Internet of Things: Architecture, security and Applications

Md Sirajuddin Inamdar and Sahadev Roy

Abstract

The reduction of costs and advancements in sensors and networks, communication standards, protocols like Bluetooth low energy (BLE), Thread (based on 6LowPAN), Z-Wave, Zigbee, have assisted in the massive surge of research interest in IoT. Additionally, cloud-Based services like data storage, data mining, application development and deployment have collectively made the process of converting IoT-based ideas into working products, significantly faster and easier. To realize the full potential of IoT synergistic efforts for the advancement of different fields such as electronics, communications, and informatics is required. This article presents an overview of underlying architecture of IoT, its security requirements, and finally different application domains such as smart cities, smart homes that will most likely be driving further research in near future of IoT. This paper addresses the people who want to quickly grasp the background of IoT and contribute towards its advancement.

Keywords

Cloud services;
Internet of things (IoT);
IoT architecture;
IoT applications;
Pervasive computing;
RFID.

I. INTRODUCTION

The Internet of Things or as it is popularly known 'IoT' is the inter-connection of embedded devices with computing capability, where these devices are uniquely identifiable within the existing framework of Internet. Characteristically, IoT is anticipated to offer sophisticated and advanced connectivity between these devices along with systems as well as services that go well beyond machine to machine (M2M) communications while covering a wide range of protocols, domains, and applications[1]. For the IoT vision to successfully materialize, the paradigm of connectivity has to think further than smartphones and advance into connecting daily objects while embedding intelligence deep into the environment. IoT can be viewed as a connecting platform between information processing and communication systems.

IoT consists of devices which can sense, calculate, communicate and actuate. These things range from minuscule chips to huge machines, all of which use some form of wireless technology to communicate with each other.

In IoT, a sizable number of devices in our surroundings are connected to the internet in one form or the other and these devices generate a large quantity of data. The generated data should be stored securely and must be reliably processed in addition to being presented in an easily understandable and flawless form. Cloud services offer virtual infrastructure required for storing, computing and presentation of generated data. This infrastructure integrates real-time analytic tools, monitoring tools, storage devices, visualization platforms, machine learning etc. Cloud computing offers a cost-based model which allows access to applications and provisioning of end to end services on demand by both users as well as businesses from anywhere [2].

The term IoT [3] or “Internet of Things” was used for the first time in the perspective of managing supply chain by Kevin Ashton back in the year 1999 but in the last decade, Internet of Things has become more wide-ranging covering a variety of sectors which include healthcare, manufacturing, utilities, transportation, etc. Even though the description of Things in IoT has changed with the evolution of technology, the main aim of helping the computer make sense of information or data without the assistance of humans remains unchanged.

Aided by the presence of open wireless technology (WiFi, Bluetooth) enabled devices in addition to embedded sensors as well as actuators, IoT has grown out its infancy stage and has started remodeling the existing Internet which is basically static into Internet which is completely integrated. The evolution of Internet has led to inter-networking or interconnection both virtual as well as real, between the people at an astonishing scale with an extraordinary pace. The subsequent revolution is the connection amongst objects to build a smarter environment. Number of the devices which are interconnected on the earth overtook the population of the earth in the year 2011. Figure 1, depicts the distribution of IoT market by 2025 as per data obtained from IDC, Intel. As per IDC, Cisco, and United Nations in 2015, there were
about 18.2 billion inter-connected devices; it is projected to reach 50.1 billion devices by the year 2020, which will be about 7 smart objects per human being on the planet earth. By the year 2025, the global value of IoT technology will be around $6.2 trillion of which $2.5 trillion value will be for devices from health care sector and about $2.3 trillion in the manufacturing sector [4].

The paper is divided into five sections. Section 1 is the introduction; Section 2 gives the definition of some commonly used terms, present trends in IoT and some key IoT enabling technologies. Section 3 explains IoT architecture and security requirements of each of its components. Section 4 gives an overview of different application areas and some examples of IoT applications in each area. A brief Summary and conclusion is presented in section 5.

II. DEFINITIONS, KEY ENABLING TECHNOLOGIES, AND TRENDS

The present growing trend of ubiquitous computing may be defined as embedding microcontrollers or microprocessors in everyday objects like glasses (Google glass) so that they can communicate and exchange information. Ubiquitous computing is also referred to as pervasive computing. Caceres and Friday identified two significant technologies that will be helpful in the building of infrastructure for ubiquitous computing as Cloud Computing and IoT [5].

Mark Weiser who is the forefather of ubicomp (Ubiquitous Computing) has defined the smart environment to be “a physical world which is invisibly and richly interwoven with computational elements, sensors, actuators, and displays, embedded seamlessly in our lives in the form of everyday objects, connected by a continuous network” [6].

As per authors of [7], RFID system which consists of both readers as well as tags, is at the vanguard of technologies that are driving the growth of IoT. This is a result of strong community support, low cost and maturity of RFID. The situation has changed at present with the development of near field communication (NFC), WiFi, IPv6 over low-power wireless personal area networks (6LoWPAN), Bluetooth low energy (BLE), wireless-sensor-networks (WSN), actuators. These along with RFID have been recognized as the basic components that are leading in the linking of digital and real world.[8][9][10]. An important role is being played by Wireless technologies in the growth of IoT. The reductions in weight, cost, size, energy consumption of sensors have also helped in the growth of IoT.

IoT may be thought of as a subset or a result of ubiquitous computing. IoT utilizes everyday objects embedded with microprocessors/controllers, which in IoT jargon are known as ‘things’ and exchange of information between these so-called things takes place through the internet. The conception of Internet has helped towards achieving the vision of ubiquitous computing which is to provide every individual device the capability of communicating with any of the other available devices in the whole world. The advancements along with the convergence of MEMS technology, digital electronics, and wireless communications has led to the progress of miniature sized devices which have the ability to compute, sense as well as wirelessly communicate in short distances. Wireless sensor networks (WSN) are formed by the interconnection of these miniature sized devices which are sometimes referred to as nodes. Wireless sensor networks are used in a broad range of applications which include environmental monitoring, traffic monitoring, infrastructure monitoring, retail etcetera. These WSN have the capability to make available ubiquitous sensing that is vital in realizing on the whole, vision of ubiquitous computing.

For the accomplishment of a complete internet of things vision, a scalable, efficient, market-oriented and most importantly secure computing and storage resources are required. The recent emergence of Cloud computing with their promises of a dependable end to end service delivered with the help of advanced data centers having storage technologies that are virtualized show great potential. These cloud services act as a platform for receiving data from the sensors while also providing services to analyze as well as interpret the data. If desired these cloud services also present the
user with web based metrics or visualization. The analysis, as well as the processing of data, is done in the background concealed from the user. Cloud computing has matured and now promises highly reliable, scalable and autonomous services to provide resource discovery, resource access, and storage necessary for the upcoming generation of IoT applications[11].

Visualization enables the communication between the environment and the user, hence playing a very significant role in an IoT application. The recent advances in technologies of the touch screen, explosive growth in the use of smart phones and tablets has been helpful in visualization. For a layman to fully gain from the revolution taking place in IoT, an easy to understand visualization which may also be flashy and attractive has to be produced. As we shift from two-dimensional to three-dimensional screens, consumers can be provided with more information than was possible with 2D screens. This also allows the policy makers to process the data in raw form into information which is influential in quick decision making. Extracting this consequential information from unprocessed data carries great significance. The conversion of raw data to useful data comprises of visualization as well as event detection of the related raw data along with modeled data. The information in the processed data is represented as per the requirements of end-user.

The popularity of most of the paradigms changes with time. As per the search trends of Google, the web search popularity for the terms IoT, Pervasive Computing and Wireless Sensor Networks(WSN) during the last 5 years is shown in Fig. 2 [12]. As can be seen, since 2011 search volume for IoT is consistently rising while a declining trend has been observed for WSN. This inclination is expected to persist as new technologies come together to form an authentic and absolute IoT.

Components essential for the IoT from a higher level perspective can be diversified into four different layers as shown in figure3. First of the four layers is the perceptual layer which includes embedded communication hardware, actuators and sensors. The second layer is called network layer whose purpose is to establish and maintain communication between components of different layers (data transfer between sensor and cloud) as well as same layer (data sharing between the sensors) when required. The third layer is the Middleware or support layer which is providing storage in addition to computing tools on demand for the purpose of data analytics. The fourth layer is the application layer whose purpose is to provide different services like intelligent transportation, smart home and so on [13].

### III. IoT ARCHITECTURE AND SECURITY REQUIREMENTS

![IoT architecture. The four layers of IoT and their functionalities.](image)

The perceptual layer is the most basic level. It collects information using different physical equipments like a variety of sensors, RFID reader, GPS. The collected information which includes environmental condition, object properties etc is used to identify the physical world. The most common component used in the perceptual layer is sensor for capturing data and using the data to depict physical world. Figure 4 lists sensors which are commonly used in IoT applications.

Nodes in the perceptual layer usually lag behind in terms of storage capacity and computing power. Consequently it is not capable of applying frequency hopping mechanism or encryption algorithm of public keys and so on for security purposes, thus making it very tricky to protect these nodes from attacks such as denial of service, data manipulation, eavesdropping etc. The main security requirement in perceptual layer is to ensure that the data from sensors and other peripherals is authentic, confidential and free from any
kind of manipulation. Security requirements of each of the four layers are summarized in Fig 5.

Authentication is the primary requirement of perceptual layer in order to prevent node access which is illegal. Further to ensure information confidentiality and authenticity of sensor data lightweight encryption of data before transmission among the nodes is needed. Care must be taken to avoid complicated encryption algorithms which cannot be handled by the available computing power of perceptual layer.

Authentication is the primary requirement of perceptual layer in order to prevent node access which is illegal. Further to ensure information confidentiality and authenticity of sensor data lightweight encryption of data before transmission among the nodes is needed. Care must be taken to avoid complicated encryption algorithms which cannot be handled by the available computing power of perceptual layer.

The next level is the networking layer. Networking layer is in charge of reliably transmitting information from the basic perceptual layer, initial information processing, classification as well as polymerization. In the network layer, the transmission of information relies on a number of basic networks like wireless network, mobile communication, and internet. Network infrastructure along with communication protocols is quite essential to smooth exchange of information between devices.

Owing to the availability of advanced computing power available at this level the security at networking layer is quite reliable, to prevent most of the attacks, but there is still a substantial risk of MitM (man in the middle) attack, counterfeiting attack. To prevent illegal node access in network layer, Identity authentication can be employed. As there is sufficient computing power available strong encryption between client and server can help in preventing MitM and counterfeiting attacks. DDoS or distributed denial of service is very commonly used to attack this layer. DDoS attacks are very severe on IoT. Identification of vulnerable nodes and strengthening it, data traffic monitoring and use of automated DDoS mitigation tools are some of the common methods employed to avoid DDoS attacks.

The 3rd layer is called the support layer. It is used to setup a reliable platform to support an application. On a support platform numerous intelligent computing machines are organized through cloud computing and network grid. It acts as a bridge between the application layer and networking layer.

A significant outcome of IoT is the generation of gargantuan amounts of data. Issues such as Storage of data, tracking its ownership if needed and knowing when data becomes obsolete, turn out to be critical. The consumption of the energy by internet is up to 5% of the total generated energy these days and with the increasing demand for internet, it is certain to escalate even further. Therefore, data centers that are centralized and utilizing harvested energy will improve reliability as well as energy efficiency.

For actuation along with smart monitoring, the data must be intelligently stored and used. It is essential to develop algorithms with artificial intelligence that can be centralized or scattered based on the situational requirements. New synthesis algorithms have to be designed to extract information from the data being collected. A centralized infrastructure in order to support data analytics and storage is an important requirement for IoT. As of 2016, an extensive range of increasingly popular Cloud-based data analytics and storage solutions are available. These cloud-based services in addition to data storage and analysis are also providing data visualization services thus becoming an inseparable part of the IoT solution.

Security requirement at this layer is critical since this layer does all the data processing in addition to taking all the decisions. Since, based on the decisions made at this layer applications perform various actions, unauthorized access to the decision making by a person with malevolent intentions could lead to disastrous end results. Since cloud computing platforms provided by major companies are mostly used at this layer security level is quite high with companies providing advanced malware protection, data security, data privacy, data encryption, threat detection etc. Furthermore, since almost 90% of the...
IoT data as per IDC will be stored in third party clouds ensuring top level security is very critical.

The application layer is the uppermost level. It provides personalized services in accordance with the user’s needs. Most of the users access IoT through the interface of the application layer for instance by using TV, mobile equipment, PC’s and so on.

The level of security required largely depends on the application. For instance the level of security should be very high if the application is a pacemaker in order to prevent altering of decisions made in the support layer since any alteration of the decision by a person with malevolent intentions could lead to the death of a person. However, security requirement for an application like glowing of a led lamp or bulb is comparatively lower but still needed. Since data sharing is quite common in this layer heavy encryption of data, ensuring the privacy of data, controlling access to the data with the help of key exchange or some other algorithm has to be done. Finally educating or creating awareness among the user’s the importance of setting up strong passwords to access application interface is very important, as a weak password will allow illegal users to bypass every security measure used in the application no matter how advanced it may be.

**Fig 5. Security requirements of different layers in IoT.**

**IV. IOT APPLICATIONS**

There are several domains where applications for IoT can be found. These domains will be heavily impacted by the growth of IoT. The classification of applications could be based on availability of the network, heterogeneity, coverage, scale, impact, repeatability. We classify the IoT applications into five domains: (1) Smart cities; (2) Manufacturing; (3) Building and home automation; (4) Healthcare and (5) Transportation and logistics industry. This is depicted in Fig 3. There is considerably huge intersect between applications and usage of data amongst different domains. For example, IoT-based Home automation produces data about usage of electricity in the home and this data is made available to the company providing electricity. The company, in turn, can use the data to optimize the demand and supply of electricity. A few of the typical applications seen in each area are listed in Fig 6.

**A. Smart Cities**

IoT in Smart Cities will tackle commonly faced urban challenges like pollution, traffic, transportation, energy efficiency, parking, security by using advanced techniques in communications, gathering and analyzing data. IoT provides the capability of real-time, remote monitoring and handling of data from areas such as communication, sensors on devices, video surveillance, transportation, and sensors that are located all over the city. Thus an intelligent environment called smart city can be created using IoT[14]. The term ‘Smart Cities’ is used to represent the cyber-physical ecological system that emerges by the deployment of advanced infrastructure for communications and novel ideas and services over a complete city. By making use of advanced services we can certainly improve the efficiency in the handling of the available physical infrastructures of a city like road networks, land, power grid and so on. This improvement in efficiency will in all certainty lead to its citizens leaving a superior class of life[15]. An overview of application areas in a smart city and few illustrations in each of those areas is shown in Fig. 7

**Fig 6. IoT application areas and examples.**

IoT can be made use of to offer sophisticated systems of controlling traffic, through which it may be possible to supervise car traffic in highways or big cities and install services that suggest traffic routing guidance to avoid congestion in areas prone to congestion[16]. In this application, cars will be thought of as representing basic IoT elements which are also known as ‘smart objects.’ [17].
IoT can be used to offer smart parking system which is based on sensors and RFID [18][19]. These smart parking systems allow monitoring of available spaces for parking and based on the availability, it provides drivers with detailed information of available parking locations, as a result improving movement in most of the urban areas and avoiding congestion as well as wastage of time and fuel.

IoT can also be used monitor the stream of vehicular traffic using sensors on highways and extract comprehensive information such as the number of cars and average speed [16].

IoT can also be used to detect the level of pollution in the air with various gas sensors and chemical sensors, extracting smog information like the level of carbon monoxide and carbon dioxide, PM10 et cetera. Such information could then be delivered to health agencies [20].

Smart bins currently in use in the city of Dublin are capable of sending emails and text to waste management division when almost full. These smart bins are also equipped with a solar compactor that is activated when it reaches a certain level thus allowing six to eight times more storage when compared to normal bins. These smart bins thus help the waste management companies in better planning and management of the garbage woes of big cities.

![Fig. 7. Overview of Smart city applications based on IoT.](image)

**B. Manufacturing**

IoT in the manufacturing industry is occasionally referred as industrial internet of things or IIoT. IIoT is expanding and growing as fast as the IoT in the outside world due to the influx of various smart devices in addition to the available connected sensors in manufacturing plants[21][22]. The connected manufacturing plant as it is used today is a comparatively closed environment designed only to communicate within the confines of the plant network and not the outside world using the Internet thus making it feasible to take advantage of many of the features of IIoT without compromising much on the security. Changing the internal network of a plant to Internet Protocol (TCP/IP) should let a company use smart devices, sensors in an internal IIoT. In a forecast of May 2016 on the global growth of the IoT, IoT market is poised to grow up by 19%. It is predicted by International data corporation (IDC) that the IoT market in the manufacturing operations sector will reach at least $98.8 bn by 2018. BI mentions a report of TATA Consultancy which indicated an average boost in revenue by 28.5% between the years 2013, 2014 for manufacturers which have implemented IoT solutions. Some of the use cases of IoT in manufacturing industry are listed below,

IoT allows predictive maintenance which is a technique through which the condition of various tools and machines or simply 'assets' is checked and the time when next maintenance should be performed is predicted. Through predictive maintenance, scheduling of corrective maintenance based on convenience can be provided which helps in avoiding unexpected equipment failures.[23]. Predictive maintenance is done using an array of embedded tools useful for monitoring assets; assets communicate their state, for example, their lubrication levels, thermal properties, vibrations, oil testing and other important indicators of asset health. This helps the asset management teams in spotting deficiencies if any before they cause unscheduled downtime.

IoT allows manufacturing systems to keep track of products in real time by scanning in and out of various raw materials as well as finished products with the help of RFID tags. This helps in prevention of theft as well as locating of items, it also helps in keeping track of expiration dates of various products, damage by weather, estimation of demand for various products based on the outflow of products etc.

The use of IoT results in the automation of a lot of work order filling and inspection thus leading to a reduction in human involvement at the ground level. This helps in solving a major issue of manufacturers which is finding young talented maintenance workers to fill in for retiring ones.

Flow optimization is being achieved by making use of IoT for predictive maintenance and scheduling maintenance without stopping production completely wherever possible around production runs. Flow optimization is also being achieved by carefully
planning the route taken by raw materials from beginning of production until the end where finished product is obtained[24].

Image analytics are being used to separate good products from defective products on the production line at a much faster rate than manual separation method.

A variety of wearable sensors that monitor human workers and provide information such as breathing, heart rate, toxic gas level, motion, and posture are being used by industries in order to ensure the safety of employees in hazardous or dangerous working environments like nuclear plants, deep earth mines and so on.

C. Smart Homes

Smart homes which are filled with products that are network connected are loaded with potential to make our living much easier, more comfortable, and very convenient. Construction of homes with IoT technology incorporated right from the planning stage will largely help in reducing the consumption of electricity, water and other resources which are associated with basic needs in a home, while also helping in increasing the level of comfort for humans occupying it, which includes employees in an office or residents of private homes[25]. There is an impact both in the economic terms such as reduced operational or regular expenditures in addition to societal terms like reducing the emissions of carbon associated with buildings, which without any doubt are one of the key contributors to the present global problem of excessive harmful gas emissions. An important role is being played by sensors in this application as sensors are extensively being utilized to both supervise consumption of resources along with proactive detection of users needs. Home automation integrates various subsystems thus requiring a level of standardization to guarantee interoperability[26].

The capacity to take decisions in a cooperative as well as distributed way and to trigger action or actuate, is essential to make sure that decisions that are taken for the resources (ex: switching on/off of lights, heating or cooling) under control are as per the needs and expectations of the users, which consecutively are strictly entwined to the activities that they take on or plan to take [27]. Figure 8 is a schematic showing the interconnection of different application modules that constitute a smart home. Some of the application modules in smart homes where the concept of IoT is being used are listed.

Controlling air conditioner based on temperature, humidity, and moisture in the surrounding environment. The Lyric®, Nest®, and many such WiFi enabled thermostats are available in the market from the past five years. They can be thought of as the starting point for the influx of WiFi enabled common household devices in the market. The smart home devices from Lyric, Nest and others act as controlling devices in the home and providing energy savings, comfort, and convenience while also providing connections to various other services using the cloud so as to help in making the user experience more efficient and comfortable. These smart home devices allow the users to directly connect and set the temperature while they are away, on the way to home, or while at home.

Controlling the light’s intensity in the home to the desired brightness level, motion-based lighting using motion sensors, mood based lighting based on music being played. Smart lighting solutions such as hue smart lights designed and developed by Philips can be used to provide mood based lighting, send alert signals etc[28].

Controlling the entertainment system using voice commands, gestures. The current generation of smart televisions from various manufacturers has these features inbuilt in them.

Automated controlling of blinds to draw themselves close or open based on the intensity of sunlight or time of the day.

Controlling devices based on audio or voice commands. Amazon Echo by Amazon and Google home from Google are two of the many voice assistant devices that are capable of listening to voice commands and respond accordingly or provide
weather updates, real-time traffic updates, set alarms and many such actions.

D. Healthcare

IoT provides novel ideas to improve present healthcare system [29]. With the help of its connectivity, all the information related to healthcare such as diagnosis reports, medication, therapy, recovery, even every day activity could be gathered, managed and shared efficiently. Take for instance, the heart rate of a patient can be gathered by sensors at regular intervals and can then be sent to the hospital or the doctor's office. Using personal devices such as a laptop, tablet, mobile phone and so on and the internet, the healthcare services based on IoT can be portable and personalized [30]. Due to the availability of mobile internet services the development of IoT-powered home healthcare services (IHHC) has been expedited [29].

Smart biosensors make precise and reliable monitoring of a person’s body to collect important indicators of health status possible. The collected indicators are then sent to doctors where it is analyzed and appropriate action is taken. Smart healthcare solutions are not only for the sick and elderly people, but active, healthy people can also be notified upon detection of irregularity.

IoT can be utilized to improve the current generation of assisted living care solutions. Medical sensors or biosensors will be either embedded or carried by Patients to monitor different parameters like blood pressure, body temperature, breathing activity and so on. Additional sensors which are either fixed like proximity sensor or wearable sensors such as gyroscopes, accelerometers can be made use of to collect data required in order to monitor activities of a patient in their homes. Locally gathered Information will then be transmitted to a distant medical center which will have the ability to perform sophisticated analysis of data and provide quick response team to a patient when needed. The connection of different sensors may possibly provide a complete picture of patient’s health parameters which may lead to a trained medical staff intervention upon the detection of conditions that act as indicators of deterioration in health, as a result realizing preventive care. An additional relevant domain of application is related to personalized healthcare solutions. By exploiting the capabilities of sensors especially wearable along with suitable device applications running on a mobile phone or other computing devices allows people to keep track of their daily routine activities like steps walked or calories burned or number of hours slept etc providing suggestions to enhance their lifestyle as well as ways to prevent onset of various health problems[31].

The idea of using biosensors to discover health conditions of a patient and monitor their recovery is not new, though, with the introduction of micro-sized sensors and the advent of embeddable devices, the prospective for embedded health technology seems to be very promising. There is a wave of companies who have started working in this exciting new space. These companies on account of the improved use of data from patients and hospital have started to radically raise the intensity of care that the patients receive as well as patient advocacy all through the healthcare industry.

The monitoring system can be used by hospitals for patients who are hospitalized and require constant monitoring of physiological status. These systems make use of biosensors to gather physiological information which is stored, analyzed using cloud services. The collected information is sent to caregivers or doctors for additional analysis as well as review. The value of care provided to the patients is significantly improved as a result of using these IoT-based monitoring systems which in turn could lower the requirement of visits to the hospital in the future.

E. Transportation And Logistics Industry

IoT has become an important part of the transportation and logistics industry [1]. IoT Logistics Solutions focuses on monitoring as well as real-time tracking of both finished products in addition to raw materials by using Smart Tags or RFID tags in the supply chain. Important information such as the date of production, date of expiry and other such information are added to tags for quicker tracking of products. Imagine prompt shipping of raw materials just in time when the production floor needs them. Envision timely Logistics Management Systems which will precisely track assets whether on the road, on water, or in the air [32]. Additionally, it is expected that IoT will offer solutions that will transform transportation and automobile services [33]. Vehicles are being equipped with increasingly powerful networking, communication, data processing, and sensing capabilities, using concepts of IoT in these cars can lead to further enhanced capabilities and may even allow sharing of underutilized resources amongst vehicles which are parked or moving. For instance, IoT makes tracking of each vehicle's current location,
monitoring of its movement, along with prediction of its future position possible. In recent times, BMW has developed iDrive system which is an informatics system which uses various sensors, tags to track the location of vehicle and to assess the condition of road and provide directions to the driver [34]. Zhang and others [35] designed a system that monitors temperature and humidity inside the refrigerator truck by using sensors, RFID tags, and wireless communications technology. Companies like Apple and Google are moving ahead with autonomous or driverless cars using IoT in transportation. These driverless cars have the ability to autonomously detect as well as differentiate between pedestrian traffic and vehicular traffic in addition to taking evasive steering actions to avoid collisions when needed [36][37]. These cars can even undertake journeys through pre-programmed routes and also provide emergency assistance whenever required. In the future these cars may even display location-based, personalized ads like nearby suitable restaurants based on your previous online food orders, preferred petrol pumps etc. Currently, these autonomous cars are in the rigorous testing stage and within the close future, we will be seeing these cars in most of the major cities throughout the world. Security and protection of privacy are the two major areas of concern that need to be handled before use of IoT is widespread in the transportation as well as logistics industry since most of the vehicle drivers are concerned about privacy invasion and information leak[38]. An effort in law, and regulation, as well as technology, is needed to thwart unauthorized access, disclosure of private data. Figure 9 lists the Smart transportation and logistics example applications.

RFID technology is already being used for the purpose of inventory management in several sectors, all over the supply as well as the delivery chain. It depends on the ability of RFID technology in order to identify, provide support for the purpose of tracking goods. This technology is usually used for a business to monitor, manage the product's movement through a company's supply chain. RFID tags, generally are attached directly either to the items or to the container being used to carry them, while RFID readers are placed all over the facility for monitoring purpose[39]. Using IoT concept enhanced flexibility can be provided in terms of the position of readers, whilst facilitating seamless interoperability amid applications being utilized by various sections that are dealing with the product through various phases of the product’s life-cycle. IoT can also be used in retail applications for real-time monitoring of product availability, maintaining an accurate inventory of stock. They can also take part in aftermarket support, where users will be capable of automatically retrieving data related to the products they bought. Identification technology can also help in reducing thefts and counterfeiting by providing a unique id to the products that include a complete description of the said good.

![Image](https://doi.org/10.24999/IJOAEM/0207003)

**Fig 9. Smart transportation and logistics applications.**

Use of IoT in Logistics serves a number of purposes in addition to purposes mentioned above such as optimizing the inbound and outbound traffic in manufacturing plants to enhance production by improving goods throughput thus helping in achieving maximum productivity. By optimizing the traffic waiting times and the environmental impact due to pollution by vehicles can be reduced, need for manual monitoring can be eliminated. Delivering finished products in the retail space only when required will get rid of the overstocking issue of retailers thus increasing the retailer's operational efficiency.

**V. CONCLUSION**

Internet has significantly altered our living style by moving interactions among people at virtual level within contexts that range from social relationships to professional life. IoT can possibly add new dimensions to this as a result of enabling communication with as well as among the smart objects, consequently leading to a vision of “anything, anytime, anymedia” communication.

Internet of things has a massive potential for development of applications apart from the applications mentioned in this paper. IoT based applications have improved the efficiency with which we lead our lives and some of them have become an

integral and inseparable part of it. IoT is projected to play very important role in development of smart cities and eventually a smarter world. The rise of cloud computing and miniaturization of sensors have aided in the exponential expansion of IoT. Privacy and security is a challenging issue faced by both cloud computing and deployment of IoT applications since sensitive personal information is accessed and stored in these applications, continuous research is being done to overcome these issues. Integration of different machine learning, artificial intelligence, data mining algorithms, context aware computing in applications such as environment monitoring, smart grid, and smart transportation can help in realizing a smart and healthy city in the true sense. Current research focus is on the development of above mentioned algorithms as well as discovering methods for its integration with diverse applications in order to enable these applications to handle complex real life problems such as pollution, energy conservation and so on.

In this paper we have introduced IoT and described the technologies aiding in its growth. It is followed by an outline of basic architecture of an IoT based application. The security challenges faced by each layer of IoT architecture, constraints of each layer and some common methods that can be used to overcome these challenges are also explained in brief. Finally we refer to the varied application areas while also mentioning some applications currently in the market. We have mentioned the expected market share of different application areas in addition to issues that can be overcome by the use of IoT in these areas. Since IoT is still in the development stage, it is continuously evolving and highly dynamic.

REFERENCES


Internet Assembly (pp. 447-462). Springer Berlin Heidelberg.


167


Md Sirajuddin Inamdar  
mdsiraj1992@gmail.com  
Dept. of ECE  
NIT Arunachal Pradesh, Yupia, India  
Sahadev Roy  
sdr.ece@nitap.in  
Dept. of ECE  
NIT Arunachal Pradesh, Yupia, India