UNIT IV –IOT PRIVACY, SECURITY AND GOVERNANCE

Introduction, Overview of Governance, Privacy and Security Issues, Contribution from FP7 Projects, Security, Privacy and Trust in IoT-Data-Platforms for Smart Cities, First Steps Towards a Secure Platform, Smartie Approach. Data Aggregation for the IoT in Smart Cities, Security.

SECURITY, PRIVACY AND TRUST IN IOT

The Internet of Things presents security-related challenges that are identified in the IERC 2010 Strategic Research and Innovation Roadmap but some elaboration is useful as there are further aspects that need to be addressed by the research community. While 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

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. IoT applications use sensors and actuators embedded in the environment and they collect large volumes of data on room temperatures, humidity, and lighting to optimize energy consumption and avoid operational failures

that have a real impact on the environment. In the retail industry, a refrigerator failing to maintain proper cooling temperatures could place high value medical or food inventory at risk. Having all of these devices connected, it is as well needed have the right data model. The data model has to accommodate high data rate sensor data and to assimilate and analyse the information. In this context database read/write performance is critical, particularly with high data rate sensor data. The database must support high-speed read and writes, be continuously available (100% of the time) to gather this data at uniform intervals and be scalable in order to maintain a cost-effective horizontal data store over time.

Large-scale applications and services based on the IoT are increasingly vulnerable to disruption from attack or information theft. Advances are required in several areas to make the IoT secure from those with malicious intent, including.

- DoS/DDOS 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 to ensure that transport, energy, city infrastructures cannot be disabled or subverted.
- 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. Advances are required to enable operators to adapt the protection of the IoT during the lifecycle of the system and assist operators to take the most appropriate protective action during attacks.
- 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 heterogeneity and diversity of the devices/gateways that require access control will require new lightweight schemes to be developed.
- The IoT needs to handle virtually all modes of operation by itself without relying on human control. New techniques and approaches e.g. from machine learning, are required to lead to a self-managed IoT.

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. Technologies such as homomorphic and searchable encryption are potential candidates for developing such approaches.

• 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 the ubiquity and pervasiveness of 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. Each soft identity can be designed for a specific context or application without revealing unnecessary information, which can lead to privacy breaches.