Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems

Srividhya
Department of Computer Science, Indian Academy Degree College, Bangalore, India

Abstract— Internet of Things is an area of improvement and growth. As anembodiment the next step in the Internet of Things advancement will be the consistency of efforts on all levels towards novelty. The Internet of Things continues to assert its important position in the context of Information and Communication Technologies and the progress of society. Whereas concepts and basic foundations have been elaborated and reached maturity, further efforts are necessary for unleashing the full potential. 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. Internet of Things has exponentially increased the scale and complexity of computing and communication systems. Autonomy is thus an imperative property for IOT systems. IOT technologies improve industrial manufacturing processes, enable new and efficient ways to operate production plants, create new service or supervision means for industrial installations, offer an optimized infrastructure, reduce operational cost or improve human safety in industrial areas. Robustness, standardization, easy installation, con- figuration and servicing are essential to keep IoT systems operational and hence offering value for the industry operation and services. One specific challenge in IoT is the control of the information collected and distributed by mobile devices which are increasingly small and pervasive like RFID or future micro-nano sensors, which can be worn or distributed in the environment. The Internet of the Future will be an essential part of the knowledge society and will provide new information-based business. The usage of the Internet of Things for large-scale, partially mission-critical systems creates the need to address trust and security functions adequately. Technically speaking IoT is mainly supported by continuous progress in wireless sensor networks software applications and by manufacturing low cost and energy efficient hardware for sensor and device communications. However, heterogeneity of underlying devices and communication technologies and interoperability in different layers, from communication and seamless integration of devices to interoperability of data generated by the IoT resources, is a challenge for expanding generic IoT solutions to a global scale. Ubiquitous computing has seen a shift from a computer-centric model, where one computer would be used by at least one person, to a user-centric one, with several computers surrounding a single person providing them information, services and applications. Thus, the foundations of the Internet of Things (the IoT) were established.

Keywords: *Internet of Things, RFID, Autonomic Computing, Ubiquitous Computing*

I. INTRODUCTION

Internet of Things (IoT) refers to physical and virtual objects that have unique identities and are connected to the internet to facilitate intelligent applications that make energy, logistics, industrial control, retail, agriculture and many other domains "smarter". Internet of Things is a new revolution of the Internet that is rapidly gathering momentum driven by the advancements in sensor networks, mobile devices, wireless communications, networking and cloud technologies. This unprecedented penetration of virtually everyone's life suggests the need for a close scrutiny of the various processes to be associated with the development of such a technology and its subsequent wide deployment. International standardization is among the most important of these processes.

In case of the IoT community this would mean that out of many possible "coherence horizons" the following will likely provide the foundation for a step forward to the Internet of Things:

Coherence of object capabilities and behaviour: the objects in the Internet of Things will show a huge variety in sensing and actuation capabilities, in information processing functionality and their time of existence. In either case it will be necessary to generally apprehend object as entities with a growing "intelligence" and patterns of autonomous behaviour.

Coherence of application interactivity: the applications will increase in complexity and modularisation, and boundaries between applications and services will be blurred to a high degree. Fixed programmed suites will evolve into dynamic and learning application packages. Besides technical, semantic interoperability will become the key for context aware information exchange and processing.

Coherence of corresponding technology approaches: larger concepts like Smart Cities, Cloud computing, Future Internet, robotics and others will evolve in their own way, but because of complementarity also partly merge with the Internet of Things. Here a creative view on potential synergies can help to develop new ecosystems.

Coherence of real and virtual worlds: today real and virtual worlds are perceived as two antagonistic conceptions. At the same time virtual worlds grow exponentially with the amount of stored data and ever increasing network and information processing capabilities. Understanding both paradigms as complementary and part of human evolution could lead to new synergies and exploration of living worlds.

The Internet of Things makes use of synergies that are generated by the convergence of Consumer, Business and Industrial Internet

The convergence creates the open, global network connecting people, data, and things. This convergence leverages the cloud to connect intelligent things that sense and transmit a broad array of data, helping creating services that would not be obvious without this level of connectivity and analytical intelligence. The use of platforms is being driven by transformative technologies such as cloud, things, and mobile. The cloud enables a global infrastructure to generate new services, allowing anyone to create content and applications for

global users. Networks of things connect things globally and maintain their identity online. Mobile allows connection to this global infrastructure anytime, anywhere. The result is a globally accessible network of things, users, and consumers, who are available to create businesses, contribute content, generate and purchase new services.

Enabling technologies for the Internet of Things such as sensor networks, RFID, M2M, mobile Internet, semantic data integration, semantic search, IPv6, etc. are considered in and can be grouped into three categories:

i. technologies that enable "things" to acquire contextual information,
ii. technologies that enable "things" to process contextual information, and
iii. technologies to improve security and privacy.

The first two categories can be jointly understood as functional building blocks required building "intelligence" into "things", which are indeed the features that differentiate the IoT from the usual Internet. The third category is not a functional but rather a de facto requirement, without which the penetration of the IoT would be severely reduced. Internet of Things developments implies that the environments, cities, buildings, vehicles, clothing, portable devices and other objects have more and more information associated with them and/or the ability to sense, communicate, network and produce new information. In addition we can also include non-sensing things (i.e. things that may have functionality, but do not provide information or data).

The combination of the Internet and emerging technologies such as nearfield communications, real-time localization, and embedded sensors lets us transform everyday objects into smart objects that can understand and react to their environment. Such objects are building blocks for the Internet of Things and enable novel computing applications. As a step toward design and architectural principles for smart objects, a hierarchy of architectures with increasing levels of real-world awareness and interactivity are introduced. In particular, they describe activity-, policy-, and process-aware smart objects and demonstrate how the respective architectural abstractions support increasingly complex application.

Ubiquitous sensing enabled by Wireless Sensor Network (WSN) technologies cuts across many areas of modern day living. This offers the ability to measure, infer and understand environmental indicators, from delicate ecologies and natural resources to urban environments. The proliferation of these devices in a communicating–actuating network creates the Internet of Things (IoT), wherein sensors and actuators blend seamlessly with the environment around us, and the information is shared across platforms in order to develop a common operating picture (COP). Fueled by the recent adaptation of a variety of enabling wireless technologies such as RFID tags and embedded sensor and actuator nodes, the IoT has stepped out of its infancy and is the next revolutionary technology in transforming the Internet into a fully integrated Future Internet. As we move from www (static pages web) to web2 (social networking web) to web3 (ubiquitous computing web), the need for data-on-demand using sophisticated intuitive queries increases significantly. This paper presents a Cloud centric vision for worldwide implementation of Internet of Things. The key enabling technologies and application domains that are likely to drive IoT research in the near future are discussed. A Cloud implementation using *Aneka*, which is based on interaction of private and public Clouds is presented. We conclude our IoT vision by expanding on the need for convergence of WSN, the Internet and distributed computing directed at technological research community.

Ubiquitous Computing

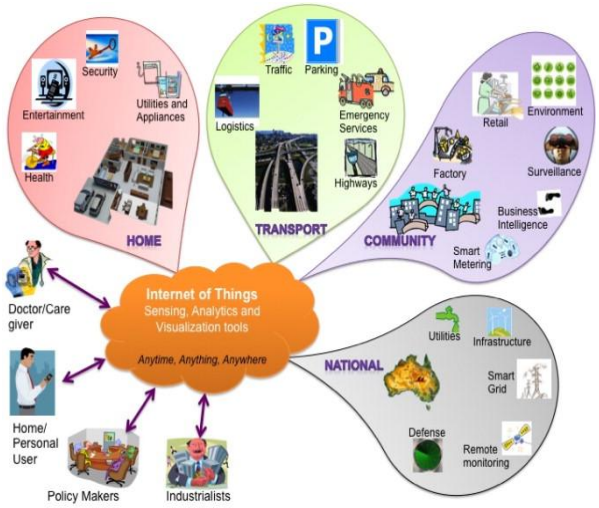
The next wave in the era of computing will be outside the realm of the traditional desktop. In the Internet of Things (IoT) paradigm, many of the objects that surround us will be on the network in one form or another. Radio Frequency IDentification (RFID) and sensor network technologies will rise to meet this new challenge, in which information and communication systems are invisibly embedded in the environment around us. This results in the generation of enormous amounts of data which have to be stored, processed and presented in a seamless, efficient, and easily interpretable form. This model will consist of services that are commodities and delivered in a manner similar to traditional commodities. Cloud computing can provide the virtual infrastructure for such utility computing which integrates monitoring devices, storage devices, analytics tools, visualization platforms and client delivery. The cost based model that Cloud computing offers will enable end-to-end service provisioning for businesses and users to access applications on demand from anywhere.

Smart connectivity with existing networks and context-aware computation using network resources is an indispensable part of IoT. With the growing presence of WiFi and 4G-LTE wireless Internet access, the evolution towards ubiquitous information and communication networks is already evident. However, for the Internet of Things vision to successfully emerge, the computing paradigm will need to go beyond traditional mobile computing scenarios that use smart phones and portables, and evolve into connecting everyday existing objects and embedding intelligence into our environment. For technology to *disappear* from the consciousness of the user, the Internet of Things demands:

1. a shared understanding of the situation of its users and their appliances,
2. software architectures and pervasive communication networks to process and convey the contextual information to where it is relevant, and
3. the analytics tools in the Internet of Things that aim for autonomous and smart behavior. With these three fundamental grounds in place, smart connectivity and context-aware computation can be accomplished.

The term Internet of Things was first coined by Kevin Ashton in 1999 in the context of supply chain management. However, in the past decade, the definition has been more inclusive covering wide range of applications like healthcare, utilities, transport, etc. Although the definition of 'Things' has changed as technology evolved, the main goal of making a computer sense information without the aid of human intervention remains the same. A radical evolution of the current Internet into a Network of interconnected *objects*that not only harvests information from the environment (sensing) and interacts with the physical world (actuation/command/control), but also uses existing Internet standards to provide services for information transfer, analytics, applications, and communications. Fueled by the prevalence of devices enabled by open wireless technology such as Bluetooth, radio frequency identification (RFID), Wi-Fi, and telephonic data services as well as embedded sensor and actuator nodes, IoT has stepped out of its infancy and is on the verge of transforming the current static Internet into a fully integrated Future Internet. The Internet revolution led to the interconnection between people at an unprecedented scale and pace. The next revolution will be the interconnection between objects to create a smart environment.

Only in 2011 did the number of interconnected devices on the planet overtake the actual number of people. Currently there are 9 billion interconnected devices and it is expected to reach 24 billion devices by 2020. According to the GSMA, this amounts to $1.3 trillion revenue opportunities for mobile network operators alone spanning vertical segments such as health, automotive, utilities and consumer electronics. A schematic of the interconnection of objects is depicted in Fig. 1, where the application domains are chosen based on the scale of the impact of the data generated. The users span from individual to national level organizations addressing wide ranging issues.



This paper presents the current trends in IoT research propelled by applications and the need for convergence in several interdisciplinary technologies.

The effort by researchers to create a human-to-human interface through technology in the late 1980s resulted in the creation of the ubiquitous computing discipline, whose objective is to embed technology into the background of everyday life. Currently, we are in the post-PC era where smart phones and other handheld devices are changing our environment by making it more interactive as well as informative. Mark Weiser, the forefather of Ubiquitous Computing (ubicomp), defined a smart environment as "the physical world that is richly and invisibly interwoven with sensors, actuators, displays, and computational elements, embedded seamlessly in the everyday objects of our lives, and connected through a continuous network".

The creation of the Internet has marked a foremost milestone towards achieving ubicomp's vision which enables individual devices to communicate with any other device in the world. The inter-networking reveals the potential of a seemingly endless amount of distributed computing resources and storage owned by various owners.

In contrast to Weiser's Calm computing approach, Rogers proposes a human centric ubicomp which makes use of human creativity in exploiting the environment and extending their capabilities . He proposes a domain specific ubicomp solution when he says—"In terms of who should benefit, it is useful to think of how ubicomp technologies can be developed not for the Sal's of the world, but for particular domains that can be set up and customized by an individual firm or organization, such as for agricultural production, environmental restoration or retailing".

Caceres and Friday discuss the progress, opportunities and challenges during the 20 year anniversary of ubicomp. They discuss the building blocks of ubicomp and the characteristics of the system to adapt to the changing world. More importantly, they identify two critical technologies for growing the ubicomp infrastructure—*Cloud Computing* and the *Internet of Things*.

The advancements and convergence of micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics has resulted in the development of miniature devices having the ability to sense, compute, and communicate wirelessly in short distances. These miniature devices called nodes interconnect to form a wireless sensor networks (WSN) and find wide ranging applications in environmental monitoring, infrastructure monitoring, traffic monitoring, retail, etc. This has the ability to provide a ubiquitous sensing capability which is critical in realizing the overall vision of ubicomp as outlined by Weiser . For the realization of a complete IoT vision, efficient, secure, scalable and market oriented computing and storage resourcing is essential. Cloud computing is the most recent paradigm to emerge which promises reliable services delivered through next generation data centers that are based on virtualized storage technologies. This platform acts as a receiver of data from the ubiquitous sensors; as a computer to analyze and interpret the data; as well as providing the user with easy to understand web based visualization. The ubiquitous sensing and processing works in the background, *hidden* from the user.

This novel integrated Sensor–Actuator–Internet framework shall form the core technology around which a smart environment will be shaped: information generated will be shared across diverse platforms and applications, to develop a common operating picture (COP) of an environment, where control of certain unrestricted 'Things' is made possible. As we move from www (static pages web) to web2 (social networking web) to web3 (ubiquitous computing web), the need for data-on-demand using sophisticated intuitive queries increases. To take full advantage of the available Internet technology, there is a need to deploy large-scale, platform-independent, wireless sensor network infrastructure that includes data management and processing, actuation and analytics. Cloud computing promises high reliability, scalability and autonomy to provide ubiquitous access, dynamic resource discovery and composability required for the next generation Internet of Things applications. Consumers will be able to choose the service level by changing the Quality of Service parameters.

Radio Frequency Identification (RFID)

RFID technology is a major breakthrough in the embedded communication paradigm which enables design of microchips for wireless data communication. They help in the automatic identification of anything they are attached to acting as an electronic barcode. The passive RFID tags are not battery powered and they use the power of the reader's interrogation signal to communicate the ID to the RFID reader. This has resulted in many applications particularly in retail and supply chain management. The applications can be found in transportation (replacement of tickets, registration stickers) and access control applications as well. The passive tags are currently being used in many bank cards and road toll tags which are among the first global deployments. Active RFID readers have their own battery supply and can instantiate the communication. Of the several applications, the main application of active RFID tags is in port containers for monitoring cargo.

Wireless Sensor Networks (WSN)

Recent technological advances in low power integrated circuits and wireless communications have made available efficient,

low cost, low power miniature devices for use in remote sensing applications. The combination of these factors has improved the viability of utilizing a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing, analysis and dissemination of valuable information, gathered in a variety of environments. Active RFID is nearly the same as the lower end WSN nodes with limited processing capability and storage. The scientific challenges that must be overcome in order to realize the enormous potential of WSNs are substantial and multidisciplinary in nature. Sensor data are shared among sensor nodes and sent to a distributed or centralized system for analytics. The components that make up the WSN monitoring network include:

- WSN hardware—Typically a node (WSN core hardware) contains sensor interfaces, processing units, transceiver units and power supply. Almost always, they comprise of multiple A/D converters for sensor interfacing and more modern sensor nodes have the ability to communicate using one frequency band making them more versatile.
- WSN communication stack—The nodes are expected to be deployed in an ad-hoc manner for most applications. Designing an appropriate topology, routing and MAC layer is critical for the scalability and longevity of the deployed network. Nodes in a WSN need to communicate among themselves to transmit data in single or multi-hop to a base station. Node drop outs, and consequent degraded network lifetimes, are frequent. The communication stack at the sink node should be able to interact with the outside world through the Internet to act as a gateway to the WSN subnet and the Internet.
- WSN Middleware—A mechanism to combine cyber infrastructure with a Service Oriented Architecture (SOA) and sensor networks to provide access to heterogeneous sensor resources in a deployment independent manner. This is based on the idea of isolating resources that can be used by several applications. A platform-independent middleware for developing sensor applications is required, such as an Open Sensor Web Architecture (OSWA). OSWA is built upon a uniform set of operations and standard data representations as defined in the Sensor Web Enablement Method (SWE) by the Open Geospatial Consortium (OGC).
- Secure Data aggregation—An efficient and secure data aggregation method is required for extending the lifetime of the network as well as ensuring reliable data collected from sensors. Node failures are a common characteristic of WSNs, the network topology should have the capability to heal itself. Ensuring security is critical as the system is automatically linked to actuators and protecting the systems from intruders becomes very important.

Addressing schemes

The ability to uniquely identify 'Things' is critical for the success of IoT. This will not only allow us to uniquely identify billions of devices but also to control remote devices through the Internet. The few most critical features of creating a unique address are: uniqueness, reliability, persistence and scalability.

Every element that is already connected and those that are going to be connected, must be identified by their unique identification, location and functionalities. The current IPv4 may support to an extent where a group of cohabiting sensor devices can be identified geographically, but not individually. The Internet Mobility attributes in the IPV6 may alleviate some of the device identification problems; however, the heterogeneous nature of wireless nodes, variable data types, concurrent operations and confluence of data from devices exacerbates the problem further.

Persistent network functioning to channel the data traffic ubiquitously and relentlessly is another aspect of IoT. Although, the TCP/IP takes care of this mechanism by routing in a more reliable and efficient way, from source to destination, the IoT faces a bottleneck at the interface between the gateway and wireless sensor devices. Furthermore, the scalability of the device address of the existing network must be sustainable. The addition of networks and devices must not hamper the performance of the network, the functioning of the devices, the reliability of the data over the network or the effective use of the devices from the user interface.

To address these issues, the Uniform Resource Name (URN) system is considered fundamental for the development of IoT. URN creates replicas of the resources that can be accessed through the URL. With large amounts of spatial data being gathered, it is often quite important to take advantage of the benefits of metadata for transferring the information from a database to the user via the Internet. IPv6 also gives a very good option to access the resources uniquely and remotely. Another critical development in addressing is the development of a lightweight IPv6 that will enable addressing home appliances uniquely.

Wireless sensor networks (considering them as building blocks of IoT), which run on a different stack compared to the Internet, cannot possess IPv6 stack to address individually and hence a subnet with a gateway having a URN will be required. With this in mind, we then need a layer for addressing sensor devices by the relevant gateway. At the subnet level, the URN for the sensor devices could be the unique IDs rather than human-friendly names as in the www, and a lookup table at the gateway to address this device. Further, at the node level each sensor will have a URN (as numbers) for sensors to be addressed by the gateway. The entire network now forms a web of connectivity from users (high-level) to sensors (low-level) that is addressable (through URN), accessible (through URL) and controllable (through URC).

Data storage and analytics

One of the most important outcomes of this emerging field is the creation of an unprecedented amount of data. Storage, ownership and expiry of the data become critical issues. The internet consumes up to 5% of the total energy generated today and with these types of demands, it is sure to go up even further. Hence, data centers that run on harvested energy and are centralized will ensure energy efficiency as well as reliability. The data have to be stored and used intelligently for smart monitoring and actuation. It is important to develop artificial intelligence algorithms which could be centralized or distributed based on the need. Novel fusion algorithms need to be developed to make sense of the data collected. State-of-the-art non-linear, temporal machine learning methods based on evolutionary algorithms, genetic algorithms, neural networks, and other artificial intelligence techniques are necessary to achieve automated decision making. These systems show characteristics such as interoperability, integration and adaptive communications. They also have a modular architecture both in terms of hardware system design as well as software development and are usually very well-suited for IoT applications. More importantly, a centralized infrastructure to support storage and analytics is required. This forms the IoT middleware layer and there are numerous challenges involved which are discussed in future sections. As of 2012, Cloud based

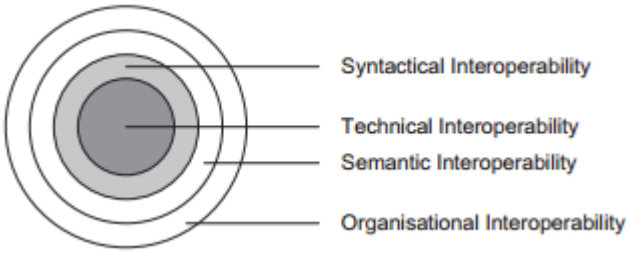
storage solutions are becoming increasingly popular and in the years ahead, Cloud based analytics and visualization platforms are foreseen.

Visualization

Visualization is critical for an IoT application as this allows the interaction of the user with the environment. With recent advances in touch screen technologies, use of smart tablets and phones has become very intuitive. For a lay person to fully benefit from the IoT revolution, attractive and easy to understand visualization has to be created. As we move from 2D to 3D screens, more information can be provided in meaningful ways for consumers. This will also enable policy makers to convert data into knowledge, which is critical in fast decision making. Extraction of meaningful information from raw data is non-trivial. This encompasses both event detection and visualization of the associated raw and modeled data, with information represented according to the needs of the end-user.

Different Types of Interoperability

A simple representation of interoperability can be seen as follows:



Technical Interoperability is usually associated with hardware/ software components, systems and platforms that enable machineto-machine communication to take place. This kind of interoperability is often centred on (communication) protocols and the infrastructure needed for those protocols to operate. Syntactical Interoperability is usually associated with data formats. Certainly, the messages transferred by communication protocols need to have a well-defined syntax and encoding, even if it is only in the form of bit-tables. However, many protocols carry data or content, and this can be represented using high-level transfer syntaxes such as HTML, XML or ASN.1 Semantic Interoperability is usually associated with the meaning of content and concerns the human rather than machine interpretation of the content. Thus, interoperability on this level means that there is a common understanding between people of the meaning of the content (information) being exchanged. Organizational Interoperability, as the name implies, is the ability of organizations to effectively communicate and transfer (meaningful) data (information) even though they may be using a variety of different information systems over widely different infrastructures, possibly across different geographic regions and cultures. Organizational interoperability depends on successful technical, syntactical and semantic interoperability. We can add two other dimensions: Static and dynamic interoperability

The Semantic Interoperability

In recent years convergence between Internet technologies for communication's, computation's and storage's networks and the semantic web has been a clear trend in the Information and Communications Technology (ICT) domain. Although widely discussed and researched, this trend has not fully run its course in terms of implementation, due to many complex issues involving deployment of non-interoperable and management infrastructural aspects, bottlenecks in the telecommunication systems, laciness on interoperability of big data processing in computing and Internet systems and also due to technological, social and economic restrictions in the ICT sector. Telecommunications networks have undergone a radical shift from a traditional circuit-switched environment with heavy/complex signalling focused on applications-oriented perspective, towards a converged service-oriented space, mostly Internet-based systems interaction by customer as end-user and network operators as service providers with the semantic web as main enabler. In this radical shift services and networks follow a common goal: to provide solutions (services and applications) in a form of implemented interoperable data mechanisms. The business benefits of this shift significantly reflect cost reduction and increase systems flexibility to react to user data demands, by replacing a plethora of proprietary hardware and ad-hoc software platforms with generic solutions supporting standardised development and deployment stacks. In the other hand emergence and wide-scale deployment of wireless access network technologies calls into question the viability of basing the future Internet-based solutions on IP and TCP — protocols that were never intended for use across highly unreliable and volatile wireless interfaces. The GENI NSF-funded initiative to rebuild the Internet, argue that the future lies in layers of overlay networks that can meet various requirements whilst keeping a very simplistic, almost unmanaged, IP for the underlying Future Internet design. Others initiatives such as Clean Slate program, Stanford University, and Architecture Design Project for New Generation Network argue that the importance of wireless access networks requires a more fundamental redesign of the core Internet Protocols themselves. Likewise the pervasiveness of the physical devices and objects, resource constraints such as memory and power limitations on daily life devices, heterogeneity of the platforms and communication protocols create new challenges in inter-networking technologies and interaction mechanisms that enable interaction between data provides and consumers in the multiple domains. These challenges have raised new issues that are reflected in the recent architecture, design and development efforts for the Future Internet. The interaction of the physical devices "objects" amongst other objects bring some implications on resource constraints such as memory and power limitations, likewise heterogeneity of the platforms and communication protocols create new challenges in inter-networking technologies and for data interaction mechanisms enabling interaction between data providers and consumers. Particularly in the IoT domain those interactions are generating a big challenge in order to establish common ways to interact and/or simply exchange information between the objects. IoT has raised new issues that are reflected in the recent Internet architecture, important aspects to consider as design and development efforts for the Future Internet. The research in IoT has recently gained momentum and is supported by new communication protocols, standards and methods that consider the dynamicity and heterogeneity of the underlying devices and resources and enable internetworking and interactions on IoT. However, the current IoT data communications often rely on binary or syntactic data models that are unable to provide machine-interpretable representation of the data. This hinders the creation of common tools and mechanisms to process and interpret the IoT data on a large scale that can be supported by different stakeholders in a global framework. In general, large-scale platforms require to support discovery and access to the resources, enable autonomous interactions with the resources, and use self-descriptive data and association mechanisms to

process and interpret the IoT data, and integrate it into the high-level applications and service layers. To achieve global IoT data distribution and utilisation, semantic interoperability between IoT resources and data providers and consumers is a key issue. This will also support effective discovery, query, interpretation and integration of the IoT data. Semantic interoperability ensures that data can be comprehended unambiguously by human users and software programs across different platforms. Automated processing and interpretation of the IoT data requires common agreements on providing and describing the IoT data. To evaluate the quality aspects of data, the source provider, device and environment specific information also need to be associated to the data. Considering the diversity of data types, device types and potential providers in the IoT domain, common description frameworks are essential to describe and represent the data to make it seamlessly accessible and process-able across different platforms and stakeholders. In general, to achieve automated and seamless integration of the IoT data in business applications and services, semantic description of different resources in the IoT domain is a key task. The aforementioned works are some examples of the recent efforts that have been made to address this issue. The semantic descriptions and annotations need to be provided at "Things" level (e.g. entity model described in, OGC O&M model), device and network level (e.g. W3C SSN ontology), Service level (e.g. SemSoS [), and interaction and business process model (e.g. the IoT-aware business process modelling described in) to enable autonomous processing and interpretation of the IoT data by different stakeholders in IoT business process lifecycle.

CONCLUSION

The proliferation of devices with communicating–actuating capabilities is bringing closer the vision of an Internet of Things, where the sensing and actuation functions seamlessly blend into the background and new capabilities are made possible through access of rich new information sources. The evolution of the next generation mobile system will depend on the creativity of the users in designing new applications. IoT is an ideal emerging technology to influence this domain by providing new evolving data and the required computational resources for creating revolutionary apps.

Presented here is a user-centric cloud based model for approaching this goal through the interaction of private and public clouds. In this manner, the needs of the end-user are brought to the fore. Allowing for the necessary flexibility to meet the diverse and sometimes competing needs of different sectors, we propose a framework enabled by a scalable cloud to provide the capacity to utilize the IoT. The framework allows networking, computation, storage and visualization themes separate thereby allowing independent growth in every sector but complementing each other in a shared environment. The standardization which is underway in each of these themes will not be adversely affected with Cloud at its center. In proposing the new framework associated challenges have been highlighted ranging from appropriate interpretation and visualization of the vast amounts of data, through to the privacy, security and data management issues that must underpin such a platform in order for it to be genuinely viable. The consolidation of international initiatives is quite clearly accelerating progress towards an IoT, providing an overarching view for the integration and functional elements that can deliver an operational IoT.

References

[1] M. Zhang, T. Yu, G.F. Zhai, Smart transport system based on "The Internet of Things", Applied Mechanics and Materials, 48–49 (2011),pp. 1073–1076.

[2] M. Yun, B. Yuxin, Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid, in: Advances in Energy Engineering, ICAEE, 2010, pp. 69–72.

[3] I.F. Akyildiz, T. Melodia, K.R. Chowdhury, A survey on wireless multimedia sensor networks, Computer Networks, 51 (2007), pp. 921–960

[4] T.S. Lopez, D.C. Ranasinghe, M. Harrison, D. McFarlane, Adding sense to the Internet of Things an architecture framework for smart objective systems, Pervasive Ubiquitous Computing, 16 (2012), pp. 291–308

[5] C. Vecchiola, R.N. Calheiros, D. Karunamoorthy, R. Buyya, Deadline-driven provisioning of resources for scientific applications in hybrid clouds with Aneka, Future Generation Computer Systems (2012), pp. 58–65

[6] A.P. Castellani, N. Bui, P. Casari, M. Rossi, Z. Shelby, M. Zorzi, Architecture and protocols for the Internet of Things: a case study, 2010, pp. 678–683.

[7] J. Gubbi, K. Krishnakumar, R. Buyya, M. Palaniswami, A cloud computing framework for data analytics in smart city applications, Technical Report No. CLOUDS-TR-2012-2A, Cloud Computing and Distributed Systems Laboratory, The University of Melbourne, 2012.

[8] R.V. Kulkarni, A. Förster, G.K. Venayagamoorthy, Computational intelligence in wireless sensor networks: a survey, IEEE Communications Surveys & Tutorials, 13 (2011), pp. 68–96

[9] K. Ashton, That "Internet of Things" thing, RFiD Journal (2009).

[10] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realising the Internet of Things, Cluster of European Research Projects on the Internet of Things—CERP IoT, 2010.

[11] J. Buckley (Ed.), The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems, Auerbach Publications, New York (2006).

[12] M. Weiser, R. Gold, The origins of ubiquitous computing research at PARC in the late 1980s, IBM Systems Journal (1999).

[13] R. Caceres, A. Friday, Ubicomp systems at 20: progress, opportunities, and challenges, IEEE Pervasive Computing, 11 (2012), pp. 14–21.