SURVEY: ESSENTIALITYOF THE INTERNET OF THING (IoT)

Yukti Varshney

Assistant Professor, Computer Science Department, Apex Institute of Technology, U.P., India

ABSTRACT

This paper presents Internet of Things in a wider context. Main enabling factor of this concept is the integration of various technologies. In this paper, we describe the key technologies involved in the implementation of Internet of Things and the major application domain where the Internet of Things will play a vital role. Later we will discuss about the open issues which are to be addressed before the worldwide acceptance of these technologies. There are lots of open issues to address. Here we address the most relevant among them in detail.

Keyword - Internet of things, Concept of IoT, applications, Enabling technologies, architectures.

1. INTRODUCTION

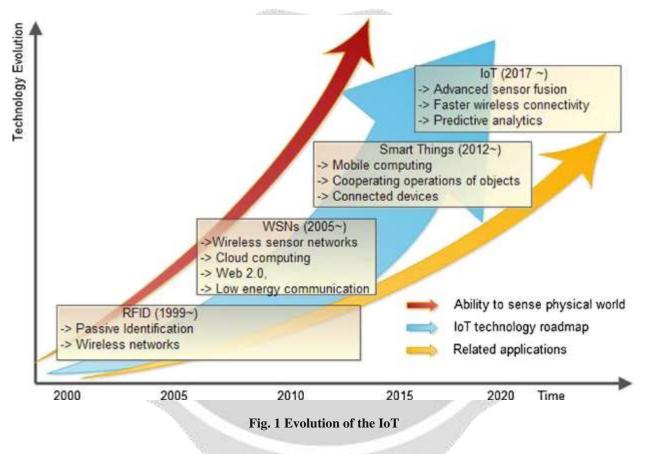
Pretz has indicated that the Internet of things (IoT) is a things connected network, where things are wirelessly connected via smart sensors (Pretz 2013); IoT is able to interact without human intervention. Some preliminary IoT applications have been already developed in healthcare, transportation, and automotive industries (He et al. 2014; Joshi and Kim 2013; Pretz 2013). Currently, IoT technologies are at their infant stages; however, many new developments have occurred in the integration of objects with sensors in the cloud-based Internet (Hepp et al. 2007; Joshi and Kim 2013; Pretz 2013). The development of IoT involves many issues such as infrastructure, communications, interfaces, protocols, and standards. We are motivated to summarize the research progress achieved so far in the development, standardization, and security assurance of IoT enabling technologies, and to identify critical research topics and future research directions of IoT.

1.1 The concept of IoT

Kevin Ashton firstly proposed the concept of IoT in 1999, and he referred the IoT as uniquely identifiable interoperable connected objects with radio-frequency identification (RFID) technology. However, the exact definition of IoT is still in the forming process that is subject to the perspectives taken (Hepp et al. 2007; Joshi and Kim2013; Pretz 2013). IoT was generally defined as "dynamic global network infrastructure with self-configuring capabilities based on standards and interoperable communication protocols; physical and virtual 'things' in an IoT have identities and attributes and are capable of using intelligent interfaces and being integrated as an information network" (IERC 2013; Kirtsis 2011; Li et al. 2012a, b). Basically, the IoT can be treated as a superset of connecting devices that are uniquely identifiable by existing near field communication (NFC) techniques (ETSI 2013).

The words "Internet" and "Things" mean an inter-connected world-wide network based on sensory, communication, networking, and information processing technologies, which might be the new version of information and communications technology (ICT) (Kranenburg 2013; Marry 2013). Despite the argument on the definition of IoT, it has been discussed widely and corresponding technologies have been rapidly developed by various institutions (Guo et al. 2012; Hepp et al. 2007; ITU 2013; Li et al. 2013b; Pretz 2013); in particular, intelligent sensing and wireless communication techniques have become part of the IoT and new challenges and research horizons have emerged (Hunter et al. 2012; Wilamowski 2010). The International Telecommunication Union (ITU) discussed the enabling technologies, potential markets, and emerging challenges and the implications of the IoT (Frenken et al. 2008; ITU 2013). The evolvement of IoT can be illustrated by several phases as shown in Fig. 1. The IoT is initiated by the use of RFID technology, which is increasingly used in logistics, pharmaceutical production, retail, and diverse industries (Fielding and Taylor 2002; Guinard et al. 2010; Guinard et al. 2009; Xu 2011b).

The emerging wirelessly sensory technologies have significantly extended the sensory capabilities of devices and therefore the original concept of IoT hence is extending to ambient intelligence and autonomous control. To date, a number of technologies are involved in IoT, such as wireless sensor networks (WSNs), barcodes, intelligent sensing, RFID, NFC, low energy wireless communications, cloud computing, and so on (Jiang et al. 2014; Kataev et al. 2013; Li et al. 2013a; Ren et al. 2012; Tao et al. 2014a, b; Wang et al. 2014). Evolutions of these technologies bring new technologies to IoT (Deng et al. 2010; Kranenburg and Anzelmo 2011; Li et al. 2012a, b; Malatras et al. 2008; Miorandi et al. 2012; Pautasso and Wilde 2009; Peris-Lopez et al. 2006; Vermesan 2013; Wang 2012). The IoT describes the next generation of Internet, where the physical things could be accessed and identified through the Internet. Depending on various technologies for the implementation, the definition of the IoT varies. However, the fundamental of IoT implies that objects in an IoT can be identified uniquely in the virtual representations. Within an IoT, all things are able to exchange data and if needed, process data according to predefined schemes.



1.2 Current research

In the last decade, the RFID-based identification has been widely used in logistics, retail, and pharmaceutics. Since 2010 (Kranenburg and Anzelmo 2011; Malatras et al. 2008; Miorandi et al. 2012), with the advances in intelligent sensors, low energy wireless communication, and sensor network technologies, a large number of 'things' can be networked as an IoT (Li and Liu 2012; Welbourne et al. 2009). To provide better services to end-users or applications, the technical standards should be designed for IoT in terms of the specifications of data exchange, processing, and communications within the network. The success of IoT depends on the standardization, which provides interoperability, compatibility, reliability, and effectiveness of the operations on a global scale. Objects in an IoT must be able to communicate and exchange data with each other autonomously (Juels 2006; Mitrokotsa et al. 2013).

Manifold definitions of Internet of Things traceable within the research community testify to the strong interest in the IoT issue and to the vivacity of the debates on it. By browsing the literature, an interested reader might

experience a real difficulty in understanding what IoT really means, which basic ideas stand behind this concept, and which social, economic and technical implications the full deployment of IoT will have.

The reason of today apparent fuzziness around this term is a consequence of the name "Internet of Things" itself, which syntactically is composed of two terms. The first one pushes towards a network oriented vision of IoT, while the second one moves the focus on generic "objects" to be integrated into a common framework. Differences, sometimes substantial, in the IoT visions raise from the fact that stakeholders, business alliances, research and standardization bodies start approaching the issue from either an "Internet oriented" or a "Things oriented" perspective, depending on their specific interests, finalities and backgrounds.

It shall not be forgotten, anyway, that the words "Internet" and "Things", when put together, assume a meaning which introduces a disruptive level of innovation into today ICT world. In fact, "Internet of Things" semantically Means "a world-wide network of interconnected objects uniquely addressable, based on standard communication Protocols" [3]. This implies a huge number of (heterogeneous) objects involved in the process.

The object unique addressing and the representation and storing of the exchanged information become the most challenging issues, bringing directly to a third, "Semantic oriented", perspective of IoT. In Fig. 1, the main concepts, technologies and standards are highlighted and classified with reference to the IoT vision/s they contribute to characterize best. From such an illustration, it clearly appears that the IoT paradigm shall be the result of the convergence of the three main visions addressed above.

The very first definition of IoT derives from a "Things oriented" perspective; the considered things were very simple items: Radio-Frequency Identification (RFID) tags. The terms "Internet of Things" is, in fact, attributed to The Auto-ID Labs [4], a world-wide network of academic research laboratories in the field of networked RFID and emerging sensing technologies. These institutions, since their establishment, have been targeted to architect the IoT, together with EPCglobal [5]. Their focus has primarily been on the development of the Electronic Product CodeTM (EPC) to support the spread use of RFID in world-wide modern trading networks, and to create the industry-driven global standards for the EPCglobal NetworkTM. These standards are mainly designed to improve object visibility (i.e. the traceability of an object and the awareness of its status, current location, etc.). This is undoubtedly a key component of the path to the full deployment of the IoT vision; but it is not the only one.

In a broader sense, IoT cannot be just a global EPC system in which the only objects are RFIDs; they are just a part of the full story! And the same holds for the alternative Unique/Universal/Ubiquitous Identifier (uID) architecture [6], whose main idea is still the development of (middleware based) solutions for a global visibility of object in an IoT vision. It is the authors' opinion that, starting from RFID centric solutions may be positive as the main aspects stressed by RFID technology, namely item traceability and addressability, shall definitely be addressed also by the IoT. Notwithstanding, alternative, and somehow more complete, IoT visions recognize that the term IoT implies a much wider vision than the idea of a mere objects identification.

According to the authors of [7], RFID still stands at the forefront of the technologies driving the vision. This a consequence of the RFID maturity, low cost, and strong support from the business community. However, they state that a wide portfolio of device, network, and service technologies will eventually build up the IoT. Near Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN) together with RFID are recognized as "the atomic components that will link the real world with the digital world". It is also worth recalling that major projects are being carried out with the aim of developing relevant platforms, such as the WISP (Wireless Identification and Sensing Platforms) project.

The one in [7] is not the only "Things oriented" vision clearly speaking of something going beyond RFID. Another one has been proposed by the United Nations, which, during the 2005 Tunis meeting, predicted the advent of IoT. A UN Report states that a new era of ubiquity is coming where humans may become the minority as generators and receivers of traffic and changes brought about by the Internet will be dwarfed by those prompted by the networking of everyday objects [8].

2. ENABLING TECHNOLOGIES

2.1 Identification and tracking technologies

The concept of IoT was coined based on the RFID-enabled identification and tracking technologies. A basic RFID system is composed of an RFID reader and an RFID tag. Due to its capability to identify, trace, and track, the RFID system has been widely applied in logistics, such as package tracking, supply chain management, healthcare applications, etc. (Krapelse 2013; Lam and Ip 2012; Li 2012; Xu 2011b). A RFID system could provide sufficient

3961

real-time information about things in IoT, which are very useful to manufacturers, distributors, and retailers. For example, RFID application in supply chain management can improve inventory management. Some identified advantages include reduced labour cost, simplified business processes, and improved efficiency. Recently, it was reported that 3 % EU companies are using RFID (Kranenburg and Anzelmo 2011). In the RFID-based applications, 56 % for access control, 29 % for supply chain, 25 % for motorway tolls, 24 % for security control, 21 % product control, and 15 % for asset management. The next generation of RFID technology will focus on the item level RFID usage and RFID-aware management issues. Although RFID technology is successfully used in many areas, it is still evolving in developing active systems, Inkjet-printing based RFID, and management technologies (Hepp et al. 2007). Other identified problems need to be solved for using in IoT, include:

- Collision of RFID readings. It covers the collisions between RFID readers or RFID tags and multiple reads of the same RFID tag.
- Signal Interferences. Interference occurs within an RFID system or with other radio-based devices.
- Privacy Protection. It covers customer privacy and the confidentiality of RFID tags that can be scanned by authorized RFID scanners.
- Standards. Universally applicable standards are still lacking for RFIDs.
- Integration. The integration of RFID and smart sensors.

2.2 Integration of WSN and RFID

Many types of intelligent sensors have been developed based on physical principles of infrared, γ -ray, pressure, vibration, electromagnetic, biosensor, and X-ray. Data from those sensors in IoT can be acquired and integrated for analysis, decision-making, and storage. Examples of RFID integrated sensors are On/Off-board locating sensor, sensor tags, independent tag and sensor devices, and RFID reading systems

(Pretz 2013; Miorandi et al. 2012).

The integration of sensors and RFID empowers IoT in the implementations of industrial services and the further deployment of services in extended applications. IoT integrating with RFID and WSNs makes it possible to develop IoT applications in healthcare, decision-making of complex systems, and smart systems such as smart transportation, smart city, or smart rehabilitation systems (Fan et al. 2014).

2.3 Communications

Hardware devices involve very diversified specifications in terms of communication, computation, memory, and data storage capacity, or transmission capacities. An IoT application consists of many types of devices. All types of hardware devices should be well organized through the network and be accessible via available communication. Typically, devices can be organized by gateways for the communication purpose over the Internet.

IoT can be an aggregation of heterogeneous networks, such as WSNs, wireless mesh networks, mobile networks, and WLAN (Chi et al. 2012). These networks help the things in fulfilling complex activities such as decision-makings, computation, and data exchange. In addition, the reliable communication between gateway and things is essential to make a centralized decision with respect to IoT. The gateway is capable of running the complicate optimization algorithm locally by exploiting its network knowledge. The computational complexity is shifted from things to the gateway; the global optimal route and parameter values for the gateway can be obtained.

This is feasible since the size of the gateway domain is in the order of a few of tens in comparison with the sizes of things. Hardware capabilities and the communication requirements vary from one device type to another. The things in IoT can have very different capabilities for computation, memory, power, or communication. For instance, a cellular phone or a tablet has much better communication and computation capabilities than a single-purpose electronic product such as a heart rate monitor watch. Similarly, things can have very different requirements of Quality of Service (QoS), in particular, in the aspects of delay, energy consumption, and reliability. For example, minimizing the energy use for communication/computation purposes is a major constraint for the battery powered devices without efficient energy harvesting techniques; this energy constraint is not critical for the devices with power supply connection. IoT would also greatly benefit from the existing protocols in Internet such as IPv6 (Pretz 2013). The commonly used communication protocols and standards include:

- RFID (e.g. ISO 18000 6c EPC class 1 Gen2),
- NFC, IEEE 802.11 (WLAN), IEEE 802.15.4(ZigBee), IEEE 802.15.1(Bluetooth)
- Multihop Wireless Sensor/Mesh Networks

- IETF Low power Wireless Personal Area Networks (6LoWPAN)
- Machine to Machine (M2M)
- Traditional IP technologies, such as IP, IPv6, etc.

2.4 Networks

There exist a lot of cross-layer protocols for Wireless Networks (ETSI 2013; IERC 2013), Wireless Mesh Networks (WMNs) (Fleisch 2013) or Ad Hoc Networks (AHNs) (Marry 2013). However, they cannot be applied to the IoT due to several reasons. First, the heterogeneity of the IoT due to the fact that things have largely diversified hardware configurations, QoS requirements, functionalities, and goals. On the other hand, nodes in aWSN usually have similar hardware specifications, similar communication requirements, and the shared goal. Second, the Internet is involved in the IoT, from which it inherits a centralized and hierarchical architecture. In comparison, WSNs, WMNs and AHNs have relatively flat network architectures: nodes in these networks communicate in a multi-hop fashion and the Internet is not involved.

2.5 Service management

Service management refers to the implementation and management of the services that meet the needs of users or applications. SoA can promote the encapsulation of services. Encapsulation allows the details of services, such as the implementation and the protocols, be hidden behind the instances of services. SoA allows applications to use heterogonous objects as compatible services. On the other hand, the dynamic nature of IoT applications requires that IoT can provide reliable and consistent service; it can benefit from an effective service-oriented architecture to avoid failures from dislocations of device or death of battery.

2.6 Security and privacy

For IoT, security and privacy are two important challenges. To integrate the devices of sensing layer as intrinsic parts of the IoT, effective security technology is essential to ensure security and privacy protection in various activities such as personal activities, business processes, transportations, and information protection (Tan et al. 2013; Wang et al. 2013; Xing et al. 2013). The applications of IoT might be affected by pervasive threats such as RFID tags attacks and data leakage.

In RFID systems, a number of security schemes and authentication protocols have been proposed to cope with security threats. For example, Juels proposed the method of "block tag' to prevent the unauthorized tracing (Juels 2006). On the other hand, low-cost symmetric-key cryptography algorithms, such as Tiny Encryption Algorithm (TEA) and Advance Encryption Standard (AES), have been proposed to protect data exchange. Besides, the low-cost RFID tag has implemented some asymmetric key cryptography algorithm such as Elliptic curve cryptography (ECC) to security. On the other hand, the security protocols developed for WSN can be integrated as an intrinsic part of IoT. The following two aspects require further study: (1) The adaption of the existing Internet standards for interoperable protocols; (2) the security assurance for compensable services. The challenges in security and privacy protection are summarized as resilience to attacks, data authentication, access control, and client privacy.

3. APPLICATONS

IoT enables information gathering, storing and transmitting be available for things equipped with the tags or sensors. The tags have been widely used in supply chain management, manufacturing, environmental monitoring, retailing, smart shelf operations, healthcare, food and restaurant industry, logistic industry, travel and tourism industry, library services, and many other areas (Bi et al. 2014; Cai et al. 2014; Fang et al. 2014; Xu et al. 2014). The IoT is of high importance to economy and society (Li et al. 2012b). To accelerate the applications of IoT, the development of IT infrastructure plays a key role (Xu et al. 2012a, b). It can be foreseen that the IoTwill greatly contribute to address the social issues such as, healthcare monitoring, daily living monitoring, and traffic congestion controlling. IoT makes the interconnected of things amplify the profound effects Currently, IoT has already been deployed in many areas successfully:

- For users, a large number of hardware and software components (RFID tags, mobile phones, social networks, and mobile apps) have been developed for the consumers that allow users to access additional information regarding products.
- For manufacturers, an increasing number of products are made with unique identification technologies, • such as barcodes, RFID tags, intelligent sensors on personal electronic devices, and home appliances. These identification technologies make products be monitored and tracked in their life cycles.
- It can increase the effectiveness of traditional industries by introducing new data exchange and processing techniques.

4.1 Industrial applications

IoT is able to improve the business transactions with smarter service networks, which will significantly improve the efficiency of real-time information processing and manage fine-grained applications, such as online-payment, critical data storage, aggregated QoS, and associated performance indicators. IoT can reduce the gap between components in current digital economy, where services-centric economy is realized through networking transactions. Meanwhile, the business model can benefit from the IoT at the levels of intra- and inter-organizations. Enterprises using IoT can benefit from competitive products, more profitable and greener business models, optimized resources, and real-time information processing.

The globally connected IoT can provide enterprises with the integrated service networks such as the example shown in Fig. 2. Manufacturers could be benefited, IoT enables the business partners to seamlessly integrate the enterprises resources .

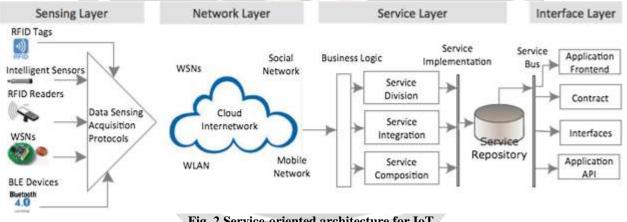


Fig. 2 Service-oriented architecture for IoT

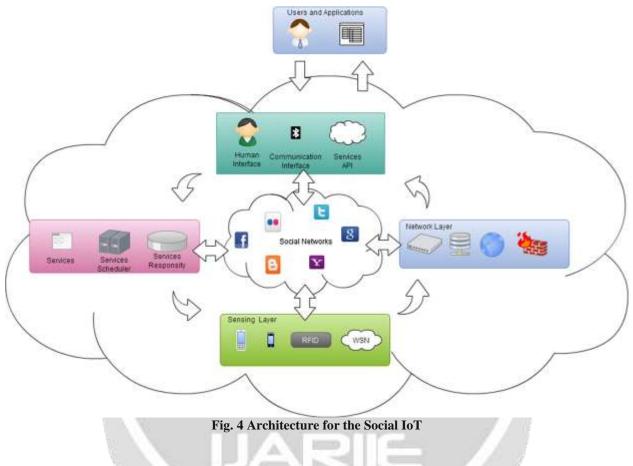
4.2 Social IoT (SIoT)

3961

Recently the idea that integrates IoT with social networks has been proposed (Atzori et al. 2011) and a new paradigm "Social Internet of Things (SIoT)" is proposed to describe a world where things around human being can be intelligently sensed and networked. SIoT can perform things and service discovery effectively and improve the scalability of IoT similar to human social networks. The privacy and protection technologies used in social networks can be implanted into IoT to improve the security of IoT.

The concept of SIoT was motivated by popular social networks over the Internet (Social Internet of Things; Li et al. 2012a, b): Facebook, Twitter, and micro-blog; these networks are permeating people's daily life. Therefore, SIoT has attracted a great deal of attentions from the scientists and researchers in E-business, E-learning, sociology, psychology, and networking. The homophile (Fielding and Taylor 2002) method is proposed to establish higher levels of trust; it can be helpful to optimize relationships among things (EPCglobal 2013; Li et al. 2012a, b). Marry (2013) and Welbourne et al. (2009) discussed the combination of social relationships into the future Internet. Hernandez-Castro et al. (2013) discussed the integration of IoT and existing social networks (such as Facebook, Twitter, etc.). Fielding and Taylor (2002) investigated the potential of SIoT to support novel applications and networking services.

In Fig. 4, an integration scheme of social networking into IoT is described and the system architecture for implementation an SIoT is given.



4. CONCLUSIONS

In the past few years, IoT has been developed rapidly and a large number of enabling technologies have been proposed. The IoT has been the trend of the next Internet. This new field offers a lot of research challenges, but the main goal of this line of research is to make sense of data in any IoT environment It has been pointed out that it is always much easier to create data than to analyze them. With this in mind, new conceptual modelling, (provided by ontologies, semantic, etc.) as well as new paradigms of data mining techniques, will be crucial to provide value and meaning to initially empty data. This paper has surveyed recent progresses on IoT from the perspective of enabling technologies. In particular, the role of SoA in IoT has been introduced and related enabling technologies to implement SoA have been discussed. Existing applications of IoT have been classified into business, social networks and security and surveillance. Finally, open problems and challenges related to IoT have been discussed.

5. ACKNOWLEDGEMENT

The authors can acknowledge any person/authorities in this section. This is not mandatory.

6. REFERENCES

- Alcaraz, C., & Lopez, J. (2010). A security analysis for wireless sensor mesh networks in highly critical systems. IEEE Transactions on Systems, Man, and Cybernetics Part C: Applications and Reviews, 40(4), 419–428.
- [2] Atzori, L., Iera, A.,&Morabito, G. (2011). SIoT: giving a social structure to the internet of things. IEEE Communication Letters, 15(11), 1193–1195.
- [3] Bi, Z., Xu, L., & Wang, C. (2014). Internet of Things for enterprise systems of modern manufacturing. IEEE Transactions on Industrial Informatics. doi:10.1109/TII.2014.2300338. Bluetooth SIG. (2014). Generic Attributed Profile (GATT). Bluetooth SIG Specification, <u>https://www.bluetooth.org/en-us/specification/</u> assigned-numbers/generic-attribute-profile.
- [4] Broll, G., Rukzio, E., Paolucci, M., Wagner, M., Schmidt, A., & Hussmann, H. (2009). Perci: pervasive service interaction with the internet of things. IEEE Internet Computing, 13(6), 74–81.
- [5] Cai, H., Xu, L., Xu, B., Xie, C., Qin, S., & Jiang, L. (2014). IoT-based configurable information service platform for product lifecyclemanagement. IEEE Transactions on Industrial Informatics. doi:10.1109/ TII.2014.2306391.
- [6] Chi, Q., Yan, H., Zhang, C., Pang, Z., & Xu, L. (2012). A reconfigurable smart sensor interface for industrialWSN in IoTenvironment. IEEE Transactions on Industrial Informatics. doi:10.1109/TII.2014. 2306798.
- [7] Ciganek, A., Haseman, W., & Ramamurthy, K. (2014). Time to decisions: the drivers of innovation adoption decisions. Enterprise Information Systems, 8(2), 279–308.
- [8] Dada, A., & Thiesse, F. (2008). Sensor applications in the supply chain: the example of quality-based issuing of perishables. LNCS, 4952, 140–154.
- [9] Deng, R. H., Li, Y., Yung, M., & Zhao, Y. (2010). A new framework for RFID privacy. LNCS, 6345, 1– 18.
- [10] ETSI. (2013). The European Telecommunications Standards Institute, [cited 2013 May 20]; available from http://www.etsi.org/.
- [11] Fan, Y., Yin, Y., Xu, L., Zeng, Y., & Wu, F. (2014). IoT based smart rehabilitation system. IEEE Transactions on Industrial Informatics.doi:10.1109/TII.2014.2302583.
- [12] Fang S., Xu, L., Zhu, Y., Ahati, J., Pei, H., Yan, J., et al. (2014). An integrated system for regional environmental monitoring and management based on Internet of Things. IEEE Transactions on Industrial Informatics. doi:10.1109/TII.2014.2302638.
- [13] Fielding, R. T., & Taylor, R. N. (2002). Principled design of the modern web architecture. ACM Transactions Internet Technology, 2(2), 115–150.
- [14] Fleisch, E. (2013) What is the Internet of things? [cited 2013 May 20]; available from http://www.im.ethz.ch/education/HS10/AUTOIDLABS-WP-BIZAPP-53.pdf.
- [15] Floerkemeier, C., Roduner, C., & Lampe, M. (2007). RFID application development with the Accada middleware platform. IEEE Systems Journal, 1(2), 82–94.
- [16] Frenken, T., Spiess, P., & Anke, J. (2008). A flexible and extensible architecture for device-level service deployment. LNCS, 5377, 230–241.
- [17] Gama, K., Touseau, L., & Donsez, D. (2012). Combining heterogeneous service technologies for building an Internet of Things middleware. Computer Communications, 35(4), 405–417.
- [18] Guinard, D., Trifa, V., Pham, T., & Liechti, O. (2009). Towards physical mashups in the web of things. Proc. IEEE Sixth International
- [19] Conference on Networked Sensing Systems (INSS 09), Pittsburgh, PA, pp.196–199.
- [20] Guinard, D., Trifa, V., Karnouskos, S., & Spiess, P. (2010). Interacting with the SoA-based internet of things: discovery, query, selection, and on-demand provisioning of web services. IEEE Transactions on
- [21] Service Computing, 3(3), 223–235.
- [22] Guo, J., Xu, L. D., Xiao, G., & Gong, Z. (2012). Improving multilingual semantic interoperation in crossorganizational enterprise systems through concept disambiguation. IEEE Transactions on Industrial Informatics, 8(3), 647–658.

BIOGRAPHIES (Not Essential)



Yukti Varshney earned her B.Tech in computer science from SSITM, Aligarh, India in 2008, and the M.Tech in computer science from Shri Venkateshwara University, Gajraula, India in 2015. She is having more than 7 years teaching experience at prestigious institute of U.P. She is currently working as assistant professor in Computer Science Department at Apex Institute of Technology; Rampur, India .She has her research interests include 5G wireless communications, Memory management techniques, Data Mining & sensor system.

