ISSN:0975-9646

A Survey on Computing, Communication & Identification Technologies Used For Internet of Things

Prof. Apurva B. Parandekar ,
Assistant Professor, Sipna College of Engineering & Technology, Amravati ,

Prof. Ambarish R. Bhuyar,
Assistant Professor, Sipna College of Engineering & Technology, Amravati

Abstract: **Internet of Things (IoT) is becoming integral and mandatory part of everyday life. Scalability and manageability of data used over internet is intimidating solutions to be found due to unbounded number of services. Identification of services and authorization in IoT with least privilege is important to establish secure communication between multiple devices and services. Internet-of-Things is a future in which digital and physical objects can be linked, by means of appropriate information and communication technologies, to enable a whole new class of applications and services. The possibility of seamlessly merging the real and the virtual world, through the massive deployment of embedded devices & communication technologies opens up new exciting directions for development of both research and business in this area. In this paper we present a survey of recent developing technologies for computing capabilities and identification of communication techniques used for Internet of- Things.**

Keywords- **Internet of Things(IoT), objects, sensors.**

1. INTRODUCTION

Nowadays, around two billions people around the world use the Internet for browsing the Web, sending and receiving emails, accessing multimedia content and services, playing games, using social networking applications and many other tasks. While more and more people will gain access to such a global information and communication infrastructure, another big leap forward is coming, related to the use of the Internet as a global platform for letting machines and smart objects communicate, dialogue, compute and coordinate. It is predictable that, within the next decade, the Internet will exist as a seamless fabric of classic networks and networked objects. Content and services will be all around us, always available, paving the way to new applications, enabling new ways of working; new ways of interacting; new ways of entertainment; new ways of living. In such a perspective, the conventional concept of the Internet as an infrastructure network reaching out to end-users' terminals will fade, leaving space to a notion of interconnected ''smart'' objects forming pervasive computing environments. The Internet infrastructure will not disappear[1]. On the contrary, it will retain its vital role as global backbone for worldwide information sharing and diffusion, interconnecting physical objects with computing communication capabilities across a wide range of services and technologies. This innovation will be enabled by the embedding of electronics into everyday physical objects, making them ''smart'' and letting them seamlessly integrate within the global resulting cyber physical infrastructure. This will give rise to new opportunities for the Information and Communication Technologies (ICT) sector, paving the way to new services and applications able to leverage the interconnection of physical and virtual realms. Within such perspective, the term ''Internet-of-Things'' (IoT) is broadly used to refer to both: (i) the resulting global network interconnecting smart objects by means of extended Internet technologies, (ii) the set of supporting technologies necessary to realize such a vision (including, e.g., RFIDs, sensor actuators machine-to-machine communication devices, etc.) and (iii) the ensemble of applications and services leveraging such technologies to open new business and market opportunities [2,3]. In this survey article, we aim at providing a holistic perspective on the Internet-of-Things concept and development, including a critical revision of application fields, enabling technologies and research challenges. As a matter of fact, the research community active on IoT-related themes is still highly fragmented, and, to a large extent, focused around single application domains or single technologies. Further, the involvement of the networking and communications scientific communities is still limited, despite the high potential impact of their contributions on the development of the field [2,4]. We do believe that this fragmentation is potentially harmful for the development and successful adoption of IoT technologies. We therefore hope this survey can help in bridging existing communities, fostering cross-collaborations and ensuring that IoT-related challenges are tackled within a system-level perspective, ensuring that the research activities can then be turned into successful innovation and industry exploitation. identified.

2. IOT FUNCTIONAL BLOCKS

An IoT system is comprised of a number of functional blocks to facilitate various utilities to the system such as, sensing, identification, actuation, communication, and management presents these functional blocks as described below.

Device: An IoT system is based on devices that provide sensing, actuation, control, and monitoring activities. IoT devices can exchange data with other connected devices and application, or collect data from other devices and process the data either locally or send the data to centralized servers or cloud based applications back-ends for processing the data, or perform some tasks locally and other tasks within IoT infrastructure based on temporal and space constraints (i.e. memory, processing capabilities, communication latencies, and speeds, and deadlines). An IoT device may consist of several interfaces for communications to other devices, both wired and wireless. These include (i) I/O interfaces for sensors, (ii) interfaces for Internet connectivity, (iii) memory and storage interfaces, and (iv) audio/video interfaces. IoT devices can also be of varied types, for instance, wearable sensors, smart watches, LED lights, automobiles and industrial machines. Almost all IoT devices generate data in some form of the other which when processed by data analytics systems generate leads to useful information to guide further actions locally or remotely, For instance, sensor data generated by a soil moisture monitoring device in a garden, when processed can help in determining the optimum watering schedules.

Communication: The communication block performs the communication between devices and remote servers. IoT communication protocols generally work in data link layer, network layer, transport layer, and application layer.

Services: An IoT system serves various types of functions such as services for device modeling, device control, data publishing, data analytics, and device discovery.

Management: Management block provides different functions to govern an IoT system to seek the underlying governance of IoT system.

Security: Security functional block secures the IoT system by providing functions such as, authentication, authorization, privacy, message integrity, content integrity, and data security.

Application: Application layer is the most important in terms of users as it acts as an interface that provides necessary modules to control, and monitor various aspects of the IoT system. Applications allow users to visualize, and analyze the system status at present stage of action, sometimes prediction of futuristic prospects.

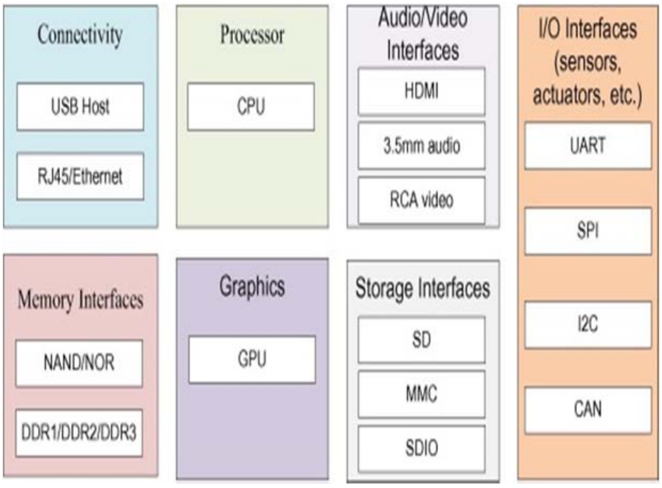

Figure 1. IoT device components.

3. Computing Technology:

It consist of hardware and software platforms. It is evident that most of the IoT solutions include both custom hardware and software. It is also to be noted that some of the solutions are not available for immediate purchase but are on the way to the market (e.g. pre-order). In terms of communication, WiFi and Bluetooth are the most commonly used protocols. Additionally, an increasing number of the IoT solutions support more than one platform (e.g. Android, iOS, browser-based, Windows, Linux, and Mac). Mostly, they are built around the Android and iOS platforms. Most of the solutions are protected under a commercial license and both software and hardware are closed-source. The majority of the IoT solutions are sold as units. Though solutions may have both software and hardware components, the price is mainly for the hardware and the accompanying software is free. The only exceptions are solutions that are completely based on the cloud, where they charge for subscription. In most of the wearable solutions, smart phones are used as an interface for human–system interaction. Smart wearable solutions generally have two or three components. Custom designed wearable devices are used to capture the context and sense the phenomena. Then, either processed or raw data is sent to a processing device, which is usually a smart phone (or a device with a similar computational capability). The smartphone then visualises and presents the outcome (e.g. alerts and notifications) to the users. One such example is Lumoback,which tracks posture and daily activities in real time Lumoback collects data through a wearable waist belt and pushes the data directly to the smartphone. Human Computer Interaction (HCI) plays a significant role in the success of IoT products and solutions. When combining different interaction mechanisms, IoT product designers will need to select the right combination of methods based on number of different factors such as data processing and communication capability, energy, hardware cost, target user knowledge, criticality of the product and so on. Commonly available options are gesture, voice, touch.[2]

4. Communication Technology:

Sensors may send data to custom gateway devices and then push to the cloud over GSM or WiFi. In such situations, cloud services push the outcome to a mobile device to update the user on the real-time activities. For example, Mimobaby is a baby movement monitoring wearable solution. Mimobaby collects data from sensors attached to the baby’s clothes. Then, it transfers the data to a nearby custom gateway which uses home WiFi connectivity to push the data to the cloud. Then, the cloud services alert the parents’ smartphone in real-time. Figure 2 illustrates some of the most common communication patterns used in the IoT solutions. Data collected by the IoT solutions may be sent to the cloud for further processing, historical archiving, or pattern recognition. Mobile devices allow users to immediately take action or perform actuation tasks. In such circumstances, the communication between the hardware and the mobile devices is performed using short distance communication protocols, such as Bluetooth, and long range communication tasks are performed via WiFi or GSM. Smart Objects Smart Phone Cloud Platform Galway Device Consumers 1 1 2 2 2 3 3 3 3 3 Fig. 2. There are mainly three types of common patterns It is also evident that cloud IoT platforms are trying to build their own ecosystems by facilitating and supporting third party extensions (also called plugins) development and distribution through app store. We have repeatedly seen such trends in both PC market and smartphone markets. IoT platform developers are increasingly support non-technical people to build IoT solutions by providing easy ways to assemble the components without programming knowledge.

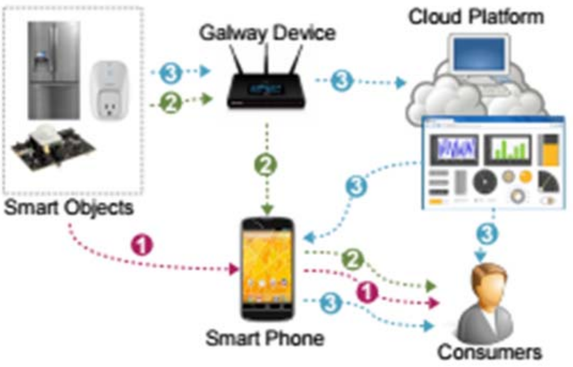

Figure 2: Common Communication Patterns in IoT Applications.

5. Identification Technology:

Each object should be identifiable. Depending on the specific scenarios, objects may require to be uniquely identified, or to be identified as belonging to a given class (e.g., this object is a pen, regardless of which pen it is). This could be done basically in two ways. The first one is to physically tag one object by means of RFIDs, QR code or similar. In such a way an object can be ‘‘read’’ by means of an appropriate device, returning an identifier that can be looked up in a database for retrieving the set of features (description) associated to it. The second possibility is to provide one object with its own description: if equipped with wireless communication means, it could communicate directly its own identity and relevant features. These two approaches are not mutually exclusive, and can complement each other. RFID-based identification is indeed cheaper in terms of requirements on the electronics to be embedded in objects, but requires the possibility for the ‘‘reader’’ to access a database where information about such an object is stored. The self description- based approach, on the contrary, relaxes the requirements to access to a global database, but still requires to embed more electronics into everyday objects. Identification and proximity detection schemes that make use of inexpensive RFIDs became recently a promising choice for commercial deployments in the logistics field. The most popular type of RFIDs are passive tags, which do not contain an on-board power source: energy for operation is supplied by the RFID interrogation signal itself. Conversely, active tags have an on-board power source that feeds the on-board receiver and transmitter, allowing for an increased radio range. Semi-active and semi-passive RFIDs differ in that the on-board power source is used to feed the microchip, whereas transmission is either active (semi-active) or performed using back-scattering (semi-passive). Several vendors propose proprietary middleware platforms that have been developed with the aim to support commercial deployments of RFIDs; see for example the SAP Auto-ID Infrastructure. Other platform include the Siemens RFID Middleware, Sun Java System RFID Software or the IBM WebSphere RFID.

6. Observation

Several domain specific IoT based architectural works have been discussed. While reviewing different areas of implementations, it is found that smart city related practices are dominant over other segments. Fig.3 illustrates the graphical representation of the rate of practice versus domains of IoT architectures. On the basis of research papers included in this survey, the graph has been plotted; where RFID and health related architectural studies are getting equally popular around at 11%. SoA based architectural research is gradually coming forwards faster than RFID and health sectors, making its mark at 12.5%. WSN being a common area of practice has secured 13.3% among all. Smart city and related applications are gaining popularity in recent days. The result shows that 16.5% of overall research has been performed collectively toward the development for in smart society only. Indeed the smart society approach touches the highest point on the plot. Cloud computing based research and practices seem to be just beyond of WSN i.e., 14%. SCM and industrial approaches are subsequently marking its position in IoT specific world. SCM secures 8.6% on the graph. Security and privacy issues are very important by its own virtue; hence researchers are coming up with novel architectural concepts to facilitate the IoT. 7% investigations are made on its behalf. Social computing based research is still at nascent stage[2]. Very few and specific explorations have been made on this ground. It has attained only 4.7%. The graphical representation of current trends in IoT based architectural research shows that more facilitation to be incurred in several domains, such as: e-learning, defense rural management, and robotics are yet to be touched. The representation of this table conglomerates different types of architectural frameworks as per their sub-domain. This will help the researchers to go into the depth of what is described in this paper as the sub-domains or domains as a whole, that need to be searched in future.

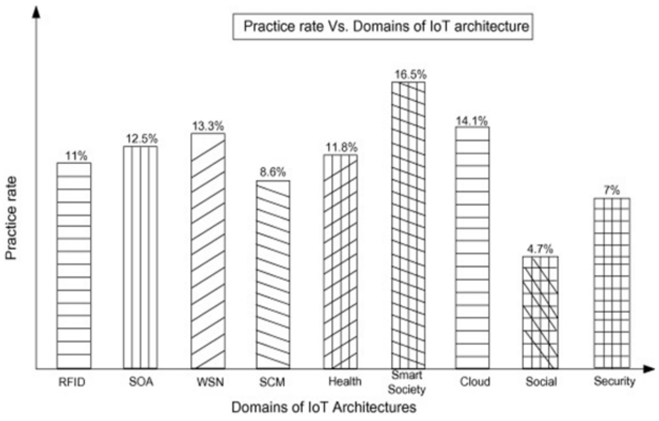

Figure 3: Observation chart of some domains of IoT

7. CONCLUSION

In this paper we tried to refer some computing, communication and identification techniques used for IoT. The Internet-of-Things may represent the new development ahead in the ICT sector. The possibility of merging the real and the virtual world, through the massive deployment of embedded devices & internet opens up new exciting areas for research sections and business. In this survey article, we provided an overview of computing, communication and identification techniques used for IoT. Some observations seen to be very useful for surveying the IoT techniques. We do hope that this survey will be useful for researchers and practitioners in the field, helping them to understand the huge development areas of IoT and what are the major issues to be overcome while devising innovative technical solutions.

REFERENCES

[1] Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. Journal of Cyber Security and Mobility, 1(4), 309-348.

[2] Daniele Miorandi Sabrina Sicari Francesco De Pellegrini Imrich Chlamtac, "Internet of things: Vision, applications and research challenges", Elsevere publisher Ad Hoc Networks 10 (2012) 1497–1516.

[3] C. Decker et al., Cost–benefit model for smart items in the supply chain, in: Proceedings of IOT Conference, Zurich, Switzerland, 2008, pp. 155–172.

[4] O.B. Akan, M.T. Isik, B. Baykal, Wireless passive sensor networks, IEEE Commun. Mag. 47 (2009) 92–99.

[5] I. Akyilidiz, F. Brunetti, C. Blazquez, Nanonetworking: a new communication paradigm, Comput. Netw. 52 (12) (2008) 2260–2279.

[6] H. Liu, M. Bolic, A. Nayak, I. Stojmenovic, Taxonomy and challenges of the integration of RFID and wireless sensor networks, IEEE Netw. 22 (2008) 26–35.

[7] Michael Braun, Erwin Hess, and Bernd Meyer. Using elliptic curves on RFID tags. International Journal of Computer Science and Network Security, 8(2), 2008.

[8] L. Zhang, Z. Wang, Integration of RFID into wireless sensor networks: architectures, opportunities and challenging problems, in: Proceedings of GCCW, 2006, pp. 463–469.

[9] V. Raghunathan, S. Ganeriwal, M. Srivastava, Emerging techniques for long lived wireless sensor networks, IEEE Commun. Mag. 44 (2006) 108–114.

[10] ITU-T Internet Reports, Internet of Things, November 2005.