A Field Guide on Internet of Things Research Methodologies

S. Divya Meena*, M. Anitha Mary, M. Mangaleswaran
Department of Computer Science and Engineering, Jansons Institute of Technology, Coimbatore- 641 659
***Corresponding author: E-Mail: divyameena.s@jit.ac.in**

ABSTRACT

One of the buzzwords within the data Technology is Internet of Things (IoT). The longer term is net of Things, which can rework the important world objects into intelligent virtual objects. Wireless communication technologies are advancing at a high rate, enabling time period multimedia system and device services provided by mobile broadband net on devices making a grid network of the web of Things (Hersent, 2011). The IoT paradigm and machine-to-machine (M2M) communication and management are speedily gaining ground in wireless telecommunication (Kortuem, 2010). IoT platforms change heterogeneous resource discovery and information sharing through the formation of communication/virtual networks. Researchers and science-practitioners are presently envision completely different properties for future IoT architectures and also the expectation are increasing regarding what this and future generation of IoT technologies will do to change a large vary of novel applications and structure business models (Ning, 2012).

KEY WORDS: IoT, Machine-to-Machine communication, Virtual networks, Cyber assurance, Cloud computing.

1. INTRODUCTION

Different Definitions - Similar Concepts: IoT is solely the network of interconnected things/devices that area unit embedded with sensors, software, network property and necessary physics that allows them to gather and exchange information creating them responsive (Kranz, 2010). Over a thought net of Things is actually a field framework that permits integration and information exchange between the physical world and pc systems over existing network infrastructure. Many people erroneously think about IoT as associate degree freelance technology (Miorandi, 2012).

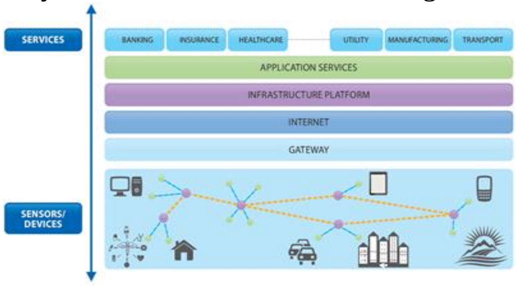

Figure.1. Conceptual IoT framework with Cloud Computing at the centre

The basic elements that build web of things a reality are:

- Hardware-Making physical objects responsive and giving them capability to retrieve information and reply to directions.
- Software-Enabling the info assortment, storage, processing, manipulating and instructing (Tan, 2010).
- Communication Infrastructure-Most necessary of all is that the communication infrastructure that consists of protocols and technologies that change two physical objects to exchange information.

Over the previous few years, the web of Things has attracted vital attention from each trade and domain. An increasing range of IoT merchandise and solutions area unit inbounds within the marketplace, ready to capture vital quantity of data. However, current approaches to explanation insights from such knowledge involve collating giant volumes of information for process (Weber, 2010). This creates vital privacy challenges: to get largest like IoT merchandise and therefore the IoT scheme, we have a tendency to should realize ways in which derive insights from knowledge generated by IoT merchandise while not violating knowledge subjects' privacy. Such privacy protective technologies can facilitate to cut back the public's negative attitudes – heightened following recent revelations regarding numerous government spy programs – towards sharing personal knowledge for common profit (Zhou, 2011).

IoT devices and networks could vary from hand-held mobile devices to a centralized high performance cloud computing setting consisting of heterogeneous communication systems of each military science (mobile, wireless) and glued (wired) communications infrastructures (Roman, 2013). From a data security perspective, the IoT should address the delivery of authentic, accurate, secure, reliable, timely data, notwithstanding threat conditions, over these distributed and heterogeneous computing and communication systems. Cyber-assurance is that the even confidence that IoT networked systems is satisfactorily secured to fulfil operational wants, even within the presence of cyber-attacks, failures, accidents and sudden events.

Internet of Things, as associate degree scheme that interconnects physical objects with telecommunication networks, introduces a tighter association between the cyber area and therefore the physical reality and can develop toward large-scale and present directions, imposing progressively higher necessities on safety, dependability, security, energy-efficiency, performance, lustiness and cost-efficiency (Roman, 2011). It conjointly poses new issues and challenges thanks to its intrinsic feature of huge scale, in terms of spatial and temporal distribution, data quantity, energy consumption, interfaces, functionalities, etc. These new difficult problems are across the disciplines of embedded system, producing, telecommunication, computing, sensing, code engineering, knowledge management and analysis. Rising and advanced communication technologies introduce several new opportunities to tackle the difficult problems in large-scale present IoT. To handle such challenges in large-scale IoT, besides requiring intelligent algorithms for knowledge assortment and analysis, economical network identification and management, we'd like new analytical tools, elementary arithmetic on the far side the scope of ancient communication and data theories, and even methodologies from alternative networking connected fields like economic science, biology, and physics, to shed light-weight on the basic performance limit of huge scale IoT system and to guide the look, implementation, development, and optimisation of rising IoT technologies.

Table.1. Potential IoT applications

Healthcare	Triage, patient monitoring, personnel monitoring, disease spread modelling and containment - real-time health status and predictive information to assist practitioners in the field, or policy decisions in pandemic scenarios
Emergency services and defence	Remote personnel monitoring (health, location); resource management and distribution, response planning; sensors built into building infrastructure to guide first responders in emergencies or disaster scenarios
Crowd monitoring	Crowd flow monitoring for emergency management; efficient use of public and retail spaces; workflow in commercial environments
Traffic management	Intelligent transportation through real-time traffic information and path optimisation
Infrastructure monitoring	Sensors built into infrastructure to monitor structural fatigue and other maintenance; accident monitoring for incident management and emergency response coordination
Water	Water quality, leakage, usage, distribution, waste management
Building management	Temperature, humidity control, activity monitoring for energy usage management, Heating, Ventilation and Air Conditioning (HVAC)
Environment	Air pollution, noise monitoring, waterways, industry monitoring

Cloud centric Internet of Things: The vision of IoT are often seen from two views – Internet ‘centric and Thing ‘centric. The net central design can involve internet services being the most focus whereas knowledge is contributed by the objects. Within the object central design, the sensible objects take the centre stage. In our work, we tend to develop an online central approach. Abstract framework desegregation the ever-present sensing devices and therefore the applications are shown in Figure. So as to comprehend the complete potential of cloud computing furthermore as present Sensing, a combined framework with a cloud at the centre looks to be most viable. This not solely offers the pliability of dividing associated prices within the most sensible manner however is additionally extremely ascendable (Zorzi, 2011). Sensing service suppliers will be part of the network and provide their knowledge employing a storage cloud; analytic tool developers will offer their computer code tools; computing consultants will offer their data processing and machine learning tools helpful in changing data to information and eventually lighting tricks designer offers a spread of visualisation tools. The cloud computing offers these services as Infrastructures, Platforms or computer code wherever the complete potential of human ability are often tapped mistreatment them as services. This in some sense agrees with the ubicomp vision of Weiser furthermore as Rogers’s human central approach (Barnaghi, 2012). The info generated, tools used and therefore the visualisation created disappears into the background, sound the complete potential of the net of Things in numerous application domains. As are often seen from Figure four, the Cloud integrates all ends of ubicomp by providing ascendable storage, computation time and different tools to make new businesses. During this section, we tend to describe the cloud platform mistreatment Manjra soft Aneka and Microsoft Azure platforms to demonstrate however cloud integrates storage, computation and visualisation paradigms. Moreover, we tend to introduce a crucial realm of interaction between cloud that is helpful for combining public and personal clouds mistreatment Aneka (Yan, 2012). This interaction is essential for application developers so as to bring detected data, analytics algorithms and visualisation beneath one single seamless framework.

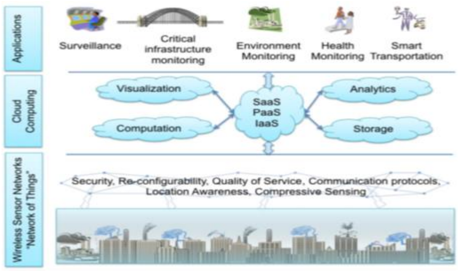

Figure.2. Conceptual IoT framework with Cloud Computing at the centre

However, developing IoT applications victimisation low-level Cloud programming models and interfaces like Thread and MapReduce models is advanced. To beat this limitation, we want associate degree IoT application specific framework for speedy creation of applications and their preparation on Cloud infrastructures (Bassi, 2013).

Open Challenges and Future Directions: The projected Cloud centric vision includes a versatile and open design that's user centric and permits completely different players to act within the IoT framework. It permits interaction in an exceedingly manner appropriate for his or her own needs, instead of the IoT being thrust upon them (Gaglio, 2014). During this method, the framework includes provisions to fulfil completely different needs for knowledge possession, security, privacy, and sharing of data (Su, 2014).

Some open challenges area unit mentioned supported the IoT components conferred earlier. The challenges embody IoT specific challenges like privacy, democratic sensing, information analytics, GIS primarily based visualisation and Cloud computing aside from the quality WSN challenges as well as design, energy potency, security, protocols, and Quality of Service (Uckelmann, 2011). The tip goal is to possess Plug and play good objects which might be deployed in Associate in nursing setting with a practical backbone permitting them to mix with alternative good objects around them. Standardization of frequency bands and protocols plays a polar role in accomplishing this goal (Sun, 2010). A roadmap of key developments in IoT analysis within the context of pervasive applications is shown in Figure nine, which incorporates the technology drivers and key application outcomes expected within the next decade. The section ends with a couple of international initiatives within the domain that may play a significant role within the success of this chop-chop rising technology (Kotis, 2013).

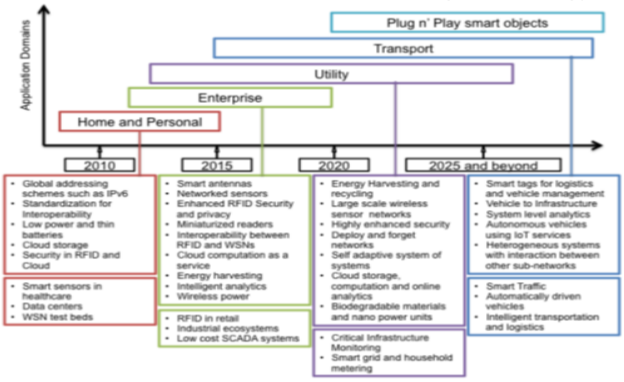

Figure.3. Roadmap of key technological developments in the context of IoT application domains

2. SUMMARY AND CONCLUSIONS

IoT has been gradually bringing a sea of technological changes in our daily lives, which in turn helps to making our life simpler and more comfortable, though various technologies and applications. There is innumerable usefulness of IoT applications into all the domains including medical, manufacturing, industrial, transportation, education, governance, mining, habitat etc. Though IoT has abundant benefits, there are some flaws in the IoT governance and implementation level. The key observations in the literature are that; a) There is no standard definition in worldwide, b) Universal standardizations are required in architectural level, c) Technologies are varying from vendor-vendor, so needs to be interoperable, d) For better global governance, we need to build standard protocols.

REFERENCES

Barnaghi P, Wang W, Henson C and Taylor K, Semantics for the Internet of Things, Early progress and back to the future, International Journal on Semantic Web and Information Systems (IJSWIS), 8 (1), 2012, 1-21.

Bassi A, Enabling things to talk, Designing IoT solutions with the IoT architectural reference model, Heidelberg, Springer, 2013.

Gaglio S and Lo R, Advances onto the Internet of Things, How ontologies make the Internet of Things meaningful, Cham, Springer, 2014.

Gubbi J, Buyya R, Marusic S and Palaniswami M, Internet of Things (IoT), A vision, architectural elements, and future directions, Future Generation Computer Systems, 29 (7), 2012, 1645-1660.

Hersent O, Boswarthick D and Elloumi O, The Internet of Things, Key applications and protocols, Hoboken, John Wiley & Sons, 25 (9), 2011, 70-84.

Kortuem G, Kawsar F, Sundramoorthy V and Fitton D, Smart objects as building blocks for the Internet of Things, IEEE Internet Computing, 14 (1), 2010, 44-51.

Kotis K and Katasonov A, Semantic interoperability on the Internet of Things, The semantic smart gateway framework, International Journal of Distributed Systems and Technologies (IJDST), 4 (3), 2013, 47-69.

Kranz M, Holleis P and Schmidt A, Embedded interaction, Interacting with the Internet of things, IEEE Internet Computing, 14 (2), 2010, 1230-1241.

Miorandi D, Sicari S, De P and Chlamtac I, Internet of things, Vision, applications and research challenges, Ad Hoc Networks, 10 (7), 2012, 1497-1516.

Ning H and Hu S, Technology classification, industry, and education for future Internet of Things, International Journal of Communication Systems, 25 (9), 2012, 1230-1241.

Roman R, Najera P and Lopez J, Securing the Internet of things, Computer, 44 (1), 2011, 51-58.

Roman R, On the features and challenges of security and privacy in distributed Internet of things, Computer Networks, 57 (10), 2013, 2266-227.

Su X, Riekki J, Nurminen J and Koskimies M, Adding semantics to Internet of Things, Hoboken, Wiley, 2014.

Sun Q.B, Liu J, Li S, Fan C and Sun J, Internet of things, Summarize on concepts, architecture and key technology problem, Journal of Beijing University of Posts and Telecommunications, 33 (3), 2010, 1-9.

Tan L and Wang N, Future Internet, The Internet of Things, Advanced Computer Theory and Engineering (ICACTE), 5 (1), 2010, 376-380.

Uckelmann D, Harrison M and Michahelles F, Architecting the Internet of things, Berlin, Springer, 2011.

Weber R, Internet of Things – New security and privacy challenges, Computer Law & Security Review, 26 (1), 2010, 23–30.

Yan L, The Internet of things, From RFID to the next-generation pervasive networked systems, New York, Auerbach Publications, 17 (6), 2012, 34-45.

Zhou X, Short sign-cryption scheme for the Internet of things, Informatica, 35 (4), 2011, 521-530.

Zorzi M, Gluhak A, Lange S, and Bassi A, From today's Intranet of things to a future Internet of things, A wireless- and mobility-related view, IEEE Wireless Communications, 17 (6), 2010, 44-51.