Attia, Tarek M.

**Conference Paper**

# Challenges and Opportunities in the Future Applications of IoT Technology

2nd Europe - Middle East - North African Regional Conference of the International Telecommunications Society (ITS): "Leveraging Technologies For Growth", Aswan, Egypt, 18th-21st February, 2019

**Provided in Cooperation with:**

International Telecommunications Society (ITS)

*Suggested Citation:* Attia, Tarek M. (2019) : Challenges and Opportunities in the Future Applications of IoT Technology, 2nd Europe - Middle East - North African Regional Conference of the International Telecommunications Society (ITS): "Leveraging Technologies For Growth", Aswan, Egypt, 18th-21st February, 2019, International Telecommunications Society (ITS), Calgary

This Version is available at:
http://hdl.handle.net/10419/201752

# Challenges and Opportunities in the Future Applications of IoT Technology

**Dr. Tarek M. Attia**
National Telecom Regulatory Authority (NTRA)
K28, Cairo-Alex. Desert Road, Smart Village, Giza, Egypt.
tattia@tra.gov.eg

**ABSTRACT**

The advent of internet of things (IoT) has influenced and revolutionized the information systems and computing technologies. A computing concept where physical objects used in daily life, will identify themselves by getting connected to the internet is called IoT. Physical objects embedded with electronic, radio-frequency identification, software, sensors, actuators and smart objects converge with the internet to accumulate and share data in IoT. IoT is expected to bring in extreme changes and solutions to most of the daily problems in the real world. Thus, IoT provides connectivity for everyone and everything at any time. The IoT embeds some intelligence in Internet connected objects to communicate, exchange information, take decisions, invoke actions and provide amazing services. It has an imperative economic and societal impact for the future construction of information, network, and communication technology. In the upcoming years, the IoT is expected to bridge various technologies to enable new applications by connecting physical objects together to support the intelligent decision making.

As the most cost-effective and performant source of positioning and timing information in outdoor environments, the global navigation satellite systems(GNSS) has become an essential element of major contemporary technology developments notably including the IoT, Big Data, Smart Cities and Multimodal Logistics.

By 2020, there will be more than 20 billion interconnected IoT devices, and its market size may reach $1.5 trillion. Projections for the impact of IoT on the Internet and economy are impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025.

Regulators can play a role in encouraging the development and adoption of the IoT, by preventing abuse of market dominance, protecting users and protecting Internet networks while promoting efficient markets and the public interest. Regulators can consider and identify some measures to foster development of the IoT. Encourage development of LTE-A and 5G wireless networks, and keep need for IoT-specific spectrum under review. Universal IPv6 adoption by governments in their own services and procurements, and other incentives for private sector adoption. Increasing interoperability through competition law and give users a right to easy access to personal data. Support global standardization and deployment of remotely provisioned SIMs for greater machine to machine competition. Particular attention will be needed from regulators to IoT privacy and security issues, which are key to encouraging public trust in and adoption of the technology.

This paper focuses specifically on the essential technologies that enable the implementation of IoT and the general layered architecture of IoT, the market of IoT and GNSS technologies and their impact of the world economy, application domain of IoT and finally the Policy and regulatory implications and best practices.

**KEYWORDS:** Internet of Things(IoT), Global Navigation Satellite Systems(GNSS), Applications, Marketing, Policy and Regulation.

## 1. Introduction

This new era of 5G promises speeds of 1-10Gbits/s, more data bandwidth, and fewer delays due to built-in computing intelligence that handles data very efficiently and will bring together improved connectivity, cloud-based storage, and an array of connected devices and services. Extensive computing capability combined with virtual system architecture will open up a mobile IoT[1,2]. Advanced digital networks will bring together a system that connects billions of devices and sensors enabling advances in health care, transportation, agriculture, environmental monitoring, education, resource management and many other areas.

It is important to note that 5G is an end-to-end system that shifts communications to a computing platform. 5G represents an evolution from a point-to-point system to one that senses data from billions of devices and works to move those communication packets seamlessly to the right device, using the appropriate processing platform.

Connected devices will enable people to enjoy more personalized, more immersive, and more enhanced experiences whenever and wherever they are. With the costs of devices and sensors coming down considerably, connectivity will be ubiquitous and unobtrusive. Rather than having to make a conscious decision to issue a computing command, people will have systems that take actions based on the predetermined preferences of that individual.

With the advancement in technology, we are moving towards a society, where everything and everyone will be connected. The IoT is considered as the future evaluation of the Internet that realizes machine-to-machine (M2M) learning. The basic idea of IoT is to allow autonomous and secure connection and exchange of data between real world devices and applications. The IoT links real life and physical activities with the virtual world [3].

The numbers of Internet connected devices are increasing at the rapid rate. These devices include personal computers, laptops, tablets, smart phones, PDAs and other hand-held embedded devices. Most of the mobile devices embed different sensors and actuators that can sense, perform computation, take intelligent decisions and transmit useful collected information over the Internet. Using a network of such devices with different sensors can give birth to enormous amazing applications and services that can bring significant personal, professional and economic benefits [3].

The IoT consists of objects, sensor devices, communication infrastructure, computational and processing unit that may be placed on cloud, decision making and action invoking system. The objects have certain unique features and are uniquely identifiable and accessible to the Internet. These physical objects are equipped with Radio-Frequency Identification (RFID) tags or other identification bar-codes that can be sensed by the smart sensor devices. The sensors communicate object specific information over the Internet to the computational and processing unit. A combination of different sensors can be used for the design of smart services. The result of processing is then passed to the decision making and action invoking system that determines an automated action to be invoked. There is a lot of pervasive presence in the human environment of things or objects, such as Figure.1 described general overview of internet evolution with several IoT services[4].

This paper discusses the perspectives, challenges and opportunities behind a future Internet that fully supports the “things”, as well as how the things can help in the design of a more synergistic future Internet. It addresses the existing development trends, the generic architecture of IoT, IoT distinguishing features and possible future

applications. The IoT is a hot research topic that is getting increasing popularity for academia, industry as well as government.

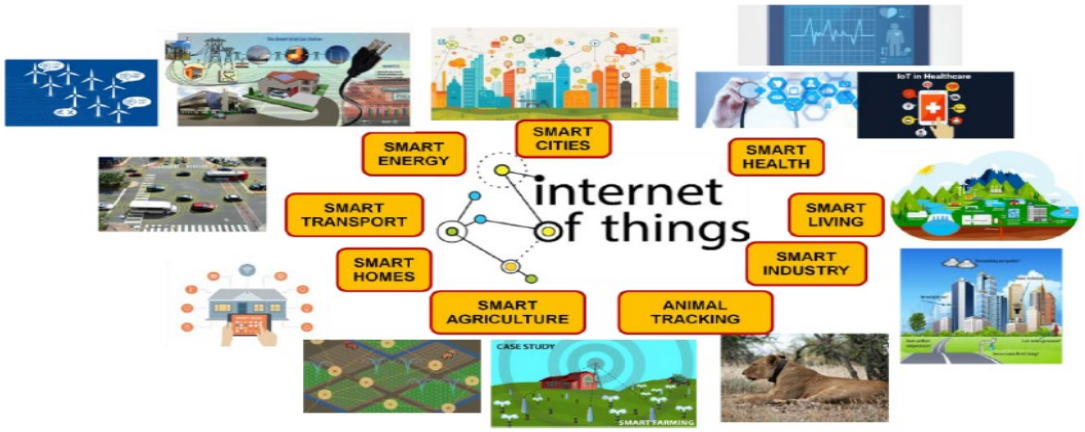


Figure.1: The IOT generic scenarios

The rest of the paper is organized as follows. Section.2 describes the future global market of IOT. Section.3 presents the generic architecture of IoT. Section.4 provides some of possible applications of IoT. Section.5 describes key challenges in the design and implementation of IoT. Finally, section.6 concludes the paper.

## 2. Market

A number of companies and research organizations have offered a wide range of projections about the potential impact of IoT on the Internet and the economy during the next few years. Cisco, for example, projects more than 24 billion Internet–connected objects by 2019 [5]; Morgan Stanley, however, projects 75 billion networked devices by 2020[6]. Looking out further and raising the stakes higher, Huawei forecasts 100 billion IoT connections by 2025[7]. McKinsey Global Institute suggests that the financial impact of IoT on the global economy may be as much as $11.1 trillion by 2025. Customers will capture most of the benefits, it estimates that the users of IoT (businesses, other organizations, and consumers) could capture 90% of the value that IoT applications generate. For example, the value of improved health of chronic disease patients through remote monitoring could be as much as $1.1 trillion per year in 2025[8].

By 2020, the 5G network is expected to support 50 billion connected devices and 212 billion connected sensors as well as enable access to 44 zettabytes of data. This will range from smartphones and tablets to smartwatches, cars, machinery, appliances, and remote monitoring devices. All of these will generate a massive amount of “useful data” that can be analyzed. Indeed, researchers estimate that this connected ecosystem will make it possible to utilize a much larger percent of digital data (35%) than before (5%) [1]. As the number of Internet-connected devices grows, the amount of traffic they generate is expected to rise significantly. For example, Cisco estimates that Internet traffic generated by non-PC devices will rise from 40% in 2014 to just under 70% in 2019[9]. Cisco also forecasts that the number of “M2M” connections (including in industrial, home, healthcare, automotive, and other IoT) will rise from 24% of all connected devices in 2014 to 43% in 2019. One implication of these trends is that over the next ten years we could see a shift in the popular notion of what it means to be “on the Internet’’.

The global GNSS market is witnessing steady growth, the global installed base is forecasted to increase from 5.8 bln GNSS devices in use in 2017 to almost 8 bln in 2020. Underpinned by an expanding mobile economy and growing purchasing power, the global installed base of GNSS devices continues to be greatly dominated by smartphones, followed a distant second by Road, with 5.4 bln and 380 mln devices respectively in use in 2017[10].

Although the number of GNSS devices in use for professional applications is far lower than their mass-market counterparts, the professional market is growing, with millions of people globally benefitting from them on a day-to-day basis - whether by enjoying the produce of sustainable and cost-effective agriculture, by using efficiently coordinated transport networks, or by leveraging on GNSS-synchronized telecommunications networks. These downstream markets are in turn enabling added-value services, they comprise all services that create an added value to users by leveraging on GNSS technology, including fleet management applications for transport and many smartphone apps.

In turn, the advent of 5G, Automated Driving, Smart Cities and the IoT is set to spawn a further proliferation and diversification of GNSS-enabled added-value services and their annual revenues will hit € 195 bln in 2025, more than 2.5 times higher than the expected GNSS device and service revenues[10]. Emerging technology paradigms such as the IoT or Smart Cities create linkages between established GNSS market segments, creating a window of opportunity for hybrid and cross-cutting applications and generating new user needs and requirements.

## 3. Generic Architecture

Today's Internet is using TCP/IP protocol stack for communication between network hosts which was proposed long time ago. However, the IoT connects billions of objects which will create much larger traffic and much more data storage is needed. Thus, IoT development depends on the technology progress and design of various new applications. Generally, the structure of IoT is divided into four layers as shown in Figure. 2. These layers are briefly described below[11]:

**1)** ***Perception Layer****:* The Perception layer is also known as 'Device Layer'. It consists of the physical objects and sensor devices. The sensors can be RFID, 2D-barcode, or Infrared sensor depending upon objects identification method. This layer basically deals with the identification and collection of objects specific information by the sensor devices. Depending on the type of sensors, the information can be about location, temperature, orientation, motion, vibration, acceleration, humidity, chemical changes in the air etc. The collected information is then passed to Network layer for its secure transmission to the information processing system.

**2)** ***Network Layer****:* The Network layer can also be called 'Transmission Layer'. This layer securely transfers the information from sensor devices to the information processing system. The transmission medium can be wired or wireless and technology can be 3G, UMTS, LTE, 4G, Wi-Fi, Bluetooth, infrared, ZigBee depending upon the sensor devices. Thus, the Network layer transfers the information from Perception layer to Middleware layer.

**3)** ***Middleware Layer****:* Middleware layer abstracts between application and network layers. This layer provides services to customers along with storing lower layer information in database. As IoT generates huge volumes of data and concentrates providing information to user data storage and analytics, visualization techniques gained importance. It performs information processing and ubiquitous computation and takes automatic decision based on the results.

**4)** ***Application Layer****:* The topmost layer which is application layer in the IoT architecture includes application management which is based on the information processed and gained from middleware layer. The applications implemented by IoT can be E-health, smart home, smart city, intelligent transportation, Retail, Agriculture, Supply chain and logistics, security and emergency, Factory, Culture and tourism, Environment and Energy, etc.

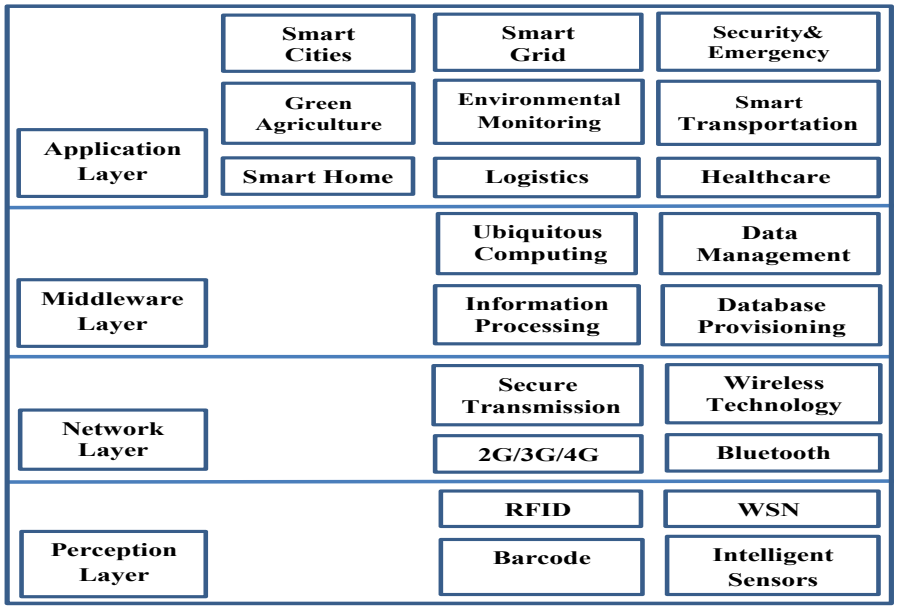


Figure.2: Basic IoT layers.

## 4. IOT Applications

The IoT is a very fragmented application scenario, and encompasses a wide range of applications, some of which are summarized in the following.

### 4.1. Smart Cities

Smart Cities through the IOT can manage resources more efficiently, be made much more resilient to temporary malfunctions and disasters, and encourage efficient behavior. Smart and weather-adapting lighting, water/gas leakage monitoring, smart parking with dynamic pricing and automated parking advice are just a few examples of how to use the IoT to solve today's urban challenges. Ubiquitous vision can enable an unprecedented level of safety and security, detecting potential danger and provide crucial information on crowd behavior and citizens' needs. Other than enabling ubiquitous and augmented surveillance, vision in IoT offers physical augmentation to social media and human activity monitoring to achieve better match between demand and supply of services dynamically. Similarly, it can be used to build real-time noise urban maps to mitigate noise pollution at critical times, and localize noise events for safety assurance [3]. Smart irrigation of green spaces and parks is another sub-area where the IoT has potential to make an impact. Smart infrastructures will also benefit from the IoT in terms of safety (e.g., structural monitoring of bridges) and security (e.g., automated identification of unattended bags and suspicious behavior). In the areas of Smart metering and monitoring, the IoT design for smart metering and monitoring will help to get accurate automated meter reading and issuance of invoice of electricity, gas and water to the customers.

Street light which can be equipped with sensors for detecting cars or human movement and which can then dynamically be turned on when there is some activity

in the zone and turned off otherwise. It can help to save energy (and money) for the city, whilst ensuring security by avoiding to create dark zones around people [12].
Smart tourism promises to give tourists the ability to have an immediate understanding of the city, such as availability, crowdedness or quietness of different places to receive dynamic recommendations on tours that adapt to their disposition, other than already available factual information on places. Waste management can be made more efficient, while detecting potentially dangerous and inappropriate waste that would need to be disposed with different procedure.

**4.2. Healthcare**

IoT technologies can find a number of applications in the health-care sector. On the one hand, they can be used to enhance current assisted living solutions. Patients will carry medical sensors to continuously monitor parameters such as body temperature, blood pressure, heartbeat, blood glucose level, blood oxygen level [4]. Other sensors will be used to gather data used to monitor patient activities in their living environments. Information will be locally aggregated and transmitted to remote medical centers, which will be able to perform advanced remote monitoring and will be capable of rapid response actions when needed. The interconnection of such heterogeneous sensors could provide a comprehensive picture of health parameters, thereby triggering an intervention by the medical staff upon detection of conditions that may lead to health deterioration, thus realizing preventive care.
In addition, the availability of big data from a large number of patients offers an unprecedented opportunity to explore correlations, build models and tools for predictive diagnosis, early treatment and make drug discovery more efficient and effective. Similar considerations hold for the elderly and the disabled, as constant non-obtrusive monitoring allows for better and highly responsive/predictive care, while preserving individual's independency and offloading hospitals. Remote supervision also enhances the ability to share professionals across a larger number of individuals and patients, thus driving the care cost down [3].

**4.3. Transportation system:** The Intelligent transportation system will provide efficient transportation control and management using advanced technology of sensors, information and network. The intelligent transportation can have many interesting features such as non-stop electronic highway toll, mobile emergency command and scheduling, transportation law enforcement, vehicle rules violation monitoring, reducing environmental pollution, anti-theft system, avoiding traffic jams, reporting traffic incidents, smart beaconing, minimizing arrival delays etc.
All types of vehicles in a city (cars, trains, buses, and bicycles) are becoming more equipped with sensors and/or actuators, resulting in a network composed of a set of mobile sensors. Both roads and rails, as well as transported goods, are also equipped with tags and sensors that send important information to traffic control sites. This not only allows monitoring of the status of the transported goods, but also allows the creation of innovative solutions, allowing transportation vehicles to better route the traffic or providing the tourist with appropriate transportation information.
Moreover, Cars can be further equipped with external sensing devices to monitor specific physical parameters, such as pollution, humidity, and temperature. Thus, the concept of "smart vehicles" emerges, if properly collected and delivered, such data can contribute to make the road transport greener, smarter, and safer [3]. For example, driving recommendations that aim at eco-efficiency for public transportation and reducing fuel consumption and emission can be provided. Mobile applications, such as Google Traffic, rely on user-contributed data to monitor traffic conditions. Smart traffic light infrastructures can be used to improve the life of drivers or make

cycling or driving in cities safer and smoother. For example, combining data from smartphones carried by cyclists and traffic data gathered from different kinds of sensors deployed in the traffic light infrastructure of a city may allow for an intelligent traffic light orchestration.

### 4.4. Retail and Logistics

Implementing the IoT in Retail/Supply Chain Management has many advantages which include monitoring of storage conditions along the supply chain and product tracking for traceability purposes and payment processing based on location or activity duration for public transport, theme park, etc. In the shop itself, IoT offers many applications like guidance in the shop according to a preselected shopping list, fast payment solutions like automatically check-out using biometrics, detection of potential allergen in a given product and control of rotation of products in shelves and warehouses to automate restocking processes. The IoT in logistics includes monitoring the whole process of the physical movement of goods from suppliers to demanders, in order to ensure their quality of shipment conditions, item location, fleet tracking, container openings for insurance purposes, search of individual items in big surfaces like warehouse and warning emission on containers storing inflammable goods closed to others containing explosive material [3].

### 4.5. Smart Energy

The smart grid is a recent kind of intelligent power system that can improve energy efficiency, reduce environmental impact, improve the safety and reliability of the electricity supply, and reduce the electricity transmission of the grid. The integration of IoT technology in smart grids can help to implement fault detection and monitoring, as well as consumption monitoring, through the installation of energy sensors [13]. Other groups of related solutions envision the heat and energy management in homes and buildings to accomplish an energy savings purpose. Using IoT technology to collect data on energy consumption can also help to improve the energy efficiency and competitiveness of manufacturing companies at the energy production level.

**Facilities Energy Management**: This application is combination of Information systems, operational technology and advanced metering, that is capable of tracking, reporting and alerting operational staff in real time. These management systems are highly capable of allowing dynamic visibility over buildings and other facility performance. They can also provide dashboard view for energy consumption levels, varying degrees of granulation and allows data feeds from a wide range of building equipment and other subsystems.

**Home Energy Management(HEM):** Energy management to set the temperature and light in a room as a function of the number of people in the room, the time of day, the external conditions, the cost of the utility.

It optimizes production and consumption of residential energy. The HEM system includes applications that analyze energy usage levels, and energy management sensors that are connected to home area network that responds to the variable power supply when optimizing energy. A combination of these solutions can contributes towards reducing overall energy consumption and carbon emissions from homes. The IoT can also be used to control the appliances in home remotely and useful in detecting and avoiding thefts [3].

### 4.6. Smart Agriculture

A network of different sensors can sense data, perform data processing and inform the farmer through communication infrastructure e.g., mobile phone text message about the portion of land that need particular attention.

This may include smart packaging of seeds, fertilizer and pest control mechanisms that respond to specific local conditions and indicate actions. Intelligent farming system will help agronomists to have better understanding of the plant growth models and to have efficient farming practices by having the knowledge of land conditions and climate variability. This will significantly increase the agricultural productivity by avoiding the inappropriate farming conditions.

The role of IoT in water management includes study of water suitability in rivers and the sea for agriculture and drinkable use, detection of liquid presence outside tanks and pressure variations along pipes and monitoring of water level variations in rivers, dams and reservoirs.

**4.7. Environmental Monitoring**

Using of wireless identifiable devices and IoT technologies in environmental conservation and other green applications are one of the top most promising market segments in the future. There will be an increased usage of these devices in environmental friendly programs in worldwide, like bio-monitoring, remote sensing, soil monitoring, water monitoring and air quality monitoring. IoT can be used to advance environmental programs, including the collection of recyclable materials for the reuse, the disposal of electronic waste (RFID used to identify electronic subcomponents of personal computers, mobile devices and other consumer electronics products to increase the re usage of these sub parts and to reduce e-waste). A very important IoT application is monitoring Air Pollution: Control of CO2 emissions of factories, pollution emitted by cars and toxic gases generated in farms, Forest Fire Detection: Monitoring of combustion gases and preemptive fire conditions to define alert zones, Weather monitoring: weather conditions monitoring such as humidity, temperature, pressure, wind speed and rain, Earthquake Early Detection, Water Quality: track the release of waste and harmful chemicals into the rivers and sea for reducing water pollution, can also maintain the quality of water being supplied for drinking, River Floods: Monitoring of water level variations in rivers, dams and reservoirs during rainy days, Protecting wildlife: Tracking collars utilizing GPS/GSM modules to locate and track wild animals and communicate their coordinates via SMS[3].

**4.8. Security & Emergencies**

The IoT technologies in the field of security and emergencies are tremendously increased in which few are listed; perimeter access control, liquid presence, radiation levels and explosive and hazardous gases, etc. The perimeter access control is used to detect and control the unauthorized people entry to restricted areas, surveillance of spaces, tracking of people and assets, infrastructure and equipment maintenance, alarming etc. The liquid presence is used for liquid detection in data centers, warehouses and sensitive building grounds to prevent break downs and corrosion. The radiation levels application used to measure the radiation levels in nuclear power stations surroundings to generate leakage alerts and the final IoT application is used to detect the gas levels and leakages in industrial environments, surroundings of chemical factories and inside mines. The combination of sensors and their autonomous coordination and simulation will help to predict the occurrence of earthquakes and tsunamis by detecting vibrations or other natural disasters and to take appropriate actions in advance [3].

**Practical System in IoT**

A real IoT application called Tsunami Detection System is discussed [3]. This system is used to facilitate early detection of the tsunami using real-time observation of the sea level in Japan. Large number of buoys equipped with sensors and small earth

stations are planned to be deployed around Japan in this system. The sensors are used to measure the fluctuation of the wave height while the small earth stations send the data gathered from the sensors to the satellite. To cover whole Japan to detect a tsunami as early as possible, it is necessary to deploy numerous sensor terminals. In the case where the sensor terminals are deployed in a large scale, it is difficult to send the data gathered from the sensors directly to the base station on the ground by ground-based wireless networks due to the remotely located base station.

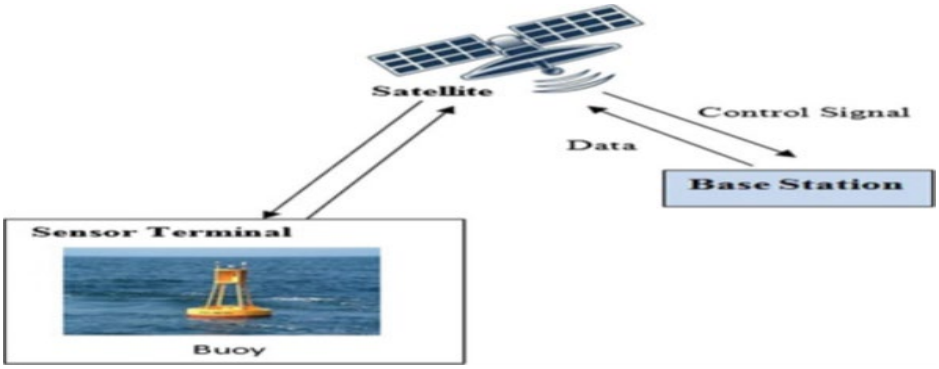


Figure. 3: Tsunami detection system

Therefore, in this system, the data is sent from the sensor terminals to the base station via a satellite. Since the satellite has a large coverage, it is possible to collect data from sensor terminals deployed throughout Japan. The construction of Tsunami detection system is shown in Figure.3. In this system; the sensors are used to measure the change of the Z-axis position by using the GPS. The change of the Z-axis position implies the change of the sea level. The collected data is sent to the base station via a satellite and then the data are analyzed to distinguish the tsunami from normal waves. Thus, the occurrence of a tsunami can be detected at the base station. This system will help early to detect of tsunami before it occurs for protect people life.

## 5. Challenges and Opportunities

We believe that the Internet should be a source of empowerment globally, regardless of a user's location, region, or state of economic development, and that the full range of abilities and principles that drive our life and the success of the Internet apply globally. It is reasonable to expect the same to be true for the potential benefits and challenges associated with the IoT. The IoT raises many new legal and regulatory questions and may raise existing challenges associated with the Internet. Promoting users' ability to connect, speak, innovate, share, chose and trust are core considerations for evolving laws and regulations. In this section however, we provide an overview of some topics frequently discussed in relation to IoT: Security, Privacy, Interoperability and Standards, Legal, Regulation and Rights.

We begin to examine these issues and present important aspects of each issue and propose several questions for discussion.

### 5.1. The IoT Security Challenge

Security represents a critical component for enabling the widespread adoption of IoT technologies and applications. Without guarantees in terms of system-level confidentiality, authenticity and privacy the relevant stakeholders are unlikely to adopt IoT solutions on a large scale[13]. If people don't believe their connected devices and their information are reasonably secure from misuse or harm, the

resulting erosion of trust causes a reluctance to use the Internet. Indeed, ensuring security in IoT products and services should be considered a top priority for the sector. As we increasingly connect devices to the Internet, new opportunities to exploit potential security vulnerabilities grow. Poorly secured IoT devices could serve as entry points for cyberattack by allowing malicious individuals to re-program a device or cause it to malfunction.

Poorly designed devices can expose user data to theft by leaving data streams inadequately protected. Failing or malfunctioning devices also can create security vulnerabilities. These problems are just as large or larger for the small, cheap, and ubiquitous smart devices in the IoT as they are for the computers that have traditionally been the endpoints of Internet connectivity. Competitive cost and technical constraints on IoT devices challenge manufacturers to adequately design security features into these devices, potentially creating security and long-term maintainability vulnerabilities greater than their traditional computer counterparts.

Along with potential security design deficiencies, the heavy increase in the number and nature of IoT devices could increase the opportunities of attack. When coupled with the highly interconnected nature of IoT devices, every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally, not just locally.

We become more connected and dependent on IoT devices for essential services, and we need the devices to be secure, while recognizing that no device can be absolutely secure. Some IoT devices are likely to be deployed in places where physical security is difficult or impossible to achieve. Attackers may have direct physical access to IoT devices. The overall security and resilience of the IoT is a function of how security risks are assessed and managed. Security of a device is a function of the risk that a device will be compromised. Several factors influence this risk assessment and mitigation calculation, factors include having a clear understanding of the present security risks and the potential future risks; the estimated economic and other costs of harm if the risks are realized; and the estimated cost to mitigate the risks.

There is a few **internet of security solutions** that experts suggest. Foremost the IoT devices that need direct access to the internet should be segmented into their own networks that have restricted access. It will then become easier to monitor a device's network segment for any anomalous traffic. Companies need to improve their data security and privacy policies. Investment should be made in provide security structure at business level. Providing training and guidance to common people and business staff on securing their IoT device will substantially decrease the security risk.

### 5.2. IoT Privacy

Privacy defines the rules under which data referring to individual users may be accessed. The main reasons that makes privacy a fundamental IoT requirement lies in the envisioned IoT application domains and in the technologies used. Health-care applications represent the most outstanding application field, whereby the lack of appropriate mechanisms for ensuring privacy of personal and/or sensitive information has harnessed the adoption of IoT technologies.

In addition, in the IoT vision, a prominent role will be played by wireless communication technologies. The ubiquitous adoption of the wireless medium for exchanging data may pose new issue in term of privacy violation. In fact, wireless channel increases the risk of violation due to the remote access capabilities, which potentially expose the system to eavesdropping and masking attacks[13]. Also, Characteristics of IoT devices and the ways they are used redefine the debate about

privacy issues, because they dramatically change how personal data is collected, analyzed, used, and protected[14].

IoT data collection and use becomes a privacy consideration when the individuals who are observed by IoT devices have different privacy expectations regarding the scope and use of that data than those of the data collector. The user might not be aware that an IoT device is collecting data about the individual and potentially sharing it with third parties. This type of data collection is becoming more prevalent in consumer devices like smart televisions and video game devices.

These kinds of products have voice recognition or vision features that continuously listen to conversations or watch for activity in a room and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. A person might be in the presence of these kinds of devices without knowing their conversation or activities are being monitored and their data captured. These kinds of features may provide a benefit to an informed user, but can pose a privacy problem for those who are unaware of the presence of the devices and have no meaningful influence over how that collected information is used.

Independent of whether the user is aware of and accepts to having their IoT data collected and analyzed, these situations highlight the value of these personalized data streams to companies and organizations seeking to collect and capitalize on IoT information. The demand for this information exposes the legal and regulatory challenges facing data protection and privacy laws.

From a broad perspective, people recognize their privacy is essentially valuable, and they have expectations of what data can be collected about them and how other parties can use that data. This general notion about privacy holds true for data collected by IoT devices, but those devices can erode the user's ability to express and enforce privacy preferences. Hence privacy represents a real open issue that may limit the development of the IoT.

### 5.3. IoT Interoperability/ Standards

Device interoperability can encourage innovation and provide efficiencies for IoT devices manufacturers, increasing the overall economic value of the market. Interoperability is the most basic core value of the internet; the first requirement of Internet connectivity is that "connected" systems be able to "talk the same language" of protocols and encodings. Barriers deliberately erected to obstruct the exchange of information can deny Internet users the ability to connect, speak, share, and innovate, which are fundamental principles of interoperability.

In a fully interoperable environment, any IoT device would be able to connect to any other device or system and exchange information as desired. Interoperability among IoT devices and systems happens in varying degrees at different layers within the communications protocol stack between the devices. The standardization and adoption of protocols that specify these communication details, including where it is optimal to have standards, are at the heart of the interoperability discussion for IoT.

Lack of standards and documented best practices have a greater impact than just limiting the potential of IoT devices. In a passive way, absence of these standards can enable bad behavior by IoT devices. If these devices are poorly designed and configured, they may have negative consequences for the networking resources they connect to and the broader Internet[14].

Beyond the technical aspects, interoperability has significant influence on the potential economic impact of IoT. Well-functioning and well-defined device interoperability can encourage innovation and provide efficiencies for IoT device manufacturers, increasing the overall economic value of the market. Furthermore, the

implementation of existing standards and development of new open standards where necessary help lower barriers to entry, facilitate new business models, and build economies of scale.

**5.4. Technical and cost constraints**

Manufacturing advances allow cutting-edge computing and communications technology to be incorporated into very small objects. Coupled with greater computing economics, this has boosted the advancement of small and inexpensive sensor devices, which drive many IoT applications.

Due to the increased usage of IoT devices, the traffic generated by these devices is also increasing. Hence there is a need to increase network capacity, therefore, it is also a challenge to store the huge amount of data for analysis and further final storage.

New algorithms and rapid increases in computing power, data storage, and cloud services enable the aggregation, correlation, and analysis of vast quantities of data; these large and dynamic datasets provide new opportunities for extracting information and knowledge.

As manufacturers develop IoT devices, there are inherent technical, time to market, and cost constraints that factor into device design. Some devices are constrained by technical factors like limited internal processing resources, memory, or power consumption demands. Similarly, manufacturers are under pressure to reduce the unit cost of the device by minimizing part and product design costs. Manufacturers make cost-benefit analyses to decide whether the additional costs and potentially reduced product performance is worth the extra benefits of implementing standards. In the short-term, it can be more expensive to design interoperability features into a product and test for compliance with a standards specification. In some contexts, the cheapest path to market may be to use proprietary protocols and systems. This needs to be compared, however, against the long-term product lifecycle gains afforded by interoperability.

Billions of batteries are required to operate the IoT, posing a significant environmental risk as many devices will not be correctly disposed of after use. Alternatively, energy harvesting which converts ambient energy sources (e.g. vibration, light and temperature) into electrical energy, can become the standard for new energy efficient devices. In recent years, such devices have been shown to operate just as well as their battery powered counterparts, and could be viable long-term alternatives.

**5.5. Regulation and Policy Issues**

The application of IoT devices poses a wide range of challenges and questions from a regulatory and legal perspective, which need more thoughtful consideration. Further, technology is advancing more rapidly than the associated regulatory and policy environments. The range of legal, regulatory and rights issues associated with the IoT is broad. IoT devices create new legal and policy challenges that didn't previously exist, and they glorify many challenges that already exist. For example, accessibility requirements for IoT devices for those with disabilities offer new challenges arising from the introduction of new kinds of IoT devices, while remaining compatible with existing accessibility standards and guidelines. On the other hand, the massive scale of wireless IoT devices and the radio frequency noise and interference they produce is an example of the way IoT devices raise the existing difficulty of regulating the use of the RF spectrum. Legal and regulatory concerns of intellectual property issues, environmental issues (e.g. disposal of devices), and legal ownership of devices are emerging challenges as well for IoT devices.

Along with the complexities of deciding the appropriate regulatory or policy strategies for IoT problems, there is the added complexity of deciding where in an IoT system architecture is the best place to achieve the desired outcomes. Should the regulatory controls be placed on the device, on the flow of the data, on the gateway, on the user, or in the cloud where data is stored?

Regulatory analysis of IoT devices is increasingly viewed from a general, technology neutral perspective legal lens, such as consumer protection laws and regulations. Assessing legal implications of IoT devices from the perspective of preventing unfair or misleading practices against consumers can help inform decisions of privacy and security among others. In some cases, IoT devices create new legal and regulatory situations and concerns over civil rights that didn't exist prior to these devices[15].

**IOT Data Protection**

Data collected by IoT devices may not be constrained from being sent across territory boundaries. These devices use the Internet to communicate, and the Internet spans territory boundaries at all levels. IoT devices can collect data about people in one territory and transmit that data to another territory for data storage or processing, often with few or no technical barriers. This can quickly become a legal problem, for example, if the data collected is deemed to be personal or sensitive data and subject to data protection laws in multiple territories. These situations are described as cross border data flows, and they raise questions about the legal scope of regulations that might be applicable. In other words, which legal regime governs the device collecting the data, and which governs the storage and use of the collected data? This scenario also raises some questions. Can these laws be modified to reduce the degree of Internet fragmentation they cause while still protecting the rights of users? Should a territory with more-restrictive data protection laws for handling and transmission of certain IoT- enabled data be able to project those legal requirements onto other territories?

Progressively, these devices will be able to automatically connect to other devices and systems and transmit information across borders without the knowledge of the user. This could create situations where a user becomes liable for cross border data flow requirements, and he is unaware that the activity is happening. These are complex issues, and only growing more so, as technology continues to outpace policy[15].

**IoT Device Liability**

IoT devices operate in a more complex way than a simple stand-alone product, which suggest more complex liability scenarios need to be considered. For example: IoT devices are likely to be used in ways never predicted by the manufacturer. An IoT device manufacturer cannot reasonably perform product assurance testing on all possible use cases of IoT devices. There is the potential for IoT devices to connect and interact with other IoT devices in untested and unforeseen ways. As interoperability of these devices increases, they may be able to form ad hoc network connections among themselves. Therefore, it is difficult for a manufacturer or user to account for all potentially harmful scenarios in advance of deploying these devices.

IoT devices will be integrated into autonomous systems like driverless cars, which incorporate adaptive machine-learning algorithms to control their behavior based on sensor inputs from IoT devices. The actions of these systems cannot be fully known and tested in advance[15].

These scenarios and others raise questions. If harm results from one of these scenarios, do existing liability laws adequately address legal responsibility and clarify the liability exposure of parties involved? Do liability laws need reconsideration for intelligent IoT devices that learn from their environment and modify themselves over

time? If autonomous systems are instructed by the end user rather than by their internal algorithms, what happens in cases of user error? Should IoT devices be smart enough to have a “do what I meant” instruction? To what extent will current liability laws for conventional products extend to products that become Internet-enabled? What can we as a community do to better inform legislators and policy makers, so that they are not as susceptible to the vast amounts of misinformation and biased advice they are receiving?

## 6. Conclusion

The IoT describes the billions of connected devices that exist in an increasingly networked society, pervading smart homes, workplaces, healthcare, logistics and retails, Transportation, industries and smart cities. The opportunities afforded by this technology are huge, connecting machine to machine, humans to their environments and allowing analysis of the world at new levels of detail. Whilst these opportunities are significant, they are accompanied by risks to society and its infrastructure. This paper covered several key points related to IOT including technology, security, privacy, interoperability and standardizations, regulations and legal policy, and global issues. Cyber-attacks on IoT devices are inevitable and the resilience of devices and networks must be carefully considered. Separation of valuable network assets may be the best way to protect them from attacks.

In a constantly developing world of apparent ubiquity and a pervasive network of interconnected things, the development of new techniques and enablers in the area of communication/middleware systems, high-performance embedded and computing technologies and WSNs amongst others will be necessary. The standardization of the IoT communication protocols and technology enablers cannot be exaggerate.

More importantly, the issues of security, privacy, vulnerability management and interoperability should be prioritized in any IoT design, build and implementation as this is, without any doubt, the biggest concern with the proliferation of the IoT in the modern era.

The legacy of devices is important when they are placed into environments for long periods. They must be resilient in terms of security, power supplies, software and hardware, but also remain interoperable with IoT devices of the future. Devices should be ‘secure by default’. Owners of IoT devices, the networks they are hosted on and the data they generate need to be accountable when problems occur, especially as artificial intelligence and machine learning becomes more commonplace. Device users should understand the choice they make when they agree to providing their data to service providers.

Society needs to reconsider legislation and regulation in a networked society to take account of the data generated by IoT devices and the power it gives to those that possess it. More transparency of who collects data and what it is used for should be provided to device users. Industry is likely to drive for standards in the IoT faster than government can legislate. The public sector may drive the creation and adoption of standards through procurement policies. The dynamic nature of IoT has challenges and concerns to be addressed. We also get an indication of the important aspects that need to be further studied and developed for making large-scale deployment of IoT a reality.

## References

[1] Darrell M. West, “How 5G technology enables the health internet of things”, Center for technology innovations at Brookings, July 2016.

[2] D. Warren, C. Dewar, , "Understanding 5G: Perspectives on future technological advancements in mobile", GSMA Technology GSMA Intelligence Dec.2014.
[3] D.P. Acharjya, M. K. Geetha, “Internet of Things: Novel Advances and Envisioned Applications”, Springer International Publishing AG 2017.
[4] Keyur K Patel, Sunil M Patel, “ IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges”, International Journal of Engineering Science and Computing, Volume 6 Issue No. 5, May 2016 .
[5] “Cloud and Mobile Network Traffic Forecast- Visual Networking Index” *Cisco, 2015*.http://cisco.com/c/en/us/solutions/service-provider/visual-networking-indexvni/index.html
[6] T. Danova, “Morgan Stanley: 75 Billion Devices Will Be Connected to The Internet of Things by 2020.”, *Business Insider*, October 2013.
[7] “Global Connectivity Index.” Huawei Technologies Co., Ltd., 2015. Web. 6 Sept.2015. http://www.huawei.com/minisite/gci/en/index.html
[8] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin and D. Aharon, “The IoT: Mapping the Value Beyond the Hype” McKinsey Global Institute, June2015
[9] “Cisco Visual Networking Index: Forecast and Methodology, 2014-2019.” Cisco, May 27, 2015. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white-paper-c11-481360.pdf
[10] GSA, “GNSS Market Report Issue 5,” European GNSS Agency Publications, 2017.
[11] T. S. Sri, J. R. Prasad, Y. Vijayalakshmi, “A review on the state of art of Internet of Things”, International Journal of Advanced Research in Computer and Communication Engineering(IJARCCE), Vol. 5, Issue 7, July 2016.
[12] C. X. Mavromoustakis, G. Mastorakis, J. M. Batalla , “Internet of Things (IoT) in 5G Mobile Technologies”, Springer International Publishing Switzerland 2016.
[13] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, “Internet of things: Vision, applications and research challenges”, Ad Hoc Networks Volume 10, Issue 7, September 2012, Pages 1497-1516.
[14] D. Bandyopadhyay, J. Sen, “ Internet of Things: Applications and Challenges in Technology and Standardization”, Wireless Pers Commun (2011) 58:49–69, DOI 10.1007/s11277-011-0288-5.
[15] K. Rose, S. Eldridge, L. Chapin, “The Internet of things: An Overview understanding the Issues and challenges of a more connected world”, Internet Society(ISOC), Oct.2015.