Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 4, April-2017

Research Perspectives for IOT in Real Life Scenario

R. M. Hushangabade[1], S. V. Kalbande[2], P. V. Dudhe[3], A. A. Gulhane[4]

[1]*Prof Ram Meghe Institute of Technology & Research, Badnera*
[2]*Prof Ram Meghe Institute of Technology & Research, Badnera*
[3]*Prof Ram Meghe Institute of Technology & Research, Badnera*
[4]*Prof Ram Meghe Institute of Technology & Research, Badnera*

***Abstract* —many technical societies are enthusiastically pursuing research that adds to the Internet of Things (IoT). Today, as sensing, actuation, communication, and control become ever more sophisticated and everywhere, there is significant overlap in these society, sometimes from slightly different view point. More support between communities is encouraged. To provide a basis for discussing open research problems in IoT, a vision for how IoT could change the world in the far-off future is first presented**

***Keywords*- Cyber Physical Systems, Internet of Things, Mobile Computing, Pervasive Computing, Wireless Sensor Networks.**

INTRODUCTION

Smart devices, Smartphone's, Smart cars, Smart homes. Smart cities, a smart world. These ideas have been promoted for many years. Achieving these goals has been investigated, to date, by many diffrent and often displaces research societies. Five such prominent research communities are: Internet of Things (IoT), Mobile Computing (MC), Wireless Sensor Networks (WSN), Pervasive Computing (PC) and most recently, Cyber Physical Systems (CPS). However, as technology and solutions progresses in each of these fields there is an escalating overlap and combination of principles and research questions. Narrow definitions of these fields are no longer suitable. Further, research in Internet of Things, PC, MC, WSN and CPS often depend on fundamental technologies such as real-time computing, machine learning, security, privacy, signal processing, big data, and others. as a result, the *smart vision of the world* involves much of computer science, electrical engineering and computer engineering and Greater connections among these communities will pace growth.

I.VISION AND IOT SCOPE

By the perspective that cities and the globe itself will be overlay with sensing and actuation, many embedded in "things" introducing what is called to as a smart world. But it is vital to keep note that single key issue is the measure of the density of sensing and actuation exposure. At that time there will be a qualitative change. For example, today many infrastructures already equipped sensors for attempting to conserve energy [7]; home automation is occurring [3]; cars, taxis, and traffic lights have devices to try and improve safety and transportation [9]; people have smart phones with sensors for running many useful apps [2]; etc. However, all of these are just the tip of the iceberg. They are all still at initial phases of development. The steady increasing density of sensing and the sophistication of the associated processing will make for a significant qualitative change in how we work and live. We will truly have systems-of-systems that synergistically interact to create totally novel and difficult to predict services. What will be the backbone that supports such a vision? One solution is a global sensing and actuation service attached to the Internet. Electricity and water are two services that can be utilized for a numerous of purposes. By means of IoT platform Sensing and actuation will become a utility. IoT can't be seen as individual systems, but as a integrated infrastructure on which many applications and services can execute. Some applications will be personally customized such as digitization of daily life activities, others will be city-wide such as effective, delay-free transport service, and others will be over the globe such as global delivery systems. In cities Smart buildings will not only control energy or security, but integrate energy savings, personal comfort, health and security and wellness aspects into suitable and efficient spaces.

II.RESEARCH

The field of research required to accomplish IoT at the level desired above requires major research along many directions. In this section research are highlighted in topic areas: massive scaling, architecture and dependencies, robustness, openness, security, privacy. Each of the topic discussions primarily focuses on new problems that arise for future IoT systems.

All Rights Reserved, @IJAREST-2017

A. Massive Scaling

The current path of the numbers of smart devices being laid down proves that ultimately trillions of things will be on the Internet. How to name, maintain, authenticate access, use, protect, and support such a huge scale of things are daunting problems. Will IPv6 is sufficient? Will protocols such a 6LowPAN useful? Will complete new standards and protocols emerge? Since many of the things on the Internet will require battery powered energy source, will energy saving and extremely low power circuits rule out the need for batteries? How will the extremely massive amounts of data be collected, fetched, and stored? How will the real-time and reliability points be addressed [5][13]? How will devices including mobile devices be registered? Many protocols and variations will simultaneously exist. What will be the architectural backbone that compatible with the expected heterogeneity of devices and applications?

B. Architecture and Dependencies

As huge amount of things are connected to the Internet it is vital to have an adequate architecture that permits easy connectivity, control, communications, and useful applications. How will these things communicate in and across applications [37]? Many times, things or sets of things must be disjoint and protected from other devices. In other scenario it makes sense to share devices and information. One feasible architectural approach for IoT is to borrow from the Smartphone world [2][4]. Smartphone's employ an approach where applications are implemented and made available from an app store. This has many advantages including an unrestrained development of novel applications that can execute on the smart phones. Various standards and automatic checks mechanisms are made sure that an app can execute on a given platform. For example, the correct version of the underlying operating system and the required sensors and actuators can be checked when the app is installed [12]. A same architectural approach for IoT would also have same advantages. However, the fundamental platform for IoT is much more complex than for smartphones. Nevertheless, if IoT is based on an fundamental sensor and actuator network that plays role as a utility similar to electricity and water, then, different IoT applications can be used with this utility. While each application must provide solution to its own problems, the sharing of a sensing and actuation utility across multiple parallel running applications can result in many systems-of-systems interference issues, especially with the actuators. Reasons for Interferences are many , but initially when the web depends on assumptions about the working environment, the H/W platform, naming, requirements, control and various device semantics. Earlier work, has considered relatively easy dependencies related to numbers and versions of underlying operating systems, types of parameters and availability of correct underlying hardware. Research is needed to develop a complete approach to defining, detecting, and solving dependencies across applications. This is especially vital for safety sensitive applications or when actuators are harmful.

III. ROBUSTNESS

If our vision is correct, many IoT applications will be work on a deployed sensing, actuation, and communication platform connecting a network of things. In these design it is common for the devices to know their locations, have synchronized clocks, know their neighboring devices when working with each other, and have a same set of parameter settings such as consistent wake-up and sleep routines, suitable power levels for communication, and pair-wise security key mechanism. However, over time these conditions can become less useful. The most common and simple example of this deterioration problem is with clock synchronization problem [15]. Over time, clock drift causes nodes to have different enough times to result in failures. While it is widely known that clock synchronization is re-occurring process, this principle is much more usual. For example, some nodes may be physically moved. More and more nodes may become lost over time. To make system-wide node locations coherent again, node localization needs to repeated and done albeit at a much slower rate than clock sync. This problem can be considered a type of entropy where a system will deteriorate lean towards disorder unless energy in the form of re-running protocols and other self-remedial mechanisms is applied [12]. Note that control of actuators can also deteriorate due to protocols and controlling software, but also due to physical deterioration. In other words, the required coherence services must put together with many other ways to produce strong system operation. This includes formal methods to develop reliable code, in-situ debugging techniques, on-line fault tolerance, in-field- maintenance, and general health monitoring services [10]. These problems get worst due to the unnoticed operation of the system, the need for a long lifespan, the openness of the systems, and realities related to physical world. The objective is for this collection of solutions to create a state of art robust system in spite of faulty, noisy, and non-deterministic underlying physical world realities.

IV.OPENNESS

Usually, the greater part of sensor based systems have been closed systems. For example, cars, airplanes and ships have had networked sensor systems that operate largely inside that vehicle. But, these systems' capabilities are expanding speedily. Cars are on their own sending maintenance information and planes are sending real-time jet engine information to its creators. There is or will be even superior mutual aid and 2-way control on a wide scale: cars planes communicating to each other and controlling each other to stay away from collisions, humans exchanging important data automatically when they meet up and this possibly affecting their next plan of actions, and physiological data uploaded to doctors in real-time with real-time feedback from the doctor. These systems require ingenuousness to achieve these benefits. On the other hand, supporting openness creates many new research tribulations. All of our in progress composition techniques,

All Rights Reserved, @IJAREST-2017

analysis techniques and tools need to be re-thought and developed to account for this openness. New combined communications interfaces will be required to enable resourceful information exchange across different systems. Certainly, openness also causes trouble with security and privacy. Therefore, openness must provide a correct balance between access to functionality and security and privacy.

V. SECURITY

A primary problem that is omnipresent in the Internet today that must be solved is dealing with security attacks [14]. Security attacks are tricky for the IoT because of the minimum capacity "devices" (things) is being used, the physical convenience to sensors, actuators and objects, and the openness of the systems, including the fact that most devices will communicate with wireless means. The security problem is further improved because temporary and enduring accidental failures are everyday and failures are vulnerabilities that can be broken by attackers. However, the substantial redundancy that is available creates probable for scheming applications to continue to provide their particular services even in the face of failures. To meet practical system requirements that obtain from long lived and unattended operation, IoT applications must be able to keep operate adequately in the presence of, and to recover efficiently from security attacks. Solutions may require downloading new code [10] and this itself is open to security attacks. The system must also be able to become accustomed to new attacks when the system was first deployed. To heal from security attacks, a system needs to detect the attack, diagnose the attack, and imply remedies and repairs, but perform all of this in a trivial manner due to the types of low capacity devices involved.

VI. PRIVACY

The ubiquity and communications involved in IoT will provide many amenities and useful services for individuals, but also create many opportunities to abuse privacy. To solve the privacy problem created by IoT applications of the future, the privacy policies for each system must be specified. Once specified either the entity IoT application or the IoT infrastructure i.e. the utility capability must insist on privacy. Therefore, the IoT prototype must be able to convey user's requests for data access and the policies such that the requests can be evaluated against the policies in order to choose if they should be approved or denied. A new language is required to express privacy policies

VII CONCLUSION

In summing up, one vision of the future is that IoT becomes a service with increased superiority in sensing, actuation, communications, control, and in creating knowledge from huge amounts of data. This will result in qualitatively different lifestyles in the present day. What the lifestyles would be is anyone's guess. It would be fair to say that we cannot forecast how lives will change. We did not foretell the Internet, the Web, social networking, Facebook, Twitter, millions of apps for Smartphone's, etc., and these have all qualitatively changed societies lifestyle. New research problems take place due to the extensive scale of devices, the correlation of the physical and cyber worlds, the openness of the systems of systems, and long-lasting problems of privacy and security. It is there are expectations that there is more collaboration between the research communities in order to solve the countless problems faster as well as to avoid re-inventing the wheel when a particular community solves a problem.

REFERENCES

[1] M1 Security and Automation Controls. http://www.elkproducts.com/m1 controls.html.
[2] Apple app store. http://www.apple.com/osx/apps/app-store.html.
[3] Control4 Home Automation and Control. http://www.control4.com.
[4] http://www.phonearena.com/news/Androids-Google-Playbeats- App-Store-with-over-1-million-apps-now-o_ciallylargestid45680.
[5] T. Abdelzaher, S. Prabh, and R. Kiran, On Real-Time Capacity Limits of ad hoc Wireless Sensor Networks, *RTSS*, December 2004.
[6] Y. Aguiar, M. Vieira, E. Galy, J. Mercantini, and C. Santoni, Refining a User Behavior Model based on the Observation of Emotional States. *COGNITIVE* , 2011.
[7] V. Bradshaw. The Building Environment: Active and Passive Control Systems. John Wiley & Sons, Inc., River Street, NJ, USA, 2006.
[8] B. Brumitt, B. Meyers, J. Krumm, A. Kern, and S. A. Shafer. Easyliving: Technologies for Intelligent Environments. *HUC*, 2000.
[9] G. Burnham, J. Seo G. Bekey, A. Identification of Human Driver Models in Car Following. *IEEE Transactions on Automatic Control 19*, 6, 1974, pp. 911–915.
[10] J. Deng, R. Han, and S. Mishra, Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks, *Proc. of ACM/IEEE IPSN*, 2006. pp. 292-300.
[11] R. Dickerson, E. Gorlin, and J. Stankovic, Empath: a Continuous Remote Emotional Health Monitoring System for Depressive Illness. *Wireless Health* , 2011.

All Rights Reserved, @IJAREST-2017

[12] C. Dixon, R. Mahajan, S. Agarwal, A. Brush, B. Lee, S. Saroiu, and P. Bahl, An Operating System for the Home, *NSDI*, 2012.
[13] T. He, J. Stankovic, C. Lu and T. Abdelzaher, A Spatiotemporal Communication Protocol for Wireless Sensor Networks, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 16, No. 10, Oct. 2005, pp. 995-1006.
[14] M. Huang, J. Li, X. Song, and H. Guo, Modeling Impulsive Injections of Insulin: Towards Artificial Pancreas. *SIAM Journal of Applied Mathematics 72*, 5, 2012, pp. 1524–1548.
[15] M. Kay, E. Choe, J. Shepherd, B. Greenstein, N. Watson, S. Consolvo, and J. Kientz, Lullaby: a Capture & Access System for Understanding the Sleep Environment. *UbiComp*, 2012.

All Rights Reserved, @IJAREST-2017