INTERNET OF THINGS

Name: Manisha Gattu

Department of Computing and Informatics

Bournemouth University

Bournemouth, Great Britain

S5231338@bournemouth.ac.uk

Abstract:

The Internet of Things (IoT) has emerged as the internet's Next big thing. The network allowed by technologies such as Embedded sensing and actuating, radio frequency identification, Wireless sensor networks. Real-time and semantic web services, Etc. to collect the data, process the information and assist with decision making.

Keywords:

Internet of things, RFID, WIFI, SENSORS

INTRODUCTION:

The internet of things is an interface that supports material things or devices that are linked to the internet on a regular basis and can be associated with other devices. In his presentation to Procter and Gamba in 1999 to introduce radio frequency id, Kevin Ashtons, co-founder of the auto-id Centre at the Massachusetts institute of technology listed the internet of things[9]. This is an internet advancement, understanding the different possible domains for IoT applications is essential. The internet of things, therefore, acts as a wireless communication to several computers. Many devices may exchange information over the internet, such as smartphones, automobiles, industrial systems, cameras, health care, buildings, home appliances and many others. In artificial intelligence and machine learning, IoT can be implemented to help gather information more securely. Internet of things offers a real time organization with scenarios about how the system really operates when offering insights into anything from efficiency to supply chain and logistic operations. IoT is the acquisition and transmission of data by computers without the direct input of people. This is where the things play their role, as familiar objects are equipped with sensors, processors, and radio chips every day as well as less familiar objects, enabling them to exchange data about their operations and their environment. IoT data is collecting into databases through computing technologies including cloud computing to support IoT data applications.

IMPORTANCE OF IoT:

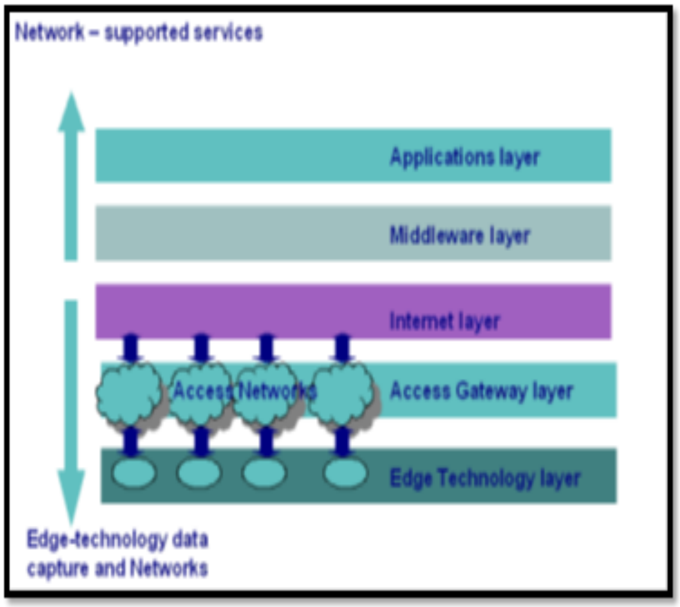
The internet of things is an emerging technology helping to shape a new era in ICT technology. From a conceptual point of view, IoT builds on three foundations, one is smart objects to be recognizable, to communicate with each other and to interact among themselves. At least one name and address are related, it is a human readable definition that can be used for interface purpose. The address is a computer-readable Data which can be used to communicate with an entity. The primary challenge ahead of us is designing technologies and solution to allow such vision. By using the internet of things, there are many advantages for companies. such as tracking their overall business, enhancing customer service, saving time and money. For example, if we choose a health sector, it depends on multiple activities and devices that can be automated and improved by various technologies, such as monitoring the compliance of patients with prescriptions and their records. It can be used in remote control systems that can be turn appliances on and off if we opt for smart living. Alarm systems and cameras to track and identify hazards are the most critical gadgets that have been developed by anyone in recent years. IoT is not just for companies or home appliances, even farmers may profit from agriculture by collecting data by adapting these types of farmers techniques to identify bugs in crops, rainfall, humidity, temperature, and soil content.

As technology progresses, more computing resources such as power, memory, processing, and battery capacity is available at reasonable low costs and with limited space requirements [1]. This allows the development of micro electronic devices that could be embedded in the environment or in everyday objects with computing capabilities. The implementation of new paradigms and technologies for communications, computing and software engineering would, in turn, entail the creation of such a new class of services[5]. All these elements are included in the IoT umbrella definition, based on the illustration of computing and communication anywhere at any time and through anything.

Day by day, the applications that use the IoT principles are emerging tremendously. These apps cover a wide range of health, security, entertainment, smart cities, protection, and many other directions that are needed. In the next few years more artifacts will also acquire the capacity to directly link to the internet. As this range of connectivity and implementation increases, our personal lives and public safety will be directly impacted by IoT. The opportunity of the framework and network with its extension becomes higher than before. Suppose if we consider a tracking system delivery timings and locations are available by using many sensors that communicate with software’s . This system needs the quality analysis process to validate the workflows and algorithms carefully.

ARCHITECTURE OF INTERNET OF THINGS:

The architecture of IoT is implemented using multiple layers stacked together, the edge technology layer is the bottom most layer and application layer is the topmost layer. This architectural approach is used in such a way to meet the business requirements originating from various industry pioneers, enterprise considerations, institutional organizations etc. The top two layers are works for data capturing while other layers is responsible for data utilization in applications.



Edge Technology Layer:

This layer contains various networks, embedded device systems, RFIDs, and readers of various other sensors. These form the primary data sources which are deployed in the environment. These hardware components may perform the following activities but not limited to the storage of identity and data, collection of raw information, processing of information, control, and actuation.

Access Gateway Layer:

This layer handles the data especially taking care of message routing and publishing. Also, it is can be used to subscribe the data and if in need it can carry out communication with other platforms as well.

Middleware Layer:

This layer operates in bidirectional mode and it is one of the most critical layers. The hardware layer and the application layer has interface between these layers.Device management and information management is responsible for dealing critical issues like data aggregation, data filtering, semantic analysis and electronic product code and object naming service.

Application layer:

Application layer is the topmost layer and is used for providing application services to targeted IoT users. These services can be utilized for various vertical sectors such as manufacturing industry, logistical industry, retail industry, climate, food and health care industry, pharmaceutical industry etc. with the rising sophistication and widespread use technology for RFID, a range of new application services are emerging under the IoT umbrella.

Challenges of IoT:

The IoT offers a host of resource for business and end-users in wide variety of applications. IoT itself lacks the philosophy, infrastructure, architecture that combines the cyber world and the real world.

1)Architecture Challenge:

By using IoT there is rapid growth in number of smart interconnected devices and sensors that ae transparent and invisible. Generally, these communications can happen anytime, and at any place by using wireless, autonomic manner.so this infrastructure solutions will compare the data from different sources and the developed features process the data and show meaningful relationships which can support decision-making.

2) Technical Challenge:

This can become a complex problem for various number of reasons there are a large number of existing architectures and different networking technologies need different environments and RFID technologies vary differently from one another. The alternative technologies may introduce problems and deployment barriers in markets, and they may also stop the users from migrating of IoT environment, which can be the most viable economic solution.

Connecting the devices to Internet using HTTP connections is not a viable solution to be implemented in IoT because of the packet size and the layers of

3) Hardware Challenge:

The main hardware challenges face in IoT is power and sensor issues that no one can do anything for that unless to change the sensors. and other challenge is that the sensors consume power even in the sleep mode and other is ultralow cost because, IoT bandwidth could vary anywhere between KBPS to multiple MBPS from sensing data and to stream the data collected.

4)Privacy Challenge:

IoT needs a significant lower cost and machine-to-machine oriented solutions to protect the privacy of communication. A key problem for IoT in terms of enabling technology is creation of effective is for recognizing smart objects and working with environmental activities. wireless sensor technologies and RFID are supposed to represent key building blocks. with several massive deployments, particularly in the materials management and logistics sectors, identification of devices using radio frequencies and their solutions can be observe as a principal communication technology. As an IoT recognition technology, Radio frequency devices plays a key role. The internet of things paradigm lies in the immense potential of incorporating computing and networking technologies into objects of common use. Two features should also be accounted.

- Identification: Every object should be recognized which needs to be uniquely defined as it belongs to a particular class. depending on specific scenarios. It can be carried out in two ways.
- The case is to tag one object physically using RFIDs, QR code. In this way, an object can be read by returning an identifier by means of an appropriate device that can be searched in a database to obtain a collection of features.
- The second possibility is to provide object with its own description it could lead to communicate its own identity and related characteristics directly if equipped with wireless means of communication.
- There are three levels of features in the internet of things can be briefly outline as follows:

  1. All communicates: Intelligent things can interact with each other wirelessly and creates extemporary interconnected objects.

  2. Everything is recognized: In digital domain things can be defined through the relationships whenever it is not possible to physical interconnection.

  3. Everything Connects: Fitness trackers such as Fitbit have been available and have recently developed into more powerful devices such as apple watch and Samsung gear fit. These usually calculate pulse rates and body temperature. For boosting fitness levels, it helps a lot.

Few scientists say that IoT progress would eventually make a person reluctant to work or use any energy. Nevertheless, depending on technology on a daily basis for assisting decisions through the insight gained from information could lead to destruction. We see technological failures that are continually happening, affecting the internet in particular.

one of the major questions to IoT in a real time world is reliability due to of the dependency on how well data is being processed, analyzed and how complex technologies are implemented to gain insights with the data gathered from the devices. Because IoT provides a platform to connect each and every device to the internet and sometimes depending upon the scenario for example, it is very simple to use IoT to turn ON/OFF an electric appliance from mobile or to control the lighting or temperature of the room using a web interface or a mobile application and in case of maintaining a enterprise level IoT eco system of devices such as real time monitoring of a data center would involve a large of devices for instance servers, network ports, routers, temperature within the data center are just a few to name and the count increases exponentially in other sectors as well. Getting an actionable result out of the data is a concern after the device is connected to internet. For automated claims processing, IoT solutions can be used as a factor in premium calculation, automated reserve setting, damage evaluation etc. The key problem facing cases of IoT use in insurance is that needs a higher degree of privacy and data governance as an industry. Insurance company barely equipped to exchange details in cases of analytical use. Traditionally the energy and power markets are known as unstructured data sectors. The main challenges of implementing IoT technologies in the energy sector would be the implementation of the right hardware, the acquisition and management of enormous data, pre-processing and useful.

Since IoT has become a vital component, the increased use of internet needs to address security and trust adequately. Here are some benefits and drawbacks, then.

- On every computer, there is a capacity to collect and access information from anywhere at any time.
- Improving contact between each electronic device linked to it.
- Automating activities helps to enhance the service of the organization and reduce the need for human interaction.

SECURITY:

Security is main issue in these days for all the aspects of internet for commercial and personal level. Without assurances about security level confidentiality and privacy the organizations are unlikely to implement the IoT solutions for large scale industries. Connecting devices provides a great experience for customers but also act for new targets for hackers. and the most challenges in other current rising technology blockchain in IoT scalability problems pertaining to the scope of ledgers in blockchain that could lead to centralization as it changed over time and needed some record management that shows over the future of block chain technology. RFID has been developed for security systems in IoT implementations. Many IoT devices are equipped with a standard initial password that is generic to the vendors. Users often leave the password unchanged if these devices are hooked up with an established ecosystem. These activities make malware and other malicious software vulnerable to the entire system.

Effects of IoT Security breach:

1.Losing sensitive information

2.Business Disruption

3.Manipulationg information

* Losing sensitive information: In sectors like medical, insurance, banking etc., IoT devices are integrated. Compromising such systems may lead to the block hackers the medical records, banking or financial details of the client. For example if we take a bank and the customer are main victims for fraud transactions i.e., for losing amount in their accounts without their knowledge and that can’t be reversed.

* Business Disruption: Hackers can gain backdoor access to the entire business servers due to the liable of any node of the IoT ecosystem. Any organization is now almost digitized, thanks to the dot net revolution. Partially compromised nodes can also lead to the entire business process being disrupted.

* Manipulating information: Hackers can manipulate data that can be led to long term consequences. In a medical use case, assume that if the application obtained by back door changes health records, the

activities have also changed. Currently every IoT use cases are combined with computing techniques.

CONCLUSION:

IoT is looking forward to be a key communication technology for developing new applications and providing new services. Currently IoT is being used in different technology domains for smart applications especially home automation and smart city applications. Many organizations tend to explore new possibilities to enable IoT in their respective business eco system. The upcoming technologies are considerate of this and even the advancements in technology are willing to accommodate IoT to further enable the end users to benefit by combining the technologies . For example, 5G is expected to be a keen communication technology which is expected to enrich IoT capability.

References:

[1] 10 Biggest security challenges for IoT", *Peerbits*, 2020. [Online]. Available: https://www.peerbits.com/blog/biggest-iot-security-challenges.html.

[2] A Brief History of the Internet of Things - DATAVERSITY", *DATAVERSITY*, 2020. [Online]. Available: https://www.dataversity.net/brief-history-internet-things/#.

[3] [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[4]Available:https://www.researchgate.net/publication/340133268_Internet_of_Things_Architecture_Challenges_and_Future_Directions. [Accessed: 17- Dec- 2020].

[5][Online].Available: https://www.scirp.org/html/56616_56616.htm.

[6] Guest Editorial - Special Issue on Internet of Things (IoT): Architecture, Protocols and Services - IEEE Journals & Magazine", *Ieeexplore.ieee.org*, 2020. [Online].

Available: https://ieeexplore.ieee.org/abstract/document/6583964.

[7] IoT and Blockchain: Challenges and Risks", *Datafloq.com*, 2020. [Online]. Available: https://datafloq.com/read/iot-and-blockchain-challenges

[8] IoT, "Challenges of IoT | Cases and Common Challenges Industry Wise In IoT", *EDUCBA*, 2020. [Online]. Available: https://www.educba.com/challenges-of-iot/.

[9] Licite-Kurbe and A. Chandra Mohan, "Characteristics and Challenges of the Internet of Things in Entrepreneurship", 2020.

[10] ScienceDirect.com | Science, health and medical journals, full text articles and books.", *Sciencedirect.com*, 2020. [Online].

Available: https://www.sciencedirect.com/.