

# An Overview of Recent Trends in IoT

**Kuljeet Kaur<sup>1</sup>, Kiran Mehta<sup>2</sup>**

ME Student, Department of Computer Science & Engineering, PEC University of Technology, Chandigarh, India <sup>1,2</sup>

**Abstract:** The necessity of getting data from every real world entity with the help of embedded sensors, communicating network and remote management resulted in the emergence of Internet of Things, acronymed as IoT. The term IoT, coined by IBM differs from IoE(Internet of Everything) in terms of advancement and interoperable technologies. IoT deals with a network of similar devices such as those of smart phones whereas IoE constitutes network of all smart devices like smart TV, smart AC, smart phone etc. Just like humans, any device with a sensor or machine can communicate in the network with the help of Internet. Thus, huge data gets generated in fraction of seconds, which can be stored and processed in cloud to generate meaningful patterns. In this paper, various aspects of IoT have been covered which provides insights into the future of Information Technology.

**Keywords:** Big data, PaaS, Internet, smart devices, IoE.

## I. INTRODUCTION

The strength of Internet lies in the trio of A's, i.e., Always, Anywhere and Anytime. With the advancement of communicating protocols, data has been emphasized to be collected with the help of Internet. The concept of data collection has been focused since centuries in the form of Data Acquisition (DAQ), Supervisory Control and Data Acquisition (SCADA), Machine to Machine (M2M) and now the future is Internet of Things (IoT). Before the era of DAQ, engineers used to collect data manually for huge machines after visiting the site or field. To automate this, DAQ came into existence and the automatically collected data was processed into signals to generate results in digital form, in order to use it on any computer. But, due to the absence of communication protocols like Infrared, Bluetooth, Wi-Fi, Internet etc., DAQ couldn't cover a network of devices. In the nutshell, DAQ is a static mono-device data collector. With the development of technologies, backup frames were used to communicate with each other [8].

In the next generation, real-time data was occupied with SCADA, in which all nodes were connected to form a network and on meeting the requirement, a predefined action was taken by a supervisory station. In fewer words, SCADA lacks the usage of database. To overcome the shortcomings of SCADA, communication technologies were used between remote machines to form M2M. Moreover, database usage started aptly for performing analytics to draw patterns and trends. The concept of utilizing the incoming real-time data as well as collected data of the past in order, popularized the framework to a huge extent. The usage of M2M for storing data and analysing generated report is utilized in crucial environments like Nuclear Power Plants, X-ray machines to detect the misbehaviour of the infrastructure in order to take timely actions.

The next phase of "Data Management" is Internet of Things (IoT). IoT is a combination of collection of data, analysis and smart actions. IoT may be defined as the concept in which smart devices are attached to living or

non-living objects to stream and process useful data for further analysis.

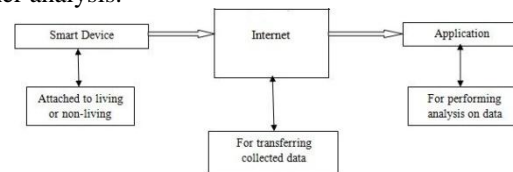


Fig1. Architecture of IoT

The Fig. 1 shows the architecture of IoT. The prerequisite for the working of IoT are sensors embedded in the form of smart device.

The smart device must fulfil all the three conditions described below:

1. It must sense some data.
2. It must automatically connect to the Internet if embedded in the mobile object. For instance, if a moving animal with a sensor enters into a neighbouring network it must connect to it.
3. It must exclusively access targeted data in an unbiased manner. For instance, if a sensor is supposed to measure moisture in the soil, it must not get affected by the variations in the temperature.

In the nutshell, under the roof of IoT, not only computers are connected but anything can be connected from humans to houses. Since every object in IoT is supposed to send data, the requirement of IPv6 raised.

The data from each device forms a huge pile of unstructured content which can't be analysed manually.

This led to the invention of "big data"[10] to draw some useful patterns. As maintaining the infrastructure and the huge data is a cumbersome task, so here came the concept of "cloud". In short, we can say that every new technology is so linked to the IoT that it may also be called as "Cloud of Things". Fig. 2 shows the IoT model with respect to big data.

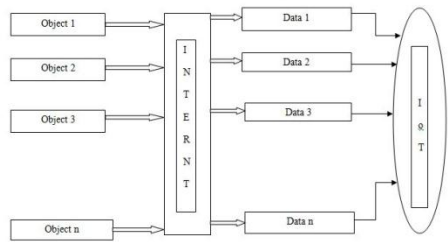


Fig2. IoT architecture with respect to big data

Some of the benefits of IoT are highlighted as follows:

1. Infrastructure at Home:
  - a) Refrigerators will inform about the stale food.
  - b) Containers will alarm if stuff is almost running out.
  - c) Sprinklers will stop either if rain is predicted or lawn doesn't need more water.
  - d) Bed or Sofa can alarm for inappropriate posture.
  - e) Streamlined images of CCTV cameras will inform about everything like if fire, geyser is on.
  - f) Wrist band will inform the doctor if something goes wrong with the body.
  - g) Toaster will toast automatically when you are home.
2. Infrastructure for Society:
  - a) Street lights will switch on if thunderstorm is there.
  - b) Tsunami warnings can be used for counter-measures at power stations, hospitals etc.
  - c) Railway tracks and bridges will inform if something goes wrong with the infrastructure.
  - d) If demand increases, supply will get increased by the manufacturing machines.
  - e) Smart grids and meters will help in energy conservation.
  - f) Smart Parking.
  - g) Smart Toll will automatically deduct money from the bank account.
  - h) Elevators will stop and buses will not stop if no person around.
  - i) Driverless cars will rule the world.
  - j) Animals will be easy to locate.

As IoT is getting more popular, once it becomes ubiquitous no privacy will be there due to continuous tracking of the person or object. Moreover, completely relying on IoT can bring the life to standstill and havoc if a malware destroys a file. For providing a more secure life, privacy is being compromised. Some of the disadvantages are listed below:

- a) The smart car will log journey, driving speed and style which can be misused.
- b) The toothbrush will inform the dentist if you forget before going to bed.
- c) The refrigerator will tell how much and what are you consuming. This type of data can be misused to manipulate the food-supply chain.
- d) Virus can start the car by attacking the chips.
- e) Environment will be affected if improper disposal of chips.
- f) The companies can also hack your systems to know your habits.

## II. IOT AND CLOUD COMPUTING

The current trend for efficiently processing and managing the sensed data is IoT and cloud computing working together. Cloud computing and IoT are tightly coupled with each other [1]. The large amounts of data produced by things (sensors) needs to be stored, processed and accessed. This is where role of cloud computing comes in. IaaS aspect of cloud is used for storing the big data produced from things in cloud hosted storage. The processing of this data is also facilitated by cloud computing. Firstly, the data is transformed into observations and then using those observations some productive actions are taken, in a cost effective manner [9]. Cloud computing provides analytical tools, monitoring devices, visualization platforms and client delivery. It complements IoT by making it an on-demand self service, providing a lot of connectivity options like mobile devices, laptops and tablets. Resource pooling, i.e., sharing of a resource among the users who know the resource address, another important feature of cloud is available for IoT. Majority of the IoT platforms nowadays are cloud based, as explained in the next section.

## III. PLATFORMS FOR IOT

An IoT platform is a set of functionalities that can be used to build, run and access IoT applications. Generally, an IoT platform exists virtually somewhere on the Internet, lives in the cloud. It is data driven and is connected, i.e., provides a link among devices and also, between devices and the Internet. An ideal platform would be the one that is cost effective, consumes less power, provides long battery and facilitates easy development of applications. An ideal IoT platform is expected to include an API for application development, data storage functionalities, a mechanism to perform analytical tasks and an authentication mechanism to ensure security of the data. There are a plenty of IoT platforms available today [3], [4], [5], [6], [7]. The table below lists some of those platforms with their features.

TABLE1. Some popular IoT platforms with their features

Name of IoT platform	Features
Axeda	<ul style="list-style-type: none"> <li>• Cloud based</li> <li>• M2M</li> <li>• provides web services like SOAP and RESTful for application development</li> <li>• provides a Groovy SDK to support application development</li> <li>• includes a dashboard containing widgets to ease the visualization of data</li> </ul>
Ericsson IoT framework	<ul style="list-style-type: none"> <li>• a PaaS that collects sensor data from IP networks</li> <li>• focuses on the analytics and mashing up of data</li> <li>• RESTful API</li> </ul>

	<ul style="list-style-type: none"> <li>• OpenId access control for the data.</li> <li>• Has pub/sub mechanism to perform analytical tasks</li> </ul>
Xively	<ul style="list-style-type: none"> <li>• Cloud based</li> <li>• Supports JSON, XML, CSV formats</li> <li>• RESTful API</li> <li>• Search mechanism to retrieve feeds based on characteristics like location, type of data stored</li> <li>• Data ownership is with user</li> </ul>
ThingSpeak	<ul style="list-style-type: none"> <li>• Decentralized, open source</li> <li>• provides a server that may be used to store and retrieve IoT data</li> <li>• support the JSON, XML, CSV data formats</li> <li>• provides visualization tools and enables the creation of widgets in Javascript/HTML/CSS to visualize the data in a more personified fashion</li> </ul>
EvryThng	<ul style="list-style-type: none"> <li>• centralized platform (SaaS)</li> <li>• provides a persistent presence on the Web of identifiable objects (RFID, NFC, connected objects, etc.)</li> <li>• RESTful API to store and retrieve metadata as well as real-time data</li> <li>• allows fine-access grained control to easy sharing of products information</li> <li>• No search tools are available to find data feeds</li> <li>• Billing is done on-demand</li> </ul>

#### IV. PRIVACY ISSUES IN IOT

Privacy is the most sensitive issue related to IoT. Various approaches are being developed to protect the personal information of IoT users. One possible scenario can be limiting access to the users, i.e., a random value will be retrieved by an unauthorized RFID reader, so it will not be able to track the user. There are also some protocols and cryptographic mechanisms that strive to protect data throughout the life cycle of a service, but due to interoperability issues, some entities lack the resources to control such mechanisms. Another important aspect is transparency. Users must know the entities managing their data and how.

#### V. SECURITY ISSUES IN IOT

Despite the immense success of IoT in the various domains, the whole communication infrastructure of the IoT is flawed from the security point of view. There is a

need to ensure security throughout the data flow within the IoT. Security at both the device and network levels is critical to the operation of IoT. Some of the challenges affecting the entire developing IoT system arise due to security issues present in the communication technology used for information transmission from one device to another in IoT.

1. Attacks on authentication and secrecy
2. Attacks on service integrity
3. Attacks on network availability (DoS attacks)

These issues can be more or less dealt with using the mechanisms [2] like access control, device authentication, firewalling, etc. But the ultimate solution will be standardization and certification.

#### VI. CONCLUSION

Despite its security and privacy issues, IoT is going to be a major part of society in coming years. Its successful implementation in various areas like smart cities, smart homes have already made lives simpler and comfortable. Being cloud based, its full time availability, flexibility, efficient computations makes it easily accessible and popular amongst users. Just like cloud, it has its shortcomings with respect to privacy of users' data, which must be worked upon. Conclusively, we can say that IoT will provide a treasure of luxuries at the cost of privacy.

#### REFERENCES

- [1]. The cloud is the secret weapon in the Internet of things, 2014. [<http://www.infoworld.com/article/2608029/cloud-computing/the-cloud-is-the-secret-weapon-in-the-internet-of-things.html>] Accessed on May 28, 2015
- [2]. Security in the internet of things, a white paper by WIND River Systems, January 2015.
- [3]. Axeda Machine cloud. URL [<http://www.axeda.com/>] Accessed on May 28, 2015
- [4]. ThingSpeak, the open data platform for the Internet of Things. [<https://thingspeak.com/>] Accessed on May 28, 2015
- [5]. EvryThng [<http://evrythng.net/>] Accessed on May 28, 2015
- [6]. Xively, Building the next big thing for the IoT. [<http://xively.com/>] Accessed on May 28, 2015
- [7]. Ericsson IoT framework, a computational engine for the Internet of Things. [<https://github.com/EricssonResearch/iot-framework-engine>] Accessed on May 28, 2015
- [8]. Hitesh Rohilla, enCypher Technologies [<http://blog.encypher.in>] Accessed on May 17, 2015
- [9]. Cloud Computing & The Internet of Things go Hand in Hand [<http://siliconangle.com/blog/2013/07/17/cloud-computing-the-internet-of-things-go-hand-in-hand/>] Accessed on May 28, 2015
- [10]. Why Big Data And The Internet of Things Are A Perfect Match, Datamation [<http://www.datamation.com/applications/why-big-data-and-the-internet-of-things-are-a-perfect-match.html>] Accessed on May 28, 2015.

#### BIOGRAPHIES



**Kuljeet Kaur** (19-02-1990) was born in Patiala, Punjab. She has done her graduation in Computer Science and Engineering from Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab in the year 2012. Currently,



she is pursuing masters in Information Security from PEC University of Technology, Chandigarh. She has attended expert lectures on Big Data, Advanced Persistent Threats, FireEye's Threat Profiling Lecture, Haxpresso 1.0, and Nanotechnology in Engineering. She is doing her research in Social Computing.



**Kiran Mehta** (05-09-1990) was born in Sirsa, Haryana. She did her graduation in Computer Engineering from Jannayak Chaudhary Devilal Memorial College of Engineering, Sirsa, Haryana in the year 2011. Currently, she is pursuing post graduation in Computer Science and Engineering from PEC University of Technology, Chandigarh. She is currently working on Behavioral study of a terrorist group using machine learning techniques.