IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Design Paradigms, Applications and Security Issues in Internet of Things (IoT)

Name of Author – Jay Prakash Soja

Designation – Assistant Professor

Name of Department – Department of Computer Engineering/Applications
Name of organization – Ambedkar Institute of Technology, Shakarpur, Delhi (India)

Abstract: The purpose of this study is to understand the perspectives of Internet of Things (IoT) which is being widely accepted and implemented by the large numbers of domestic and commercial users for various day-to-day applications to facilitate the optimum use of devices/objects (things) over the internet. IoT fulfills the requirements of almost all kind of users to use their domestic and commercial equipments/ devices by accessing them remotely over the internet. As the backbone of IoT is internet, so provision of security of data and information being exchanged is important for users and service providers. The fact that IoT is so expansive and affects practically all areas of our lives, makes it a significant research topic for studies in various related fields such as information technology and computer science. Thus, IoT is paving the way for new dimensions of research to be carried out**.** This paper will cover design paradigms, types and applications of IoT with security challenges in remotely accessing of heterogeneous networks and devices.

Keywords – IoT-Internet of Things, M2M-Machine to Machine, IoE-Internet of Everything, IIoT- Industrial Internet of Things, WoT-Web of Things, IoMT – Internet of Medical Things, SIoT-Social Internet of Things.

I. INTRODUCTION

The word Internet of Things (IoT) is made up of two main parts- Internet which is the backbone of connectivity and Things meaning objects or devices. IoT is a network in which all physical objects like mechanical and digital machines, interrelated computing devices, animals or people are connected to the internet through network devices or routers and exchange data. IoT allows objects to be controlled remotely across existing network infrastructure. IoT allows autonomous control of device. Thus Internet of Things (IoT) is described as "the network of physical devices/ objects ("things") that are embedded with sensors, software, and other technologies for the purpose of connecting, communicationg and exchange of data with other devices and systems over the internet. The rapid growth of internet technologies leads to access of various online applications for controlling the domestic and commercial electronic equipments/ devices for various types of applications for example - remote access of home CCTVs over the internet, switching on or setting the temperature of your AC from a remote location etc. Some of the applications of IoT are - Smart Homes, Smart City, Self-driven Cars, IoT Retail Shops, Farming, Wearables, Industrial Internet, Telehealth, Smart Supply-chain Management, Traffic management, Water and Waste management.

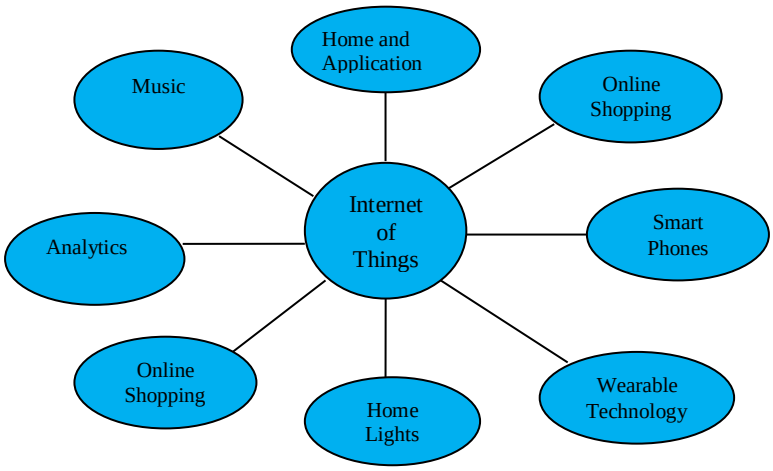


Fig (1) – Perspective view of IoT

(II) Design Architecture - Internet of Things, works accordingly as per it has been designed/developed. But it has not a standard defined architecture of working which is strictly followed universally. The architecture of IoT depends upon its functionality and implementation in different sectors. Still, there is a basic process flow based on which IoT is built.

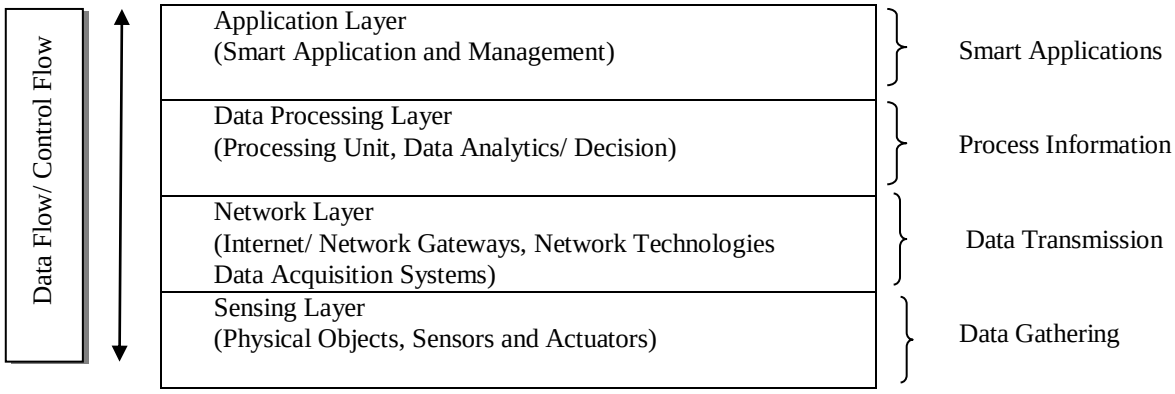


Fig (2) – 4 Layered IoT Architecture

1. **Sensing Layer -**Sensors, actuators, devices are present in this Sensing layer. These Sensors or Actuators accepts data (physical/environmental parameters), processes data and emits data over network.
2. **Network Layer -** Internet/Network gateways, Data Acquisition System (DAS) are present in this layer. DAS performs data aggregation and conversion function (Collecting data and aggregating data then converting analog data of sensors to digital data etc). Advanced gateways which mainly opens up connection between Sensor networks and Internet also performs many basic gateway functionalities like malware protection, and filtering also some times decision making based on inputted data and data management services, etc.
3. **Data processing Layer -**This is processing unit of IoT ecosystem. Here data is analyzed and pre-processed before sending it to data center from where data is accessed by software applications often termed as business applications where data is monitored and managed and further actions are also prepared. So here Edge IT or edge analytics comes into picture.
4. **Application Layer** - This is last layer of 4 stages of IoT architecture. Data centres or cloud is management stage of data where data is managed and is used by end-user applications like agriculture, health care, aerospace, farming, defence, etc.

(III) Characteristics of Internet of Things (IoT)

(i) **Connectivity -** Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connect, this should be guaranteed at all times. For example, connection between people through internet devices like mobile phones and other gadgets, also connection between Internet devices such as routers, gateways, sensors etc.

(ii) **Intelligence and Identity -** The extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tacking the equipment and at times for querying its status.

(iii) **Scalability -** The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous, and it should be handled appropriately.

(iv) **Dynamic and Self-Adapting (Complexity) -** IoT devices should dynamically adapt themselves to the changing contexts and scenarios. Assume a camera meant for the surveillance. It should be adaptable to work in different conditions and different light situations (morning, afternoon, night).

(v) **Architecture -** IoT architecture cannot be homogeneous in nature. It should be hybrid, supporting different manufacturer's products to function in the IoT network. IoT is not owned by anyone engineering branch. IoT is a reality when multiple domains come together.

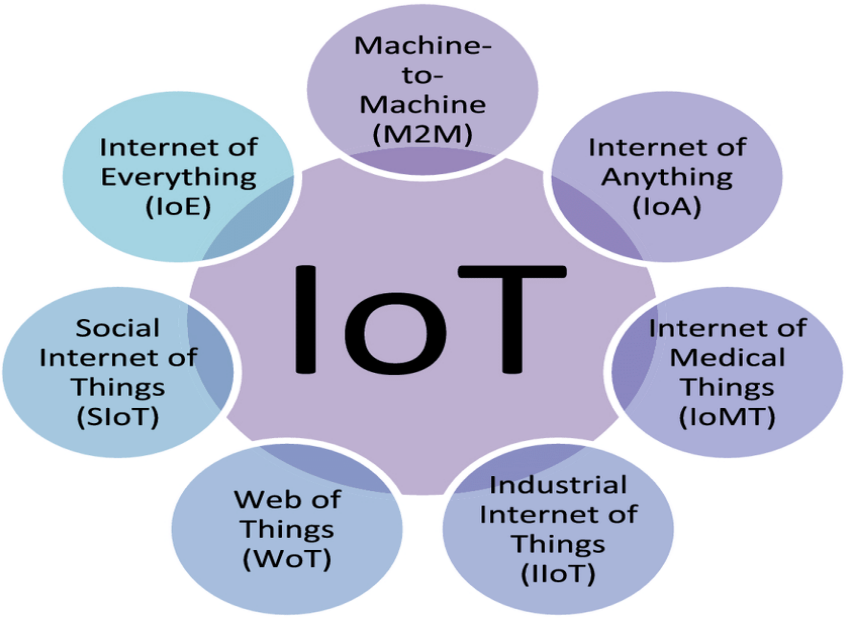
(vi) **Safety -** There is a danger of the sensitive personal details of the users getting compromised when all his/her devices are connected to the internet. This can cause a loss to the user. Hence, data security is the major challenge. Besides, the equipment involved is huge. IoT networks may also be at the risk. Therefore, equipment safety is also critical.

(vii) **Self Configuring -** IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation. Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.

(IV) Internet of Things (IoT) Technologies

There are several technologies and protocols that are used while designing the IoT based applications, Bluetooth, wifi, radio protocols, LTE-A etc are some major IoT technologies and protocols.

Machine-to-Machine (M2M) - This is commonly known as Machine to machine communication. It is a concept where two or more than two machines communicate with each other without human interaction using a wired or wireless mechanism. M2M is an technology that helps the devices to connect between devices without using internet. M2M communications offer several applications such as security, tracking and tracing, manufacturing and facility management.



Internet of Everything (IoE) -Internet of Everything (IoE) is defined as the networked connection of people, process, data, and things. The benefit of IoE is derived from the compound impact of connecting people, process, data, and things, and the value this increased connectedness creates as "everything" comes online. For example- the wearable fitness bands of various companies such as Nike, Fitbit, Samsung etc. along with smart sports apparel and gear, have chips that collect vital user data to track their key health parameters.

Internet of Medical Things (IoMT) - IoMT include remote patient monitoring of people with chronic or long-term conditions; tracking patient medication orders and the location of patients admitted to hospitals; and patients' wearable mHealth devices, which can send information to caregivers. The capabilities of IoMT are more accurate diagnoses, fewer mistakes and lower costs of care. Paired with smartphone applications, the technology allows patients to send their health information to doctors in order to better surveil diseases and track and prevent chronic illnesses.

Industrial Internet of Things (IIoT) - The industrial internet of things (IIoT) refers to interconnected sensors, instruments, and other devices networked together with computers' industrial applications, including manufacturing and energy management. With IIoT, industrial companies can digitize processes, transform business models, and improve performance and productivity, while decreasing waste. Using industrial IoT platforms, companies connect, monitor, analyse and act on industrial data in new ways to improve efficiency, maximize revenue growth, reduce costs and more.

Web of Things (WoT) - Web of Things (WoT) describes a set of standards by the World Wide Web Consortium (W3C) for the interoperability of different Internet of things (IoT) platforms and application domains. The WoT provides a set of standardized technology building blocks that help to simplify IoT application development by well-known and successful Web paradigm. This approach increases flexibility and interoperability, especially for cross-domain applications, as well as enabling reuse of established standards and tools. WoT unlocks commercial potential being held back by IoT fragmentation.

Social Internet of Things (SIoT) – SIoT is defined as an IoT where things are capable of establishing social relationships with other objects, autonomously with respect to humans. SIoT provides a platform for worldwide interconnected objects to establish social relationships by trading-off their individuality for common interests and better services to users. This relationship among objects can be of co-location, co-work, parental, social or co-ownership. Due to the all-in-one nature of SIoTs, its architectural design, implementation, and operational manageability and maintenance are raising numerous prevalent concerns that are the challenges for researchers, academicians, engineers, standardization bodies and other market players.

(V) Some Applications of Internet of Things (IoT)

(i) Smart City
(ii) Smart Home
(iii) Smart Car Parking
(iv) Smart Farming
(v) Smart Retail
(vi) Smart Supply Chain

(i) Smart City - Smart city is another powerful application of IoT generating curiosity among world's population. Smart surveillance, smarter energy management systems, automated transportation, water distribution, urban security and environmental monitoring all are examples of internet of things applications for smart cities. IoT will solve major problems faced by the people living in cities like pollution, traffic congestion and shortage of energy supplies etc. Smart City are built by installing sensors and using web applications, citizens can find free available parking slots across the city. Also, the sensors can detect meter tampering issues, general malfunctions and any installation issues in the electricity system (Fig-3).

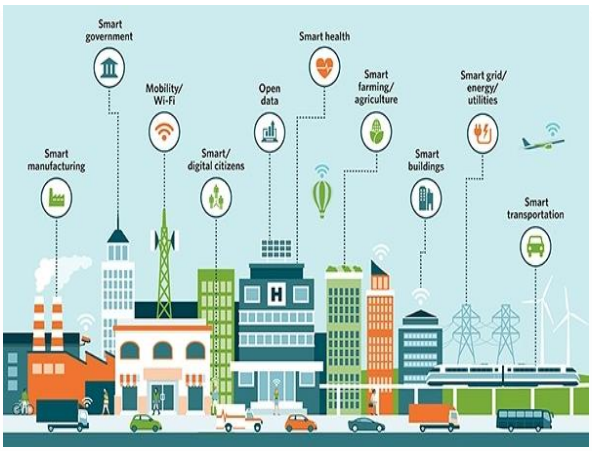


Fig-3 (IoT based Smart City)

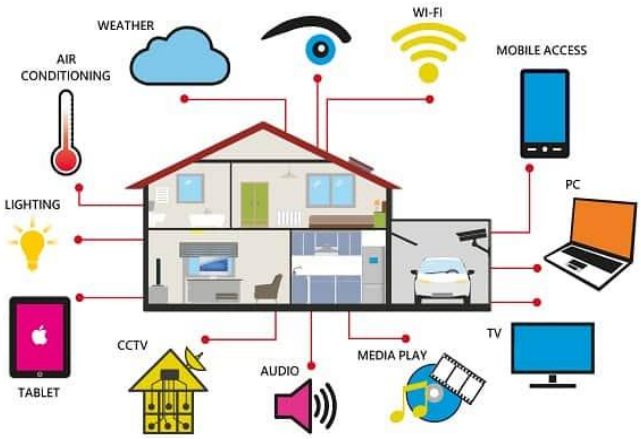


Fig-4 (IoT based Smart Home)

(ii) Smart Home - Smart Home Smart Home has become the revolutionary ladder of success in the residential spaces and it is predicted Smart homes will become as common as smartphones Whenever we think of IoT systems, the most important and efficient application that stands out every time is Smart Home ranking as highest IOT application on all channels. Smart Home products are promised to save time, energy and money.Wouldn't you love if you could switch on air conditioning before reaching home or switch off lights even after you have left home? Or unlock the doors to friends for temporary access even when you are not at home (Fig-4).

(iii) Smart Car Parking - IoT-based smart parking system transmits available and occupied parking spaces via a web/mobile application. Each parking space has an IoT gadget, which includes sensors and microcontrollers. The user gets real-time updates on the availability of all parking spaces and, therefore, an option to choose the best one. The smart vehicle presence sensor comprises a single-board computer, sensors, LED indicator, beeper, and battery pack. The vehicle presence sensors sense the parking lot occupancy. (Fig-5)

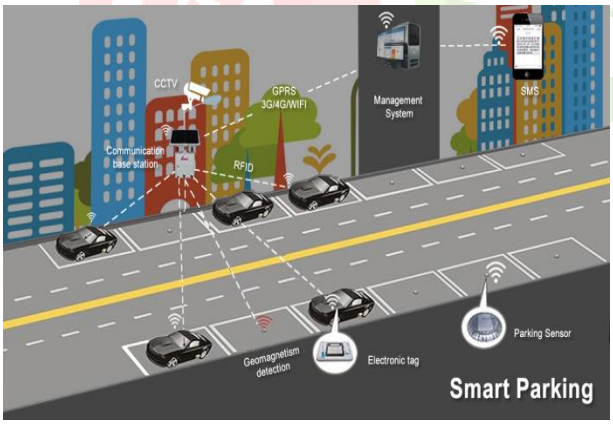


Fig-5 (IoT based Smart Car Parking)

Fig-6 (IoT based Smart Farming)

(iv) Smart Farming - IoT in agriculture uses robots, drones, remote sensors, and computer imaging combined with continuously progressing machine learning and analytical tools for monitoring crops, surveying, and mapping the fields, and providing data to farmers for rational farm management plans to save both time and money. Smart farming based on IoT technologies enables growers and farmers to reduce waste and enhance productivity ranging from the quantity of fertilizer utilized to the number of journeys the farm vehicles have made, and enabling efficient utilization of resources such as water, electricity etc. IoT smart farming solutions is a system that is built for monitoring the crop field with the help of sensors (light, humidity, temperature, soil moisture, crop health etc. and automating the irrigation system. The farmers can monitor the field conditions from anywhere.

(v) Smart Retail - Smart retail refers to the hybridization between traditional shopping methods and modern "smart" technologies. Through the Internet of Things, data is accumulated by way of communication between implanted devices and computers. As a result, consumers may enjoy a more personalized, faster, and smarter experience. Personalized retail marketing and content delivery. Smart retails based on IoT include - optimal staffing level indicators, cashierless payment, systems, movement tracking systems for optimal store setup, IoT-enabled warehouse robots, wireless shipment tracking devices, real-time condition monitoring of goods.

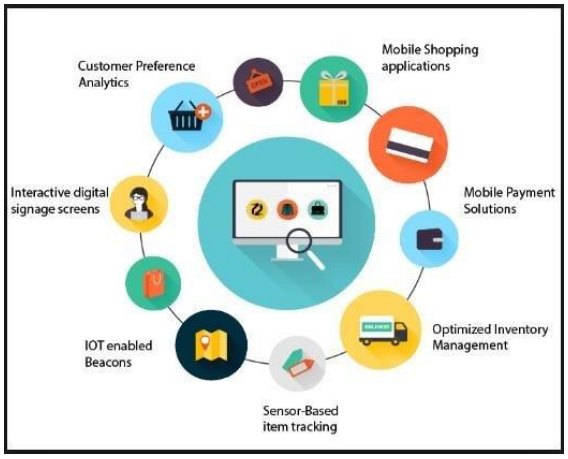


Fig-7 (IoT based Smart Retail)

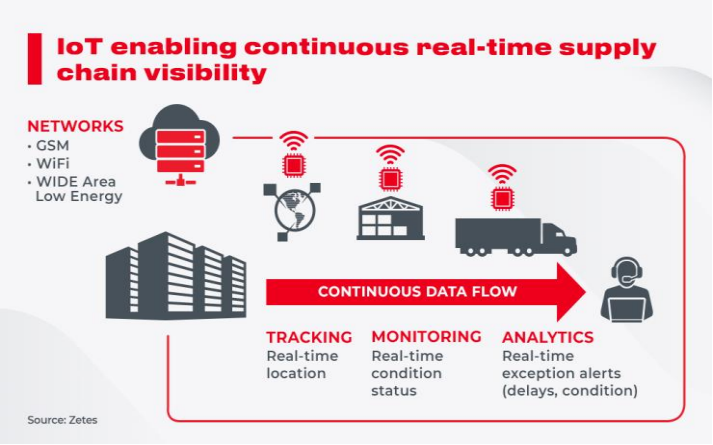


Fig-8 (IoT Based Smart Supply Chain)

(vi) Smart Supply Chain - IoT allows supply chain managers to connect vehicles, equipment and devices for real-time status updates on jobs. This can offer an end-to-end supply chain picture - from manufacturer to customer, via the warehouse. IoT devices are an effective way to track and authenticate products and shipments using GPS and other technologies. They can also monitor the storage conditions of products which enhances quality management throughout the supply chain. Revolutionary changes in supply chain include inventory forecasting, Shipment and Asset tracking, maintenance & repair, quality control, storage condition monitoring.

(vii) Smart Wearables – In the IoT world, wearable technology is a hallmark, and probably one of the earliest applications of IoT. We have now become accustomed to wearing wearable devices, for example, virtual glasses, fitness bands that measure heartbeats and calories, GPS tracking belts, and smartwatches, among others. Today, wearable devices can display calls, texts, and social media updates in addition to tracking health and fitness.

Fig – 9 (IoT based Smart Wearables)

(VI) Security Issues/ Challanges in IoT - Security challenges abound, because of the high volume of flaws regularly discovered in IoT systems. Robust IoT security includes all facets of protection, including hardening components, monitoring, keeping firmware updated, access management, threat response, and remediation of vulnerabilities. IoT security is critical as these systems are sprawling and vulnerable, making them a highly-targeted attack vector. Securing IoT devices from unauthorized access ensures that they do not become a gateway into other parts of the network or leak sensitive information. IoT security vulnerabilities are found in everything from vehicles and smart grids to watches and smart home devices. For example, researchers found webcams that could be easily hacked to gain access to networks and smart watches containing security vulnerabilities that allowed hackers to track the wearer's location and eavesdrop on conversations. Some of the IoT security issues are as follows-

Lack of visibility -Users often deploy IoT devices without the knowledge of IT departments, which makes it impossible to have an accurate inventory of what needs to be protected and monitored.

Limited security integration- Because of the variety and scale of IoT devices, integrating them into security systems ranges from challenging to impossible.

Open-source code vulnerabilities -Firmware developed for IoT devices often includes open-source software, which is prone to bugs and vulnerabilities.

Overwhelming data volume - The amount of data generated by IoT devices make data oversight, management, and protection difficult.

Poor testing - Because most IoT developers do not prioritize security, they fail to perform effective vulnerability testing to identify weaknesses in IoT systems.

Unpatched vulnerabilities - Many IoT devices have unpatched vulnerabilities for many reasons, including patches not being available and difficulties accessing and installing patches.

Vulnerable APIs - APIs are often used as entry points to command-and-control centers from which attacks are launched, such as SQL injection, distributed denial of service (DDoS), man-in-the-middle (MITM), and breaching networks

Weak passwords - IoT devices are commonly shipped with default passwords that many users fail to change, giving cyber criminals easy access. In other cases, users create weak passwords that can be guessed.

Possible

(VII) Addressing IoT Security Issues/ Challenges

Regularly check for patches and updates - Vulnerabilities are a major and constant issue in the field of the IoT. This is because vulnerabilities can come from any layer of IoT devices. Even older vulnerabilities are still being used by cybercriminals in order to infect devices, demonstrating just how long unpatched devices can stay online.

Use strong and unique passwords for all accounts - Strong passwords help prevent many cyberattacks. Password managers can help users create unique and strong passwords that users can store in the app or software itself.

Prioritize Wi-Fi security - Some of the ways users can do this include enabling the router firewall, disabling WPS and enabling the WPA2 security protocol, and using a strong password for Wi-Fi access. Ensuring secure router settings is also a big part of this step.

Monitor baseline network and device behavior - Cyberattacks can be difficult to detect. Knowing the baseline behavior (speed, typical bandwidth, etc.) of devices and the network can help users watch for deviations that hint at malware infections.

Apply network segmentation - Users can minimize the risk of IoT-related attacks by creating an independent network for IoT devices and another for guest connections. Network segmentation also helps prevent the spread of attacks, and isolate possibly problematic devices that cannot be immediately taken offline.

Secure the network and use it to strengthen security - IoT devices can place networks at risk, but networks can also serve as levelled ground through which users can implement security measures that cover all connected devices.

Secure IoT-cloud convergence and apply cloud-based solutions - The IoT and the cloud are becoming increasingly integrated. It is important to look at the security implications of each technology to the other. Cloud-based solutions can also be considered to deliver added security and processing capabilities to IoT edge devices.

Consider security solutions and tools - A large hurdle that users face in trying to secure their IoT ecosystems is the limited capacity in which they can implement these steps. Some device settings might have restricted access and are difficult to configure. In such cases users can supplement their efforts by considering security solutions that provide multi-layered protection and endpoint encryption.

Take into consideration the different protocols used by IoT devices - To communicate, IoT devices use not only internet protocols, but also a huge set of different networking protocols and well-known Bluetooth, Near Field Communication (aka NFC) and optical infrared communication. Administrators must understand the whole set of protocols used in their IoT systems in order to reduce risks and prevent threats.

Secure the heavy use of GPS - Some IoT devices and applications use GPS heavily, which carries potential security concerns. Organizations, in particular, need to be wary of cases where GPS signals can be jammed or even faked, especially if they use positioning systems for manufacturing, monitoring, and other functions. If these positioning systems are crucial to a company, means of monitoring the GPS signal should then also exist in the company. Another option would be for the company to use other positioning systems as well, such as Real-Time Kinematic (RTK).

Conclusion - The IoT is a cyber-physical system that integrates billions of heterogeneous devices and smart objects. These things are enabled by various technologies such as identification, embedded sensors, intelligent management, protocols, data storage/processing/analytics, etc. A wide range of IoT applications have been adopted and deployed in the last few years. In this paper, an overview study of the Internet of Things is presented introducing the vision, concepts, features and the promise future. Brief discussions of the main technologies, the newly developed protocols, and the most common applications of the IoT are provided. The research directions/future challenges are listed for more efforts in the near future. We emphasize the importance of the power-efficiency and time-synchronization as future trends that, we believe, need a significant focus and more investigations. The major contribution of this paper is that it brings the main aspects of the IoT and its relevance together in one paper, presented in a straightforward manner.

References-

[1] "The Internet of Things" by Samuel Greenguard
[2] **"** Getting started with Internet of Things by Cuno Pfister
[3] "Building the Internet of things: Implement new business models, disrupts competitors, Transform your Industry (Meciej Kranz)
[4] Analytics of Internet of Things – Andrew Minteer
[5] Internet of Things : A hands-on Approach – Vijay K. Medisetti
[6] IoT Fundamentals : Networking Technologies, Protocols and use cases of Internet of Things- Gonzalo Salgueiro
[7] Programming the Internet of Things- An Introduction to building integrated device-to-cloud IoT Solutions – A.C. King
[8] Designing the Internet of Things – Hakim Cassimally
[9] Internet of Things – Principles and Paradigms
[10] The Internet of Things – How smart TVs, Smart Cars, Smart Homes and Smart Cities are changing the world – Michael Miller.