International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 02, July-December 2016
ISSN (O) 2321-2055
ISSN (P) 2321 -2045

RECENT TRENDS IN IOT

P.Saichaitanya[1], N.Karthik[2], D.Surender[3]
[1,2,3]Asst.prof, ECE, KITS(S)

ABSTRACT

Many technical communities are vigorously pursuing research topics that contribute to the Internet of Things (IoT). Today, as sensing, actuation, communication, and control become ever more sophisticated and ubiquitous, there is significant overlap in these communities, sometimes from slightly different perspectives. More cooperation between communities is encouraged. To provide a basis for discussing open research problems in IoT, a vision for how IoT could change the world in the distant future is first presented. Then, eight key research topics are enumerated and research problems within those topics are discussed.

Keyterms: **internet of things, communication**

I. INTRODUCTION

Ten "critical" trends and technologies impacting IT for the next five years were laid out by Gartner and among them the Internet of Things. All of these things have an IP address and can be tracked. The Internet is expanding into enterprise assets and consumer items such as cars and televisions. The problem is that most enterprises and technology vendors have yet to explore the possibilities of an expanded Internet and are not operationally or organizationally ready. four basic usage models that are emerging:

- Manage
- Monetize
- Operate
- Extend.

These can be applied to people, things, information, and places, and therefore the so called "Internet of Things" will be succeeded by the "Internet of Everything."

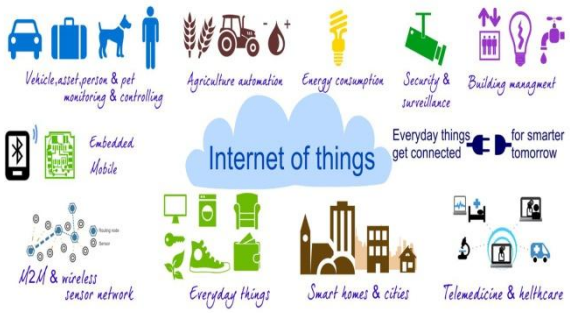


Fig : internet of things

The fundamental characteristics of the IoT are as follows :

- **Interconnectivity**: With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.
- **Things-related services:** The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things.
- **Heterogeneity**: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.
- **Dynamic changes**: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.
- **Enormous scale**: The number of devices that need to be managed and that communicate with each otherwill be at least an order of magnitude .

II. INTERNET OF THINGS VISION:

Internet of Things (IoT) is a concept and a paradigm that considers pervasive presence in the environment of a variety of things/objects that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications/services and reach common goals. In this context the research and development challenges to create a smart world are enormous. A world where the real, digital and the virtual are converging to create smart environments that make energy, transport, cities and many other areas more intelligent. The goal of the Internet of Things is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service. Internet of Things is a new revolution of the Internet. Objects make themselves recognizable and they obtain intelligence by making or enabling context related decisions thanks to the fact that they can communicate information about themselves and they can access information that has been aggregated by other things, or they can be components of complex services.

III. IOT STRATEGIC RESEARCH AND INNOVATION DIRECTIONS:

The development of enabling technologies such as nano electronics, communications, sensors, smart phones, embedded systems, cloud networking, network virtualization and software will be essential to provide to things the capability to be connected all the time everywhere. This will also support important future IoT product innovations affecting many different industrial sectors. Some of these technologies such as embedded or cyber-physical systems form the edges of the Internet of Things bridging the gap between cyber space and the physical world of real things, and are crucial in enabling the Internet of Things to deliver on its vision and become part of bigger systems in a world of “systems of systems”.

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 02, July-December 2016
ISSN (O) 2321-2055
ISSN (P) 2321 -2045

IV. IOT FUNCTIONAL VIEW:

The Internet of Things concept refers to uniquely identifiable things with their virtual representations in an Internet-like structure and IoT solutions comprising a number of components such as:

- Module for interaction with local IoT devices (for example embedded in a mobile phone or located in the immediate vicinity of the user and thus contactable via a short range wireless interface). This module is responsible for acquisition of observations and their forwarding to remote servers for analysis and permanent storage.
- Module for local analysis and processing of observations acquired by IoT devices.
- Module for interaction with remote IoT devices, directly over the Internet or more likely via a proxy. This module is responsible for acquisition of observations and their forwarding to remote servers for analysis and permanent storage.
- Module for application specific data analysis and processing. This module is running on an application server serving all clients. It is taking requests from mobile and web clients and relevant IoT observations as input, executes appropriate data processing algorithms and generates output in terms of knowledge that is later presented to users.
- Module for integration of IoT-generated information into the business processes of an enterprise. This module will be gaining importance with the increased use of IoT data by enterprises as one of the important factors in day-to-day business or business strategy definition.
- User interface (web or mobile): visual representation of measurements in a given context (for example on a map) and interaction with the user, i.e. definition of user queries.

It is important to highlight that one of the crucial factors for the success of IoT is stepping away from vertically-oriented, closed systems towards open systems, based on open APIs and standardized protocols at various system levels.

Effectively extract actionable information from vast amounts of raw data, while providing a robust timing and systems framework to support the real-time control and synchronization requirements of complex, networked, engineered physical/cyber/virtual systems.

A large number of applications made available through application markets have significantly helped the success of the smart phone industry. The development of such a huge number of smart phone applications is primarily due to involvement of the developers' community at large. Developers leveraged smart phone open platforms and the corresponding development tools, to create a variety of applications and to easily offer them to a growing number of users through the application markets.

Similarly, an IoT ecosystem has to be established, defining open APIs for developers and offering appropriate channels for delivery of new applications. Such open APIs are of particular importance on the level of the module for application specific data analysis and processing, thus allowing application developers to leverage the underlying communication infrastructure and use and combine information generated by various IoT devices to produce new, added value.

The complete system will have to include supporting tools providing security and business mechanisms to enable interaction between a numbers of different business entities that might exist.

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 02, July-December 2016
ISSN (O) 2321-2055
ISSN (P) 2321 -2045

V. RESEARCH CHALLENGES:

- Design of open APIs on all levels of the IoT ecosystem
- Design of standardized formats for description of data generated by IoT devices to allow mashups of data coming from different domains and/or providers.

VI. RESEARCH:

- The spectrum of research required to achieve IoT at the scale envisioned above requires significant research along many directions. In this section problems and required research are highlighted in 8 topic areas: massive scaling, architecture and dependencies, creating knowledge and big data, robustness, openness, security, privacy, and human-in-the-loop. Each of the topic discussions primarily focuses on new problems that arise for future IoT systems of the type described in Section II. The research topics presented in each case are representative and not complete.
- Many important topics such as the development of standards, the impact of privacy laws, and the cultural impact on use of these technologies are outside the scope of the paper.

VII. CREATING KNOWLEDGE AND BIG DATA

- In an IoT world there will exist a vast amount of raw data being continuously collected. It will be necessary to develop techniques that convert this raw data into usable knowledge. For example, in the medical area, raw streams of sensor values must be converted into semantically meaningful activities performed by or about a person such as eating, poor respiration, or exhibiting signs of depression. Main challenges for data interpretation and the formation of knowledge include addressing noisy, physical world data and developing new inference techniques that do not suffer the limitations of Bayesian or Dempster-Shafer schemes. These limitations include the need to know a priori probabilities and the cost of computations. Rule based systems may be used, but may also be too ad hoc for some applications.

The amount of collected data will be enormous. It can be expected that a very large number of real-time sensor data streams will exist, that it will be common for a given stream of data to be used in many different ways for many different inference purposes, that the data provenance and how it was processed must be known, and that privacy and security must be applied. Data mining techniques are expected to provide the creation of important knowledge from all this data. Enabling streams to act as primitives for unexpected future inferences is an interesting research problem. In addition, the overall system solution must deal with the fact that no inference method is 100% correct. Consequently, uncertainty in interpreted data can easily cause users not to trust the system.

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 02, July-December 2016
ISSN (O) 2321-2055
ISSN (P) 2321 -2045

VIII. SECURITY IN IOT:

A fundamental problem that is pervasive in the Internet today that must be solved is dealing with security attacks. Security attacks are problematic for the IoT because of the minimal capacity "things" being used, the physical accessibility to sensors, actuators and objects, and the openness of the systems, including the fact that most devices will communicate wirelessly. The security problem is further exacerbated because transient and permanent random failures are commonplace and failures are vulnerabilities that can be exploited by attackers. However, the considerable redundancy that is available creates potential for designing applications to continue to provide their specified services even in the face of failures. To meet realistic system requirements that derive from long lived and unattended operation, IoT applications must be able to continue to operate satisfactorily in the presence of, and to recover effectively from security attacks. Solutions may require downloading new code and this itself is open to security attacks. The system must also be able to adapt to new attacks unanticipated when the system was first deployed.

IX. IOT SMART-X APPLICATIONS

It is impossible to envisage all potential IoT applications having in mind the development of technology and the diverse needs of potential users. In the following sections, we present several applications, which are important. These applications are described, and the research challenges are identified. The IoT applications are addressing the societal needs and the advancements to enabling technologies such as nano electronics and cyber-physical systems continue to be challenged by a variety of technical (i.e., scientific and engineering), institutional, and economical issues.

The list is focusing to the applications chosen by the IERC as priorities for the next years and it provides the research challenges for these applications. While the applications themselves might be different, the research challenges are often the same or similar.

X. SMART CITIES

By 2020 we will see the development of Mega city corridors and networked, integrated and branded cities. With more than 60 percent of the world population expected to live in urban cities by 2025, urbanization as a trend will have diverging impacts and influences on future personal lives and mobility. Rapid expansion of city borders, driven by increase in population and infrastructure development, would force city borders to expand outward and engulf the surrounding daughter cities to form mega cities, each with a population of more than 10 million. By 2023, there will be 30 mega cities globally, with 55 percent in developing economies of India, China, Russia and Latin America .

A smart city is defined as a city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rail/subways, airports, seaports, communications, water, power, even major buildings, can better optimize its resources, plan its preventive maintenance activities, and monitor security

aspects while maximizing services to its citizens. Emergency response management to both natural as well as man-made challenges to the system can be focused. With advanced monitoring systems and built-in smart sensors, data can be collected and evaluated in real time, enhancing city management's decision-making. For example, resources can be committed prior to a water main break, salt spreading crews dispatched only when a specific bridge has icing conditions, and use of inspectors reduced by knowing condition of life of all structures. In the long term Smart Cities vision, systems and structures will monitor their own conditions and carry out self-repair, as needed.

An illustrative example is depicted in Figure. The deployment of ICT to create 'smart cities' is gaining momentum in Europe, according to a study by Frost & Sullivan, accentuated by the numerous pilot projects running at regional, country and EU levels. Initiatives revolve around energy and water efficiency, mobility, infrastructure and platforms for open cities, citizen involvement, and public administration services.Projects are carried out in the form of collaborative networks established between the research community, businesses, the public sector, citizens and the wider community, and they foster an open innovation approach. Technologies such as smart metering, wireless sensor networks, open platforms, high-speed broadband and cloud computing are key building blocks of the smart city infrastructure.

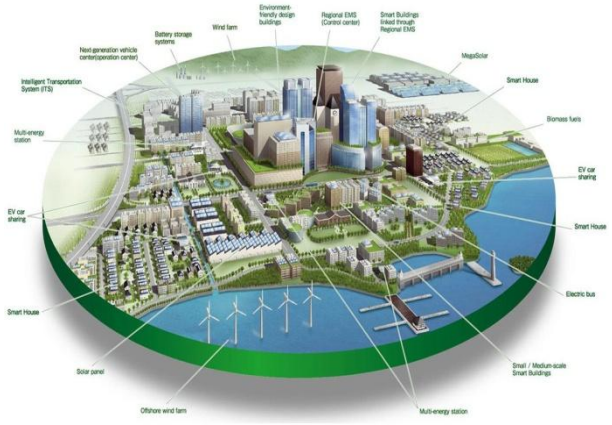


Figure 3.18 Smart City Concept.

XI. TRUST FOR IOT

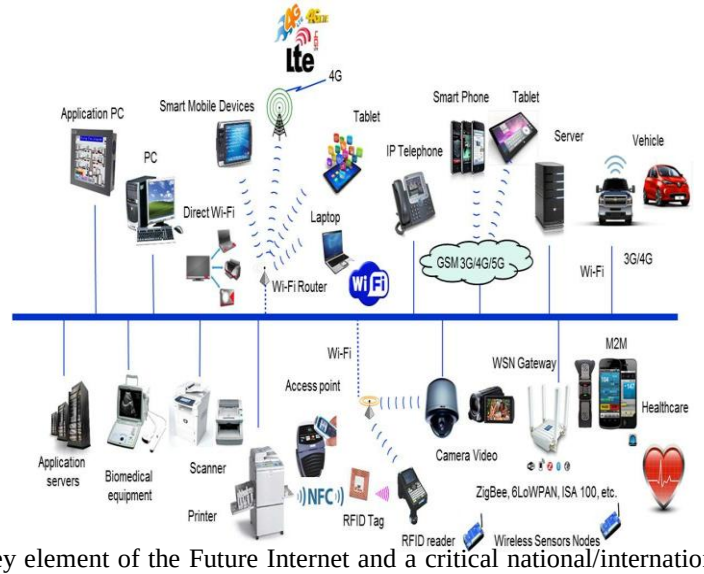
As IoT-scale applications and services will scale over multiple administrative domains and involve multiple ownership regimes, there is a need for a trust framework to enable the users of the system to have confidence that the information and services being exchanged can indeed be relied upon. The trust framework needs to be able to deal with humans and machines as users, i.e. it needs to convey trust to humans and needs to be robust enough to be used by machines without denial of service. 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 man-agement. Advances are expected in hierarchical and cross certification concepts to enable solutions to address the scalability requirements.

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 02, July-December 2016
ISSN (O) 2321-2055
ISSN (P) 2321 -2045

- Lightweight key management systems to enable trust relationships to be established and the distribution of encryption materials using minimum communications and processing resources, as is consistent with the resource constrained nature of many IoT devices.
- Quality of Information is a requirement for many IoT-based systems where metadata can be used to provide an assessment of the reliability of IoT data.
- Decentralised and self-configuring systems as alternatives to PKI for establishing trust e.g. identity federation, peer to peer.
- Novel methods for assessing trust in people, devices and data, beyond reputation systems. One example is Trust Negotiation. Trust Negotiation is a mechanism that allows two parties to automatically negotiate, on the basis of a chain of trust policies, the minimum level of trust required to grant access to a service or to a piece of information.
- Assurance methods for trusted platforms including hardware, software, protocols, etc.
- Access Control to prevent data breaches. One example is Usage Control, which is the process of ensuring the correct usage of certain information according to a predefined policy after the access to information is granted.

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 analyze 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 spe-cific 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 account-ing schemes to support the various authorisation 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.

XII. 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 pro-cessed 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 decentralised 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.

XIII. CONCLUSION

In summary, one vision of the future is that IoT becomes a utility with increased sophistication in sensing, actuation, communications, control, and in creating knowledge from vast amounts of data. This will result in qualitatively different lifestyles from today. What the lifestyles would be is anyone's guess. It would be fair to say that we cannot predict how lives will change. We did not predict the Internet, the Web, social networking, Face book, Twitter, millions of apps for Smartphone, etc., and these have all qualitatively changed societies' lifestyle. New research problems arise due to the large scale of devices, the connection of the physical and cyber worlds, the openness of the systems of systems, and continuing problems of privacy and security. It is hoped that there is more cooperation between the research communities in order to solve the myriad of problems sooner as well as to avoid re-inventing the wheel when a particular community solves a problem.

REFERENCES

[1] NFC Forum, online at http://nfc-forum.org

[2] METIS, Mobile and wireless communications Enablers for the Twenty-twenty (2020) Information Society, online at https://www.metis2020 .com/

[3] Wemme, L., "NFC: Global Promise and Progress", NFC Forum, 22.01.2014, online at http://nfc-forum.org/wp-content/uploads/2014/01/ Omnicard Wemme 2014 website.pdf

[4] Bluetooth Special Interest Group, online at https://www.bluetooth.org/en-us/members/about-sig

[5] Bluetooth Developer Portal, online at https://developer.bluetooth.org/ Pages/default.aspx

[6] ANT+, online at http://www.thisisant.com/

[7] ANT, "Message Protocol and Usage rev.5.0", online at http://www .thisisant.com/developer/resources/downloads#documents tab

[8] ANT, "FIT2 Fitness Module Datasheet", online at http://www.thisisant .com/developer/resources/downloads#documents tab

[9] Wi-Fi Alliance, online at http://www.wi-fi.org/

[10] Z-Wave alliance, online at http://www.z-wavealliance.org

[11] Pätz, C., "Smart lighting. How to develop Z-Wave Devices", EE Times europe LEDLighting, 04.10.2012, online at http://www.ledlighting-eetimes.com/en/how-to-develop-z-wave-devices.html?cmp id=71& news id=222908151

[12] KNX, online at http://www.knx.org/knx-en/knx/association