where the biochemical operations taking place inside the human body can communicate with the online virtual environment. The IoBNT model is a product of a synthetic biology and nanotechnology tool that enables the design of biological embedded computer systems, also known as Nano machines. Nano machines are powerful, useful, and tiny man-made gadgets. The behavior of atomic and molecular structures made up of Nano size components serves as an inspiration for these devices' functionality.

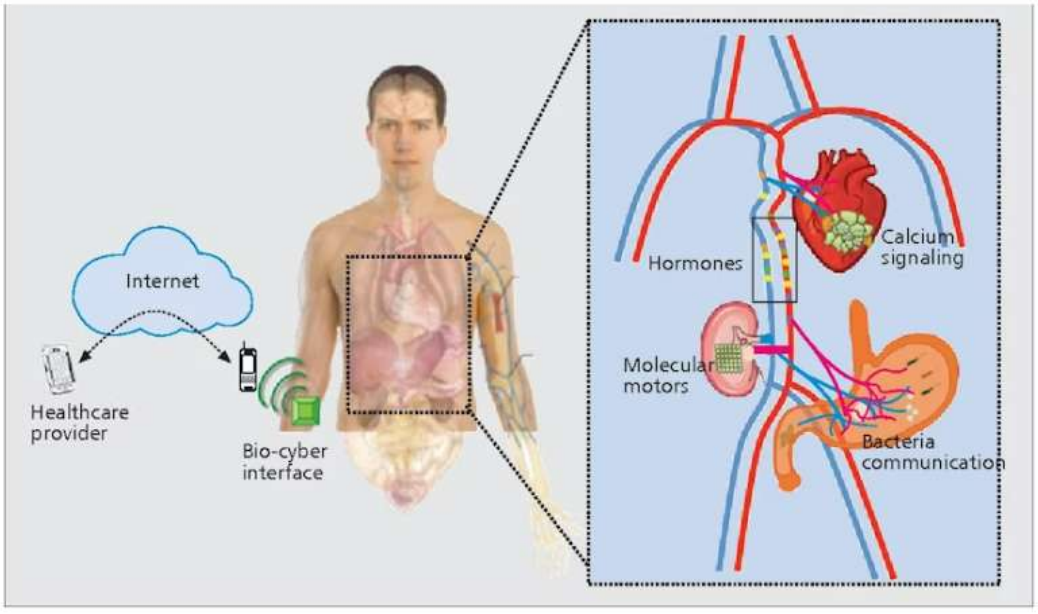

Figure 7: Architecture of Internet of Bio Nano-Things

Another revolutionary innovation in IoNT in healthcare domain is the IoNT driven smart face masks to combat the airborne health hazards. The Nano nodes and Nano routers can be installed within the face mask and the contact of airborne bacteria and virus may produce the structural changes in the nanomaterial. The changes will be converted to digital data via Nano biosensor embed in the face mask. The digital data will then process to Nano nodes and Nano routers to different fixed as well as mobile gateways. The signal from gateways will be processed through internet and finally reach to user at another destination or doctor. This arena of telemedicine is enthusiastic for the researches and scientists.

Figure 8: Schematic representation IoNT driven Smart Face Masks

VI. ADVANTAGES OF INTERNET OF NANO-THINGS

It is clear that the IoNT is currently provided in practically all of the IoT areas. Due to its miniaturized nature, the IoNT fared better (than the IoT) in each of these fields, depending on the situation. As a result, the following are some possible benefits of the IoNT:

1. **Improved Accuracy:** Compared to larger devices, Nano scale devices can be used to measure and monitor with a considerably better degree of accuracy since they are so small. This can be especially helpful in situations when accuracy is essential, such as in the diagnosis and treatment of illness.

2. **Higher Sensitivity:** Nano devices can be made to be extremely responsive to a variety of stimuli, including changes in pressure, temperature, or chemical composition. Due to this, they may be able to notice and react to environmental changes that larger equipment would be unable to notice.

3. **Greater Energy Efficiency:** Since Nano scale devices are so tiny, they require extremely low levels of power to function.

4. **Miniaturization:** The ability to create incredibly small devices is one of nanotechnology's main benefits. This might result in the creation of wearable or implantable Internet of Things devices that are less intrusive and easier to operate.

5. **Increased Durability:** Compared to their larger equivalents, Nano scale components are frequently more durable and resistant to wear. This might result in IoT devices that survive longer and need less upkeep and repair over time.

VII. SECURITY AND PRIVACY CHALLENGES OF INTERNET OF NANO-THINGS

The IoNT is in some cases alluded to as a scaled down frame of the IoT that has a noteworthy potential for joining into real-time applications. In show disdain toward of the reality that it offers unbounded preferences, the IoNT is tormented by a number of impediments that ought to be overcome some time recently it can be considered an irreplaceable component of people within the not-too-distant future and without any limitations.

These gadgets are associated to the Web and have digitalized control and observing forms, which postures a few security and protection concerns. Another completely modern degree of security-related challenges is brought almost by the integration of Body Region Systems frameworks with body contraptions and Nano machines. The security of information transmitted over the Web is one of the foremost critical troubles brought on by the development of the Internet of Nano Things. People's private wellbeing data, for occurrence, can be stolen in a bio-cyber-attack within the healthcare industry. This information can be utilized to create unused infection sorts that can enter already-installed Nano sensors within the Web of Nano Things. Subsequently, 4G communication systems ought to execute security affirmation measures.

Given that this kind of contraption does not meet with consistent consideration, the Internet of Nano Things is vulnerable to all assaults, both physical and wireless. Attacks may be carried out to take private information from sensors, stop computer-controlled computer program programs, or modify the Nano networks' communication joins. Usually due to the fact that miniaturized scale systems that work in the terahertz range cannot be secured using conventional security measures. Unused security measures must be made in arrange to ensure the IoNT system.

Potential get to and control of Nano gadgets by unfriendly on-screen characters postures a noteworthy security chance to the IoNT. Since these gadgets are regularly coordinates into or inserted in greater frameworks, a security or protection compromise on one gadget seem have far-reaching impacts on those larger frameworks. For instance, a programmer may be able to get to a Nano robot utilized in therapeutic strategies and alter its working by jeopardizing the security of endpoint or miniaturized scale organize gadgets through tainted malware, with conceivably dangerous comes about. The plausibility for following and surveillance by Nano gadgets postures another danger.

Strong security strategies, counting encryption and confirmation conventions, should be put in put by businesses and people to watch against unauthorized get to Nano gadgets in arrange to address these concerns. To assure the secure and mindful improvement and

sending of modern innovations, it is similarly pivotal for governments and businesses to make and implement directions and benchmarks. Security and privacy challenges of IoNT are as follows:

1. **Lack of Encryption:** Failure to encrypt sensitive data shared between Nano devices results in a number of security difficulties that get progressively worse, such as the ability for attackers to eavesdrop on the sensitive data that is being transmitted.

2. **Internet Exposure:** The IoNT becomes susceptible due to this ongoing connection to the Internet since it makes it possible for invaders to use the Internet to take advantage of known software and hardware flaws.

3. **Denial of Service:** Distributed Denial of Service or DDOS, is an aggressive variation of a denial-of-service attack that uses more compromised nodes to overwhelm the system. It becomes more challenging to pinpoint the attack's starting point as a result.

4. **Wearable Malware Threats:** Since Bluetooth uses frequency hopping, which enables multiple devices to simultaneously transmit a signal over the same frequency, wearable gadgets may attract malicious software as tempting targets. This raises the likelihood that attackers may intercept signals and steal crucial data from these unencrypted sources.

VIII. SECURITY GOALS OF INTERNET OF NANO-THINGS

1. **Authenticity:** It must be ensured that the message's transmission source is trustworthy and guards against an attacker sending fake messages.

2. **Availability:** It must be impossible for a malevolent user to obstruct or negatively impact communication or the level of service offered by Nano devices or Nano networks. Therefore, IoNT availability for components working at both the micro scale and the Nano scale should be ensured.

3. **Confidentiality:** The content of communications sent back and forth between a sender and a recipient shouldn't be accessible to an attacker. This means that, in our scenario, secrecy must be assured outside of the Body Area Network, for example, by utilizing encryption techniques.

4. **Integrity:** It refers to the preservation of data's coherence, accuracy, and dependability over the course of its whole existence. Data cannot be changed while in transit, and measures must be made to prevent it from being changed by bad users.

IX. SECURITY MECHANISMS OF INTERNET OF NANO-THINGS

The security of IoT systems is discussed in this part, and the following approaches are taken into consideration for establishing secure communications in Nano sensor networks. They are as follows:

1. **Key Management:** It is commonly acknowledged that the primary task at the core of almost any key management system is the distribution of security keys, such as public and private encryption keys. Key pre-distribution can be used to distribute keys prior to

deployment or before any data transmission occurs. These two approaches are both practical choices. It is essential to be able to restrict access to a key once it has been compromised. One of the most challenging issues with sensor networks and IoNT systems is still this one. Standard operating processes for generating shared keys must be established, as must the conditions under which keys may be revoked.

2. **Cryptography Advancements:** The effectiveness of classical cryptography may decline with the introduction of quantum computing. Therefore, new encryption methods that can withstand quantum attacks are required. In order to ensure security for the IoNT, post-quantum cryptography is an area that is currently being studied and developed.However for Body Nano Communication, we need more portable options as the suggested biochemical cryptography.

3. **AI-Based Security:** Real-time security threat detection and response within the IoNT is possible using AI techniques. Malicious Nano device detection and blocking, real-time and distributed denial-of-service assaults detection and mitigation, and recognizing and responding to suspicious network activity are some examples of this.

4. **Edge and Fog Computing Techniques:** The management and processing of the data produced by these devices will get harder as more Nano devices are connected to the IoNT. By bringing processing and storage closer to the devices, edge and fog computing can reduce the need to send sensitive data over the Internet.

5. **Block Chain-Based Techniques:** To manage the identities and interactions of Nano devices in the IoNT in a secure and transparent manner, block chain technology's decentralization and immutability can be implemented.

6. **Access Control and Authenticity:** To ensure the goal of confidentiality, authentication is necessary. All messages intended for Nano communication systems must pass through a gateway and undergo authentication. Typically, traditional symmetric or asymmetric cryptography is used to provide authentication. Biological molecules like DNA and RNA are used in biochemical cryptography, a relatively new and unexplored topic, to encrypt data and safeguard its confidentiality and integrity.

X. MARKET ANALYSIS OF INTERNET OF NANO-THINGS

The relatively recent succession of Nano-scale gadgets and the systems created utilizing them can be used to describe the global market for the internet of Nano things. Thus, his worldwide market for the "Internet of Nano things" denotes a market devoted to enabling connectivity amongst Nano-scale systems for improved data gathering, processing, and directing. Additionally, it enables a more seamless transition when sharing the data with the various end users. Retail, media and entertainment, energy and utilities, transportation and logistics, manufacturing, and healthcare are just a few of the sectors that now make use of the worldwide internet of Nano things market. The IoNT is made up of a network of several physical objects at the Nano scale that communicate with one another via nanotechnology. IoNT market is anticipated to grow, according to latest research.

The market size for the Internet of Nano Things is projected to be USD 22.02 billion in 2023 and USD 55.31 billion in 2028, rising at a CAGR of 20.23% over the forecast period (2023-2028).

The major market participants concentrated on upgrading the solutions and forming strategic alliances, which created more prospects for the IoNT Market. At the CES in January 2022, Qualcomm Technologies, Inc. and Microsoft announced a partnership to expand and hasten the uptake of augmented reality (AR) in both the consumer and business markets. Both businesses support the metaverse, and Qualcomm Technologies and Microsoft are working together on a number of initiatives to advance the ecosystem.

IoNT market is anticipated to expand from approximately USD 5 billion in 2016 to USD 10 billion by 2020, as shown in Figure 9, at an estimated pace of more than 24.12% for the present forecast period of 2016 to 2025.

Figure 9: Market growth of Internet of Nano-Things by region

It is anticipated that the healthcare and life sciences sector would expand significantly during the projection period. IoNT helps with the real-time data collection from patients and can identify life-threatening illnesses early on, enabling life-saving medical interventions.

In 2022, the American Cancer Society predicts that 1.9 million new cancer cases and 609,360 cancer deaths will be recorded in the country. As a result, the growing incidence of cancer drives the growth of the healthcare nanotechnology sector. This will significantly evoke the hype of the market of IoNT.

The players in the global internet of Nano things are anticipated to be concentrated in North American and European developed economies, which have more extensive IoT and IoNT usage. In contrast to developing economies, which have only recently shown a greater level of interest in the industry, a larger variety of companies in the global IoNT market are present in these regions.

Among the top companies in the IoNT market are Intel Corporation, Cisco Systems Inc., Qualcomm Incorporated, Juniper Networks, and IBM Corporation in the United States, Schneider Electric and Alcatel-Lucent S.A. in France, SAP SE and Siemens AG in Germany and Schneider Electric and Alcatel-Lucent S.A. in France.

XI. CONCLUSION

The IoNT, which is rapidly developing with applications in smart cities, smart agriculture, the military, healthcare, and other fields, has been made possible by the rapid advancement of nanotechnology and its integration with the IoT. The IoNT is rapidly becoming a necessary component of our daily lives due to its miniaturized nature and the enormous advantages that may be anticipated compared to its counterpart, the IoT. Although technology has many advantages, using IoNT technology comes at a price because of Internet connectivity, built-in weaknesses, and miniaturization, which outweighs the majority of the advantages and creates serious security and privacy concerns.

In the study, we gave a general overview of the IoNT and highlighted the present research status, its architecture, its different uses and advantages, and its security and privacy. We've quickly covered the difficulties with the IoNT that prevent proper adoption of security and privacy in the context of security and privacy. In addition, we have classified security and privacy threats according to the attack routes used, offered defenses, and predicted future research areas. Overall, we have emphasized that security must be an essential component of IoNT, whether it is at the Nano scale or the micro scale.

Hence we can conclude that The Internet of Nano Things (IoNT) paradigm will take IoT to a new level that will eventually benefit the mankind in the near future.

REFERENCES

[1] M.H.Miraz, M.Ali, P.S.Excell, R.Picking, "A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)", 2015.
[2] A.Alabdulatif, N.N.Thilakarathne, Z.K.Lawal, K.E.Fahim, R.Y.Zakari, "Internet of Nano-Things (IoNT): A Comprehensive Review from Architecture to Security and Privacy Challenges",Sensors 2023,23,2807,3 March,2023.
[3] P.K.D.Pramanik, A.Solanki, A.Debnath, A.Nayyar, S.El-Sappagh, K.S.Kwak, "Advancing Modern Healthcare with Nanotechnology, Nanobiosenosrs, and Internet of Nano Things: Taxonomies, Applications, Architecture, and Challenges", April 17, 2020.
[4] A.O.Balghusoon, S.Mahfoudh, "Routing Protocols for Wireless Nanosensor Networks and Internet of Nano Things: A Comprehensive Survey", volume 8, 2020.
[5] Akyildiz I.F., Jornet J.M. The Internet of nano-things. IEEE Wirel. Commun. 2010;17:58–63. doi: 10.1109/MWC.2010.
[6] Agarwal K., Agarwal K., Agarwal S. Evolution of Internet of Nano Things (IoNT) Int. J. Eng. Technol. Sci. Res. 2017;4:274–277.
[7] Kulakowski P., Solarczyk K., Wojcik K. Routing in FRET-Based Nanonetworks. IEEE Commun. Mag. 2017;55:218–224. doi: 10.1109/MCOM.2017.1600760.
[8] Atlam H.F., Walters R.J., Wills G.B. Internet of Nano Things: Security Issues and Applications; Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing—ICCBDC'18; Barcelona, Spain. 3–5 August 2018; pp. 71–77.
[9] Ali N.A., Aleyadeh W., AbuElkhair M. Internet of Nano-Things network models and medical applications; Proceedings of the 2016 International Wireless Communications and Mobile Computing Conference (IWCMC); Paphos, Cyprus. 5–9 September 2016; pp. 211–215.
[10] V.Chaudhary, A.Goutam, P.Silotia, S.Malik, R.O.Hansen, M.Khalid, A.Khosla, A.Kaushik, Y.K.Mishra, "Internet-of-nano-things(IoNT) driven intelligent face masks to combat airborne health hazard.", Volume 60, November 2022, Pages 201-226.

