INTERNET OF THINGS (IOT): Iot Applications & Future Technology

Satya Prakash
Assistant Professor
Department Of Computer Application,
DPBS College Anupshahar- 203390, (UP) India

P.K. Tyagi
Professor And Head
Department Of Statistics, DPBS College
Anupshahar- 203390, (UP), India

Abstract:
We’re entering a new era of computing technology that many are calling the Internet of Things (IoT). Machine to machine, machine to infrastructure, machine to environment, the Internet of Everything, the Internet of Intelligent Things, intelligent systems—call it what you want, but it’s happening, and its potential is huge. We see the IoT as billions of smart, connected “things” (a sort of “universal global neural network” in the cloud) that will encompass every aspect of our lives, and its foundation is the intelligence that embedded processing provides. The IoT is comprised of smart machines interacting and communicating with other machines, objects, environments and infrastructures. As a result, huge volumes of data are being generated, and that data is being processed into useful actions that can “command and control” things to make our lives much easier and safer—and to reduce our impact on the environment. The creativity of this new era is boundless, with amazing potential to improve our lives. The following thesis is an extensive reference to the possibilities, utility, applications and the evolution of the Internet of Things. The Internet of Things (IOT) describes a kind of network which interconnects various devices with the help of internet. IOT assists to transmit data with among devices, tracing and monitoring devices and other things. IOT make objects ‘smart’ by allowing them to transmit data and automating of tasks, without lack of any physical interference. A health tracking wearable device is an example of simple effortless IOT in our life. A smart city with sensors covering all its regions using diverse tangible gadgets and objects all over the community and connected with the help of internet. Thus, IoT is paving the way for new dimensions of research to be carried out. This paper presents the recent development of IoT technologies and discusses future applications and research challenges.

Keywords: Internet of Things (IoT), Architecture of IOT; Implementaation;IOT Aplicacations ;future technologies; IoT Challenges ; Conclusion,

Introduction:
IoT stands for Internet of Things. It refers to the interconnectedness of physical devices, such as appliances and vehicles that are embedded with software, sensors, and connectivity which enables these objects to connect
and exchange data. This technology allows for the collection and sharing of data from a vast network of devices, creating opportunities for more efficient and automated systems. The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. The IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit; when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its transport.

The Internet of Things (IoT) is an emerging paradigm that enables the communication between electronic devices and sensors through the internet in order to facilitate our lives. IoT use smart devices and internet to provide innovative solutions to various challenges and issues related to various business, governmental and public/private industries across the world. IoT is progressively becoming an important aspect of our life that can be sensed everywhere around us. In whole, IoT is an innovation that puts together extensive variety of smart systems, frameworks and intelligent devices and sensors. Moreover, it takes advantage of quantum and nanotechnology in terms of storage, sensing and processing speed which were not conceivable beforehand. Extensive research studies have been done and available in terms of scientific articles, press reports both on internet and in the form of printed materials to illustrate the potential effectiveness and applicability of IoT transformations. It could be utilized as a preparatory work before making novel innovative business plans while considering the security, assurance and interoperability. As the internet continues to evolve, it has become more than a simple network of computers, but rather a network of various devices, while IoT serves as a network of various “connected” devices a network of networks [3], as shown in Fig. 1. Nowadays, devices like smartphones, vehicles, industrial systems, cameras, toys, buildings, home appliances, industrial systems and countless others can all share information over the Internet. Regardless of their sizes and functions, these devices can accomplish smart reorganizations, tracing, positioning, control, real-time monitoring and process control. In the past years, there has been an important propagation of Internet capable devices. Even though its most significant commercial effect has been observed in the consumer electronics field; i.e. particularly the revolution of smartphones and the interest in wearable devices (watches, headsets, etc.), connecting people has become merely a fragment of a bigger movement towards the association of the digital and physical worlds. With all this in mind, the Internet of Things (IoT) is expected to continue expanding its reach as pertains the number of devices and functions, which it can run. This is evident from the ambiguity in the expression of “Things” which makes it difficult to outline the ever-growing limits of the IoT [4]. While commercial success continues to materialize, the IoT constantly offers a virtually limitless supply of opportunities, not just in businesses but also in research. Accordingly, the understudy addresses the various potential areas for application of IoT domains and the research challenges that are associated with these applications.

Internet of Things (IOT):

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced
customer service, improve decision-making and increase the value of the business.

This word IOT was first suggested by Kevin Ashton in 1999. The subsequent segment represents fundamental of IOT. It hands out several covering pre-owned in IOT and varied fundamental denominations connected. It is primarily enlargement of helping-hand using internet. When the household devices are connected with the help of internet, this can help to automate homes, offices or other units using IOT. IOT is being used during COVID-19 pandemic for contact tracing.

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.

INTERNET-OF-THINGS (IOT) EXAMPLES

Connected cars.
Smart appliances.
Connected security systems.
Smart agriculture equipment.
Connected retail.
Connected healthcare monitors.
Connected manufacturing equipment.
Connected cities.

IoT architecture: Due to the ever-evolving nature of IoT devices, and the wide diversity of sensors, there is no one-size-fits-all architecture for IoT projects. However, some of the building blocks will be similar from project to project.

First, you will need to build with scalability in mind. The amount of data that you will collect over time will take on enormous proportions and you will need a platform that can accommodate this in the long run.

You will also need to ensure that you have high availability at any given time. Having system failures could make you lose some business in the best case, or could have fatal consequences in the worst cases.

Finally, you will need a system that is flexible enough to accommodate quick and frequent changes. As your architecture evolves, or your business needs change, you will need to iterate quickly without breaking the existing architecture.

The three layers are Perception (or Devices), Network, and Application.

- Perception / Sensing Layer: The sensors themselves are on this layer. This is where the data comes from. The data could be gathered from any number of sensors on the connected device. Actuators, which act on their environment, are also at this layer of the architecture.
- Network: The network layer describes how large amounts of data are moving throughout the application. This layer connects the various devices and sends the data to the appropriate back-end services.
- Application: The application layer is what the users see. This could be an application to control a device in a smart-home ecosystem, or a dashboard showing the status of the devices which are part of a system.
Three Layer IOT Architecture | Five Layer IOT Architecture

In addition to the Perception and Application layers, which are the same, you will usually see the following three layers.

- **Transport:** This layer describes the transfer of data between the sensors in the Perception layer and the Processing layer through various networks.

- **Processing:** Sometimes referred to as the Middleware layer, this one stores, analyzes, and pre-processes the data coming from the Transport layer. In modern software applications, this is often located on the edge of the cloud for low latency communications.

- **Business:** This layer is often referred to as the Business Intelligence layer. Located at a higher level than the Application layer, the Business layer describes everything that has to do with the stakeholders. Decision-making will be done here based on the data found and consumed at the Application layer.

**Stages of IoT Solutions Architecture:**

Having discussed the IoT layers, how can businesses benefit from them and how can they maximize the value of IoT? The Internet of Things (IoT) may refer to connected devices and protocols, but in reality, the data from these devices is siloed, fragmented, and isolated. As such, these fragmented insights alone do not provide enough information to justify an IoT strategy that involves a significant investment of resources. To capitalize on IoT, enterprises must allow devices to interact freely, and they must maximize device and system synergies. You need to ensure your infrastructure supports the IoT architecture. The following are various stages of IoT architecture implementation in enterprises:

**Connected Objects/Devices:** As a first step towards IoT architecture, the physical layer must be established within the environment. There would be no Internet of Things without “smart” or connected objects. Typically, these are wireless sensors or actuators in the perception layer.

Sensors collect and analyze data from the environment in order to make it usable for further analysis. Actuators are involved in measuring the change recorded by the sensors. It is possible to connect sensors or actuators in a wired or wireless manner in order to perform sensing and actuation. Local Area Networks (LANs) and Personal Area Networks (PANs) can be used for connecting sensors and actuators.

**Internet Gateway:** When step one is done properly, the next step that needs to be done is to set up an internet gateway. As the sensors and actuators collect data in analog form, we must have a means of converting the analog data into digital data in order to process it. We use the internet gateway to accomplish this task. In the internet gateway stage, raw data will be received from the devices and pre-processed before being sent to the cloud.

**Edge IT Systems:** The third stage of an IoT architecture involves pre-processing and enhanced data analytics. In light of the significant amount of data collected by IoT systems and the consequent bandwidth requirements, edge IT systems play a crucial role in reducing the pressure on the core IT infrastructure. Edge IT systems employ machine learning and visualization techniques to generate insights from collected data. Machine learning algorithms provide insights into the data while visualization techniques present the data in an easy-to-understand manner.

**Data Centers and Cloud Storage:** After the data has been properly preprocessed and analyzed, and all loopholes have been removed, the data is sent to the data centers and servers for final analysis and reporting. Data Centers and Cloud services fall...
under the Management Services category and usually process data through analytics, device management, and security controls. Furthermore, the cloud also enables the transfer of data to end-user applications like Healthcare, Retail, Environment, Emergency, Energy, etc.

**How does IoT work?**

An IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for instance, to set them up, give them instructions or access the data. The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed. IoT can also make use of artificial intelligence (AI) and machine learning to aid in making data collecting processes easier and more dynamic.

**IoT implementations:**

use different technical communications models, each with its own characteristics. Four common communications models include: Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data-Sharing . These models highlight the flexibility in the ways that IoT devices can connect and provide value to the user. Further, for the IoT to function three major components are required: Devices, Communication Network and Computing and Storage machines. IoT platforms connect the sensors and data network to one another, integrating with back-end applications to provide insight into large volumes of data. For example, healthcare with IoT networks can trigger an alarm automatically when a device with a particular sensor, senses something wrong with the person wearing .

**Implementation Requirements & Steps:**

Effective and seamless implementation of IoT depends on specific tools, such as:

- **High-Level Security**
- **Asset Management**
- **Cloud Computing**
- **Data Analytics**

**History of the Internet of Things:**

The idea of adding sensors and intelligence to basic objects was discussed throughout the 1980s and 1990s (and there are arguably some much earlier ancestors, but apart from some early projects -- including an internet-connected vending machine -- progress was slow simply because the technology wasn’t ready. Chips were too big and bulky and there was no way for objects to communicate effectively. Processors that were cheap and power-frugal enough to be all but disposable were needed before it finally became cost-effective to connect up billions of devices. The adoption of RFID tags -- low-power chips that can communicate wirelessly -- solved some of this issue, along with the increasing availability of broadband internet and cellular and wireless networking. The adoption of IPv6 -- which, among other things, should provide enough IP addresses for every device the world (or indeed this galaxy) is ever likely to need -- was also a necessary step for the IoT to scale.
Applications of IoT: The IoT finds application in various private and public aspects of life.

Agriculture: The ever-increasing world population drives up the demand for agricultural products. However, the migration of young people to big cities destabilizes the human resource required for agricultural development. IoT and related technologies can be pivotal in automating farming processes and fulfilling food demand.

Consumer Applications: The Internet of Things makes people’s lives easier by monitoring and managing their lifestyles. There is a massive market for intelligent electronics, watches, television systems, health tracking, and virtual reality. In addition, IoT is leading the market with applications such as home security and personal asset tracking.

Healthcare: Wearable IoT devices provide a range of benefits to patients and healthcare providers alike. By extension, IoT enables healthcare professionals to monitor patients remotely. The devices can automatically collect patients’ health vitals like blood pressure, heart rate, temperature, and more.

Insurance: IoT is altering traditional business models like insurance. It simplifies and accelerates the claim and underwriting process. Besides reducing costs, digital networking via IoT generates additional revenues. Cross-selling and more significant customer interaction become a strategic component for insurers.

Manufacturing: The Internet of Things creates a more technically-driven environment for manufacturing industries. It can automatically track development cycles, facilitate the production flow, and manage inventories.

Retail: IoT devices can collect vital data on a product’s shopping lifecycle. Once this data is processed and analyzed, retail managers can make valuable decisions to improve retail operations and the customer experience.

Transportation: IoT applications integrate personal and commercial vehicles by improving communication and information distribution. Besides connecting consumers and goods, it offers benefits such as route optimization, automobile tracking, weather monitoring, distance coverage, and more.

Utilities/Energy: A grid can have IoT capabilities with intelligent meters, receivers, sensors, and energy boxes communicating. IoT applications in utilities generate revenue, improve efficiency, and conserve resources. Utility providers can keep up with the rising demand by optimizing energy and distribution with the help of IoT.

Traffic Monitoring: Intelligent traffic monitoring helps improve decision-making and achieve urban growth. An IoT-based system collects, processes, and analyzes real-time traffic data to provide updates on traffic incidents and congestion. In addition, early warning messages save commute time during peak hours.

Hospitality: Many hotels allow guests to control air conditioning, heating, or ventilation from a central location. Television control and greeting devices are also common. Moreover, Internet of Things devices alert the staff about various appliances’ operating status. As a result, technicians can fix critical appliances even before any major functionality loss occurs.

Water Supply: Water scarcity is a reality. IoT applications have a potential solution to monitor, control, and regulate the quality and usage of water. Besides, it also maintains associated equipment such as pumps, pipes, etc. Smart water technology connects water systems with people.

Fleet Management: IoT enables predictive fleet maintenance by boosting visibility, efficiency, and manageability. It helps to monitor cargo better and
improves driver operation. In addition, IoT devices can predict maintenance and help replace parts before the issue gets too expensive.

**Smart Pollution Control:** IoT devices and attached sensors are stationed at key city locations. They monitor pollution levels and periodically upload data to the IoT cloud. The system then processes the information to trigger public actions such as diversions or road closures.

**Smart Cities:** A smart city has better public utilities, infrastructure, services, and more. Smart meters allow utility companies to regulate energy flow efficiently, while connected vehicles make public transit tremendously efficient. In addition, smart grids are coming up to conserve resources and lower peak hour stress.

**Future technologies:**

Fast-forward to 2025, and there’ll be more than 21 billion IoT devices. The connected technology can pave the way to increase energy efficiency, minimize waste, and nurture personal autonomy. First, however, the IoT architecture needs a rich feedback mechanism and a responsive system to make it sustainable.

IoT and AI can team up to drive intelligent actions from collected data. Together, they can predict, prescribe, and deliver an adaptive response. For example, they can detect fraudulent ATM behavior, increase equipment uptime by predicting maintenance, predict driver insurance premiums based on performance, and improve overall maintenance cost.

However, any budding technology is vulnerable, and applications of IoT are no different. Malicious malware is always on the prowl to access and affect connected devices. Such attacks can disrupt services and halt critical processes for hours. Therefore, security initiatives must be sharp enough to stop distributed denial of service (DDoS) attacks.

**IoT Companies & a Circular Economy**

IoT companies are helping pave the way for a future with minimized waste, energy efficiency and greater personal autonomy. However, to be sustainable, a connected device system must be feedback rich and responsive, and actions must be connected through data. Some of the pathways to achieving a responsive and actionable system include:

- **Extending the use cycle** with predictive maintenance, instead of the “break-fix” model of manufacturing.
- **Increasing utilization** and reducing unplanned downtime.
- **Looping the asset** to reuse, remanufacture, or recycle, thanks to improved information of the condition and use history.

**IoT Security Improvements**

A challenge for businesses making a pivot to IoT is that it not only requires a full stack team of mechanical, electrical, and firmware engineers for the hardware, but also a software team to design and manage the cloud infrastructure and app developers so your users can understand the data and make their own decisions.

**Artificial Intelligence and IoT**

IoT delivers data, but it's only valuable if the data is actionable. AI helps provide context and creativity to drive intelligent actions from the collected data. There are 3 levels of utility of AI and IoT:

1. **Basic:** A prediction to forecast and mitigate risky events, using real-time data to determine when machinery and equipment will break down.
2. **Middle:** A power of prescription (vehicles can course-correct when car veers from center of the lane, railway track sensors can warn against track failures).
3. **Advanced:** Deliver adaptive or autonomous response (blood glucose sensors can alter insulin delivery levels in response to changing patient needs).

The future of IoT is looking bright, with new technologies and access to information that we may not previously have thought possible. We will soon see massive shifts in how our data is regulated and can expect better security legislation. IoT will continue to form the backbone of many technologies that will change the way we all live. This is certainly an exciting industry to be in right now!
**IoT CHALLENGES**: The major concerns related to IoT are (Rose, Eldridge, & Chapin, 2015): • Infrastructure: The availability of high end infrastructure is essential for implementing IoT. The devices and the wireless network should be reliable for actual realization. • Physical location: As the Internet of Things is strongly rooted in the physical world, the notion of physical location and position are very important, especially for finding things, but also for deriving knowledge. Therefore, the infrastructure has to support finding things according to location. • Security and Privacy: Major security concerns include identification, confidentiality, integrity, authentication and authorization. With the increase in hacking incidents, the IoT application to be developed should be reliable. • Network Issues: The widespread use of IoT depends on the wireless network it uses for communication. The networking challenges need to be addressed to enable using the technology efficiently.

**CONCLUSION**: IoT is a technology that simplifies life and will continue to do so. That said, many innovative technologies have also been disastrous at the same time. Nuclear energy can be the best example to explain it better. In the current situation, however, it is necessary to live in the standard lifestyle equipped with various modern technologies. Technological progress can be mixed, but the long-term effects must be analyzed before they are negative. The authors hope that this article would have provided a clear picture of the IoT and its details. We hope that more research in the future will lead to the IoT trend.


