**Capability Discovery**

**Complex Event Processing (Cep)**

**Protocol Interoperability**

**Non-Functional Properties**

1. Future Internet: The Internet of Things Architecture,Possible Applications and Key Challenges

1) Naming and Identity Management: The IoT will connect billions of objects to provide innovative services. ach object/sensor needs to have a unique identity over the Internet. Thus, an efficient naming and identity anagement system is required that can dynamically assign and manage unique identity for such a large number of bjects.

2) Interoperability and Standardization: Many manufacturers provide devices using their own technologies and services that may not be accessible by others. The standardization of IoT is very important to provide better interoperability for all objects and sensor devices.

3) Information Privacy: The IoT uses different kind of object identification technologies e.g., RFID, 2D-barcodes etc. Since, every kind of daily use objects will carry these identification tags and embed the object specific information, it is necessary to take proper privacy measures and prevent unauthorized access.

4) Objects safety and security: The IoT consists of a very large number of perception objects that spread over some geographic area, it is necessary to prevent the intruder’s access to the objects that may cause physical damage to them or may change their operation.

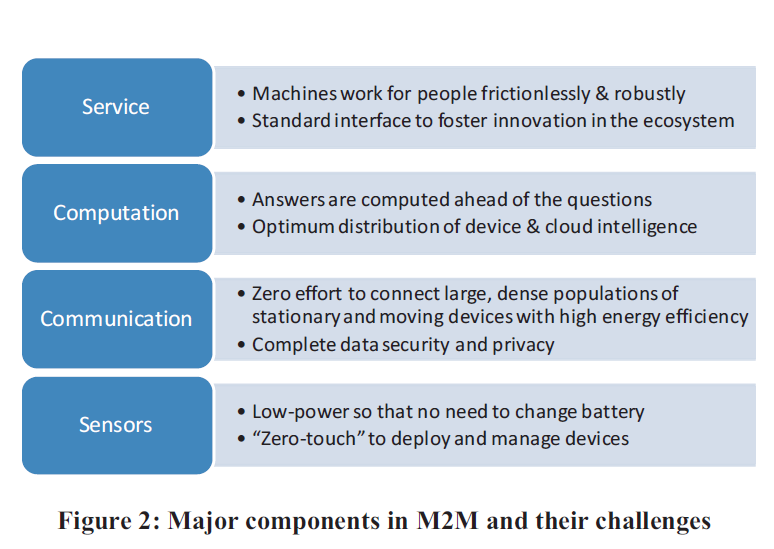
5) Data confidentiality and encryption: The sensor devices perform independent sensing or measurements and transfer data to the information processing unit over the transmission system. It is necessary that the sensor devices should have proper encryption mechanism to guarantee the data integrity at the information processing unit. The IoT service determines who can see the data, thus, it is necessary to guard the data from externals.

6) Network security: The data from sensor devices is sent over wired or wireless transmission network. The transmission system should be able to handle data from large number of sensor devices without causing any data loss due to network congestion, ensure proper security measures for the transmitted data and prevent it from external interference or monitoring.

7) Spectrum: The sensor devices will require dedicated spectrum to transmit data over the wireless medium. Due to limited spectrum availability, an efficient dynamic cognitive spectrum allocation mechanism is required to allow billions of sensors to communicate over the wireless medium.

8) Greening of IoT: The network energy consumption is increasing at very high rate due to increase in data rates, increase in the number of Internet-enabled services and rapid growth of Internet connected edge-devices. The future IoT will cause significant increase in the network energy consumption. Thus, green technologies need to be adopted to make the network devices as energy efficient as possible.

1. A survey of Internet-of-Things: Future Vision,Architecture, Challenges and Services
2. Communication Mechanism- 6lowpan Challenges
3. Data Fusion Mechanism and challenges
4. A SURVEY ON THE IETF PROTOCOL SUITE FOR THE INTERNET OF THINGS : STANDARDS, CHALLENGES, AND OPPORTUNITIES (pour la problème de thèse est intéressant aussi ) .
5. Convergent networks
6. Hybrid communication paradigm
7. Joint data processing and networking
8. Social and economic awareness
9. An analysis of M2M platforms: challenges and opportunities for the Internet of Things
10. Challenges and Opportunities of Internet of Things



1. Challenges in Middleware Solutions for the Internet of Things
2. Interoperability The IoT represents a huge interoperability challenge for middleware approaches since heterogeneous devices are expected to collaborate together in communication and information exchange. This challenge increases the research effort to design a middleware that can cover a large number of different types of devices, and even new types of devices that may be discovered in the future. The approach proposed in [8] assumes an IEEE 1451compilant sensor device, in which a significant drawback is raised because not all sensors can integrate that approach. In contrast, the semantic web approaches such as [9] overcome this challenge, since interoperability is a significant advantage of the semantic web technology.
3. Scalability

Since the IoT is expected to support a large number of devices, scalability seems to be one of the major challenges faced by the middleware approaches. This is the result of having thousands of devices that will interact, but fortunately, almost in one place. A reliable IoT middleware is required to effectively manage scalability issues so that the basic functions will operate efficiently in small-scale and largescale environments [10]. In [9], scalability is one of the proposed approach drawbacks, while in [8], scalability support is an advantage.

1. Abstraction Provision

An ideal middleware for an intelligent environment such as the IoT should provide abstractions at various levels such as heterogeneous input and output hardware devices, hardware and software interfaces, data streams, hysicality and the development process.

1. Spontaneous Interaction

In the IoT, spontaneous events are generated due to the sudden interactions that are caused by the movement of

things, where new objects are coming into the wireless range of other objects [10]. In this context, middleware is required to manage events in an “arrive and operate” [11] fashion.

E. Unfixed Infrastructure

Unlike the traditional distributed environment, where resources are managed by a certain server, each device in the IoT should be capable of announcing its existence and the resources it provides without requiring a fixed infrastructure [10]. Using a dedicated server for resource management does not hold in the IoT, because of the high distribution and mobility of devices. In this context, a middleware for the IoT should provide automatic discovery of devices in addition to management of resources over different types of services.

F. Multiplicity

Two major multiplicity challenges should be taken into the consideration of the IoT middleware design. First, devices in the IoT are often required to communicate with other devices simultaneously [10]. Second, a device that is participating in an IoT environment is required to select the most suitable services from a massive set of services, because such devices will often rely on services that are available at other nearby devices. In addition, they should deal with the results returned from different services, which may contradict with each other.

G. Security and Privacy

Automatic communication of real-life objects represents a huge challenge in terms of trust, security and privacy.

H. Embedded RFID tags in the personal devices, groceries and even in our clothes can be triggered to respond with their ID and other information. This type of surveillance would affect many parts of our everyday life. The management support of security and privacy has to be considered as a main function of the middleware for the IoT [1]. In SOA-based approaches, for example, the functions related to security and privacy can be either built on a single layer or distributed among all other layers. In the latter case, other issues have to be considered, so as not to affect the system’s performance or introduce excessive overhead.

1. Data Management for Internet of Things: Challenges, Approaches and Opportunities
2. *Data Cleaning Layer*
3. *Event Processing Layer*
4. *Data Storage and Analysis Layer*
5. *Middleware for IoT Data Management*
6. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions
7. *Architecture*
8. *Energy efficient sensing*
9. *Secure reprogrammable networks and Privacy*
10. *Quality of Service*
11. *New protocols*
12. *Participatory Sensing*
13. *Data mining*
14. *GIS based visualization*
15. *Cloud Computing*
16. *International Activities*
17. Internet of Things: Challenges and Opportunities

S. C. Mukhopadhyay and N. K. Suryadevara

A Availability of internet at everywhere and at no cost

• Security issues

• Low-cost smart sensing system development

• Energy

• Computational ability

• Scalability

• Fault Tolerance

• Power Consumption

• Acceptability among the society

1. Internet of Things in Industries: A Survey
2. Technical Challenges ( je le vois intérésant pour moi à relire )
3. Standardization
4. Information Security and Privacy Protection
5. Research Trends
6. Internet of Things: Objectives and Scienti¯c Challenges

Data exchange among large-scale heterogeneous network elements.

E®ective integration and interaction adaptation of uncertain information*.*

Service adaptation in the dynamic system environment.

1. The Internet of Things (IoT): Applications, investments, and challenges for enterprises

Challenges in IoT development

6.1. Data management challenge

6.2. Data mining challenge

6.3. Privacy challenge

6.4. Security challenge

6.5. Chaos challenge