Internet of Things
Unit 4

-Madhavi Dave

Data Management

Introduction

- Data management is a crucial aspect in the Internet of Things.
- When considering a world of objects interconnected and constantly exchanging all types of information, the volume of the generated data and the processes involved in the handling of those data become critical.
- Sales in M2M could rise by as much as a factor of ten over the next five years(more than 90 million) and thus the data management.

- There are many technologies and factors involved in the “data management” within the IoT context.
- Some of the most relevant concepts which enable us to understand the challenges and opportunities of data management are:
    - Data Collection and Analysis
    - Big Data
    - Semantic Sensor Networking
    - Virtual Sensors
    - Complex Event Processing.

Data Collection and Analysis (DCA)

- Data Collection and Analysis modules or capabilities are the essential components of any IoT platform or system.
- The DCA module is part of the core layer of any IoT platform. Some of the main functions of a DCA module are:
  - **User/customer data storing**
  - **User data & operation modeling**
  - **On demand data access**
  - **Device event publish/subscribe/forwarding/notification:**

- **Customer rules/filtering**
- **Customer task automation**
- **Customer workflows**
- **Multitenant structure**
  - **Multi-protocol**
  - **De-centralisation**
  - **Security**
  - **Data mining features**

Big Data

- Big data is about the processing and analysis of large data repositories, so disproportionately large that it is impossible to treat them with the conventional tools of analytical databases.
- The IoT devices generate data a lot faster than people can, and their production rates will grow exponentially with Moore’s Law.
- Storing this data is cheap, and it can be

- Web logs;
- RFID;
- Sensor networks;
- Social networks;
- Social data (due to the Social data revolution);
- Internet text and documents;
- Internet search indexing;
- Call detail records;
- Astronomy, atmospheric science, genomics, biogeochemical, biological, and other complex and/or interdisciplinary scientific research;
- Military surveillance;
- Medical records;
- Photography archives;
- Video archives;
- Large scale e-commerce.

- Big data requires exceptional technologies to efficiently process large quantities of data within a tolerable amount of time.
- Technologies being applied to big data include massively parallel processing (MPP) databases, data-mining grids, distributed file systems, distributed databases, cloud computing platforms, the Internet, and scalable storage systems.
- These technologies are linked with many aspects derived from the analysis of natural phenomena such as climate and seismic data to environments such as health, safety or, of course, the business environment.

- The biggest challenge of the Petabyte Age will not be storing all that data, it will be figuring out how to make sense of it.
- Big data deals with unconventional, unstructured databases, which can reach petabytes, exabytes or zettabytes, and require specific treatments for their needs, either in terms of storage or processing/display

- Companies focused on the big data topic, such as Google, Yahoo, Facebook; they opt instead for an approach based on distributed, cloud and open source systems.
- Hadoop, an Open Source framework in this field that allows applications to work with huge repositories of data and thousands of nodes.
- These have been inspired by Google tools such as the MapReduce and Google File system, or NoSQL systems, which in many cases do not comply with the ACID (atomicity, consistency, isolation, durability) characteristics of conventional databases.

- In future, it is expected a huge increase in adoption, and many, many questions that must be addressed.
  - **Privacy**. Big data systems must avoid any suggestion that users and citizens in general perceive that their privacy is being invaded.
  - Integration of both relational and NoSQL systems.
  - More efficient indexing, search and processing algorithms, allowing the extraction of results in reduced time and, ideally, near to “real time” scenarios.
  - **Optimised storage of data**. Given the amount of information that the new IoT world may generate, it is essential to avoid that the storage requirements and costs increase exponentially

Semantic Sensor Networks and Semantic Annotation of Data

- The Semantic Sensor Web (SSW) proposes annotating sensor data with spatial, temporal, and thematic semantic metadata.
- Associating sensor and sensor network data with other concepts and reasoning makes the data information widely available for different applications, front-end services and data consumers.
- The semantic description allow machines to interpret links and relations between the different attributes of a sensor description and also other data existing on the Web or provided by other applications and resources.

Virtual Sensors

- A virtual sensor can be considered as a product of spatial, temporal and/or thematic transformation of raw or other virtual sensor producing data with necessary provenance information attached to this transformation.
- Virtual sensors and actuators are a programming abstraction simplifying the development of decentralized WSN applications

Complex Event Processing

- Complex event processing (CEP) is an emerging network technology that creates actionable, situational knowledge from distributed message-based systems, databases and applications in real time or near real time.
- CEP can provide an organization with the capability to define, manage and predict events, situations, exceptional conditions, opportunities and threats in

Security, Privacy & Trust

- There are a number of specific security, privacy and trust challenges in the IoT, they all share a number of transverse non-functional requirements:
  - Lightweight and symmetric solutions, Support for resource constrained devices
  - Scalable to billions of devices/transactions
- Solutions will need to address federation/ administrative co-operation
  - Heterogeneity and multiplicity of devices and platforms
  - Intuitively usable solutions, seamlessly integrated into the real world

Trust for IoT

- There is a need for a trust framework to enable the users of the system to have confidence that the information and services being exchanged can indeed be relied upon.
- The trust framework needs to be able to deal with humans and machines as users.
- The development of trust frameworks that address this requirement will require advances in areas such as:

- Lightweight Public Key Infrastructures (PKI) as a basis for trust management.
- Lightweight key management systems to enable trust relationships to be established and the distribution of encryption materials using minimum communications and processing resources.
- Quality of Information is a requirement for many IoT-based systems.

- Decentralized and self-configuring systems as alternatives to PKI for establishing trust.
- Novel methods for assessing trust in people, devices and data, beyond reputation systems.
- Assurance methods for trusted platforms including hardware, software, protocols, etc.
- Access Control to prevent data

Security for IoT

- As the IoT becomes a key element of the Future Internet and a critical national/international infrastructure, the need to provide adequate security for the IoT infrastructure becomes ever more important.
- Advances are required in several areas to make the IoT secure from those with malicious intent, including:

- DoS attacks are already well understood for the current Internet, but the IoT is also susceptible to such attacks and will require specific techniques and mechanisms.
- General attack detection and recovery/resilience to cope with IoT specific threats, such as compromised nodes, malicious code hacking attacks.
- Cyber situation awareness tools/techniques will need to be developed to enable IoT-based infrastructures to be monitored.

- The IoT requires a variety of access control and associated accounting schemes to support the various authorization and usage models that are required by users.
- The IoT needs to handle virtually all modes of operation by itself without relying on human control.

Privacy for IoT

- As much of the information in an IoT system may be personal data, there is a requirement to support anonymity and restrictive handling of personal information.
- There are a number of areas where advances are required:
- Cryptographic techniques that enable protected data to be stored processed and shared, without the information content being accessible to other parties.

- Techniques to support Privacy by Design concepts, including data minimisation, identification, authentication and anonymity.
- Fine-grain and self-configuring access control mechanism emulating the real world.
- There are a number of privacy implications arising from IoT devices where further research is required, including

- Preserving location privacy, where location can be inferred from things associated with people.
- Prevention of personal information inference, that individuals would wish to keep private, through the observation of IoT-related exchanges.
- Keeping information as local as possible using decentralized computing and key management.
- Use of soft identities, where the real identity of the user can be used to generate various soft identities for specific applications

IoT Related Standardizations

- Standards are needed for interoperability both within and between domains.
- Within a domain, standards can provide cost efficient realizations of solutions, and a domain here can mean even a specific organization or enterprise realizing an IoT.
- Between domains, the interoperability ensures cooperation between the engaged domains, and is more oriented towards Internet of Things applications.

- Significant attention is given to the “pre-selection” of standards through collaborative research, but focus should also be given to regulation, legislation, interoperability and certification as other activities in the same life-cycle.
- It would be beneficial to develop a wider approach to standardization and include anticipation of emerging or on-going policy making in target application areas.

- The standardisation bodies are addressing the issue of interoperable protocol stacks and open standards for the IoT.
- This includes as well expending the HTTP, TCP, IP stack to the IoT-specific protocol stack.
- This is quitechallenging considering the different wireless protocols like ZigBee, RFID,Bluetooth, BACnet 802.15.4e, 6LoWPAN, RPL, and CoAP.

- Agreed standards do not necessarily mean that the objective of interoperability is achieved.
- The mobile communications industry has been successful not only because of its global standards, but also because interoperability can be assured via the certification of mobile devices and organizations.

Current Situation

- The current M2M related standards and technologies landscape is highly fragmented.
- The fragmentation can be seen across different applied domains where there is very little or no re-use of technologies beyond basic communications or networking standards.
- Even within a particular applied sector, a number of competing standards and technologies are used and promoted.

Interoperability in the Internet of Things

- The Internet of Things is shaping the evolution of the future Internet.
- After connecting people anytime and everywhere, the next step is to interconnect heterogeneous things/machines/smart objects both between themselves and with the Internet.
- As for the IoT, future networks will continue to be heterogeneous, multi-vendors, multi-services and largely distributed.
- Consequently, the risk of non-interoperability will increase. This may lead to unavailability of some services for end-users.

- The framework for sustainable interoperability in Internet of Things applications needs (at least) to address the following aspects:
- Management of Interoperability in the IoT
- Dynamic Interoperability Technologies for the IoT
- Measurement of Interoperability in the IoT
- Interaction and integration of IoT in

Device Level Energy Issues

- Challenges in IoT is how to interconnect “things” in an interoperable way while taking into account the energy constraints, knowing that the communication is the most energy consuming task on devices

Low Power Communication

- **IEEE 802.15.4** has developed a low-cost, low-power consumption, low complexity, low to medium range communication standard at the link and the physical layers
- **Bluetooth lowenergy** (BLE) is the ultra-lowpower version of the Bluetooth that is up to 15 times more efficient than Bluetooth.
- **Ultra-Wide Bandwidth (UWB) Technology** is an emerging technology in the IoT domain that transmits signals across a much larger frequency range than conventional systems

- **RFID/NFC** proposes a variety of standards to offer contact less solutions.
- Cable-powered devices are not expected to be a viable option for IoT devices as they are difficult and costly to deploy.
- Battery replacements in devices are either impractical or very costly in many IoT deployment scenarios.
- As a consequence, for large scale and autonomous IoT, alternative energy sourcing using ambient energy should be considered.

Energy Harvesting

- Four main ambient energy sources are present in our environment: mechanical energy, thermal energy, radiant energy and chemical energy.
- Energy harvesting (EH) must be chosen according to the local environment.
- For outside or luminous indoor environments, solar energy harvesting is the most appropriate solution.
- In a closed environment thermal or mechanical energy may be a better alternative.

IoT Related Standardisation

- Standards are needed for interoperability both within and between domains.
- Within a domain, standards can provide cost efficient realizations of solutions, and a domain here can mean even a specific organization or enterprise realizing an IoT.
- Between domains, the interoperability ensures cooperation between the engaged domains, and is more oriented towards Internet of Things applications.

- A complexity with IoT comes from the fact that IoT intends to support a number of different applications covering a wide array of disciplines
- Policy making can have a direct requirement for supporting IoT standards to be developed.
- It would therefore be beneficial to develop a wider approach to standardization

- The standardization bodies are addressing the issue of interoperable protocol stacks and open standards for the IoT.
- This includes as well expending the HTTP, TCP, IP stack to the IoT-specific protocol stack.
- Agreed standards do not necessarily mean that the objective of interoperability is achieved.

- From the point of view of standardisation IoT is a global concept, and is based on the idea that anything can be connected at any time from any place to any network, by preserving the security, privacy and safety.
- Interoperability is a key challenge in the realms of the Internet of Things.
- This is due to the intrinsic fabric of the IoT as: (i) *high–dimensional*, (ii) *highly-heterogeneous,* (iii) *dynamic and non-linear*, (iv) *hard to describe/model.*