IJETMR
International Journal of Engineering Technologies and Management Research
A Knowledge Repository

ONGOING CHALLENGES AND RESEARCH OPPORTUNITIES IN INTERNET OF THINGS (IOT)

Sachin Upadhyay [*1]
[*1] Assistant Professor, Department of Mathematical Sciences & Computer Applications, Bundelkhand University, Jhansi (UP), India

Abstract:
The Internet of Things (IoT) opens opportunities for handheld devices, home appliances, and software to share and communicate information on the Internet. Advances in the areas of embedded systems, computing, and networking are leading to an infrastructure composed of millions of heterogeneous devices. These devices will not simply convey information but process it in transit, connect peer to peer, and form advanced collaborations. This "Internet of Things (IoT)" infrastructure will be strongly integrated with the environment. This paper focuses on researching on the architecture and technology of Internet of Things. Moreover, the applications of Internet of Things are interpreted in this paper. We begin with general information security background of IoT and continue on with information security related challenges that IoT will encountered. Finally, we will also point out research directions that could be the future work for the solutions to the security challenges that IoT encounters. The future is Internet of Things, which will transform the real world objects into intelligent virtual objects.

Keywords: *Internet of Things; IoT Applications; Future Technology.*

Cite This Article: Sachin Upadhyay. (2018). "ONGOING CHALLENGES AND RESEARCH OPPORTUNITIES IN INTERNET OF THINGS (IOT)." *International Journal of Engineering Technologies and Management Research,* 5(2:SE), 216-222. DOI: 10.5281/zenodo.1195065.

1. Introduction

The Internet of Things (IoT), sometimes referred to as the Internet of Objects, will change everything including ourselves. The Internet has an impact on education, communication, business, science, government, and humanity [1]. Clearly, the Internet is one of the most important and powerful creations in all of human history and now with the concept of the internet of things, internet becomes more favorable to have a smart life in every aspects [2] .Smart devices. Smartphones. Smart cars. Smart homes. Smart cities. A smart world. These notions have been espoused for many years. Achieving these goals has been investigated, to date, by many diverse and often disjoint research communities. Five such prominent research communities are: Internet of Things (IoT), Mobile Computing (MC), Pervasive Computing (PC), Wireless Sensor Networks (WSN), and most recently, Cyber Physical Systems (CPS). However, as technology and solutions progress in each of these fields there is an increasing overlap and merger of principles and research questions. Narrow definitions of each of these fields are no

longer appropriate. Further, research in IoT, PC, MC, WSN and CPS often relies on underlying technologies such as real-time computing, machine learning, security, privacy, signal processing, big data, and others. Consequently, the smart vision of the world involves much of computer science, computer engineering, and electrical engineering. Greater interactions among these communities will speed progress.

1. Challenges in Internet of Things

The fact that Internet of things applications and scenarios outlined above are very interesting which provides technologies for smart everything , but there are some challenges to the application of the Internet of Things concept in cost of implementation. The expectation that the technology must be available at low cost with a large number of objects. IoT are also faced with many other challenges [69, 70],

Internet of Things has a big concept than the conventional Internet of computers, because of things are cooperated within an open environment. Basic functionality such as communication and service discovery therefore need to function equally efficiently in both small scale and large scale environments. Some application scenarios of the internet of things will involve to infrequent communication, and gathering information's form sensor networks, or form logistics and large scale networks, will collect a huge volumes of data on central network nodes or servers. The term represent this phenomena is big data which is requires many operational mechanism in addition to new technologies for storing, processing and management.

The Internet of Things is no different in this respect, and security in IoT is fundamentally linked to the ability of users to trust their environment. If people don't believe their connected devices and their information are reasonably secure from misuse or harm, the resulting erosion of trust causes a reluctance to use the Internet. This has global consequences to electronic commerce, technical innovation, free speech, and practically every other aspect of online activities. Indeed, ensuring security in IoT products and services should be considered a top priority for the sector.

Each type of smart objects in Internet of Things has different information, processing and communication capabilities. Different smart objects would also be subjected to different conditions such as the energy availability and the communications bandwidth requirements. To facilitate communication and cooperation of these objects, common standards are required. A more extensive software infrastructure will be needed on the network and on background servers in order to manage the smart objects and provide services to support them. that because the software systems in smart objects will have to function with minimal resources, as in conventional embedded systems.

In addition to the security and protection aspects of the Internet such in communications confidentiality, the authenticity and trustworthiness of communication partners, and message integrity, other requirements would also be important in an Internet of Things. There is a need to access certain services or prevent from communicating with other things in IoT and also business transactions involving smart objects would need to be protected from competitors prying eyes. Objects in internet of things is much more dynamic and mobile than the internet computers, and they are in changing rapidly in unexpected ways. Structuring an Internet of Things in a robust

and trustworthy manner would require redundancy on several levels and an ability to automatically adapt to changed conditions.

2. Challenges

2.1. Technology Challenge

IoT has already turned into a serious security concern that has drawn the attention of many private companies and government agencies across the world. The hacking of smart refrigerators, drug infusion pumps, bank servers, cameras and even your mobile are signifying a security threat being caused by the future of IoT. The future of IoT will very much have to depend on decentralizing IoT networks. Part of it can become possible by moving some of the tasks to the edge, such as using fog computing models where smart devices such as IoT hubs take charge of mission-critical operations and cloud servers take on data gathering and analytical responsibilities [5].

The bottom line is a big motivation for starting, investing in, and operating any business, without an appropriate and definite business model for IoT we will have another myth , this model must satisfy all the requirements for all kinds of e-commerce; vertical markets, horizontal markets, and consumer markets. But this category is always a victim of regulatory and legal scrutiny. End-to-end solution providers operating in vertical industries and delivering services using cloud analytics will be the most successful at monetizing a large portion of the value in IoT. While many IoT applications may attract modest revenue, some can attract more. For little burden on the existing communication infrastructure, operators have the potential to open up a significant source of new revenue using IoT technologies.

2.2. Artificial Intelligences Challenge

The newest challenge seems to be how to incorporate the human behavior as part of the system itself. Can we define/guarantee/learn the stability, accuracy, settling time and overshoot properties of such systems, initially and as the system and human behavior evolves? If we can model such an operator behavior using formal methodology of feedback control and if we can incorporate these operator models into the system, we will be able to analyze various safety properties of the overall system. The need for extensions to system identification or other techniques to derive models of human behaviors, System identification is a powerful technique to create system models. It is a new challenge to apply it to human behaviors. The order and types of equations to use, how to produce adequate testing inputs, what output variables are required, and how such a model accounts for human traits are unknown. If we were to use system identification technique to model a human being who is suffering from depressive illness, it is not clear what are the inputs, what are the states and how the state transitions occur based on different physiological, psychological and environmental factors. If there was a formal model of human behavior or even an estimated model, then by combining all the factors that affect depression, we could close the loop by changing the factors in a way that helps the patients and that is based on an established methodology rather than ad hoc rules.

2.3. Security and Privacy Challenge

Security attacks are problematic for the IoT because of the minimal capacity of devices is being used, the physical accessibility to sensors, equipment's and objects, and ease in connectivity of the systems, including the fact that most devices will communicate wirelessly. The security problem is further inflamed because transient and permanent random failures are commonplace and failures are vulnerabilities that can be exploited by attackers. However, the considerable redundancy that is available creates potential for designing applications to continue to provide their specified services even in the face of failures. To meet realistic system requirements that derive from long lived and unattended operation, IoT applications must be able to continue to operate satisfactorily in the presence of, and to recover effectively 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 adapt to new attacks unpredicted when the system was first installed. [34].When the system operates with a base level of support including strong attack detection capabilities. Once an attack is detected then reaction to it occurs, by self-healing. In addition to the security and protection aspects of the Internet such in communications confidentiality, the authenticity and trustworthiness of communication partners, and message integrity, other requirements would also be important in an Internet of Things. The pervasiveness and interactions involved in IoT will provide many conveniences and useful services for individuals, but also create many opportunities to violate privacy. To solve the privacy problem created by IoT applications of the future, the privacy policies for each system or domain must be specified and be enforced as required. Consequently, the IoT model must be able to express users' requests for data access and the policies such that the requests can be evaluated against the policies in order to decide if they should be granted or denied.

The Internet of Things presents some unique challenges when it comes to privacy, and a lot of that goes far beyond the data privacy issues that exist currently. Much of this is because of the trouble integrating devices into the environments without people using them consciously. This is becoming even more prevalent when it comes to consumer devices, such as tracking devices for cars and phones and also smart TVs. Yes, your TV will soon be smarter than you. Humbling, right? Vision features and voice recognition are now being integrated into smart TVs. These features can listen continuously to conversations or look for activity and transmit data selectively to cloud services for processing. These cloud services may sometimes even include third parties. The collection of all this information faces a number of regulatory and legal challenges. Apart from this, there are a number of IoT scenarios that involve the data collection and the deployment of devices with a global or multinational scope that crosses cultural and social boundaries. But what does this mean for the development of broadly applicable privacy-protection models? If we are to realize the opportunities of the Internet of Things, strategies are going to have to be developed that respect the individual privacy choices while fostering innovation for new services and technologies.

3. Research Opportunities

The opportunities of research required to achieve IoT at the scale envisioned above requires significant research along many directions. In this section problems and required research are highlighted in 8 topic areas: massive scaling, architecture and dependencies, creating knowledge and big data, robustness, openness, security, privacy, and human-in-the-loop. Each of the topic discussions primarily focuses on new problems that arise for future IoT systems of the type

described in Section II. The research topics presented in each case are representative and not complete. Many important topics such as the development of standards, the impact of privacy laws, and the cultural impact on use of these technologies are outside the scope of the paper.

3.1. Better Connectivity

Machine-to-machine communication has several unique characteristics: the data rate is often lower, the information from different sensors or at different time steps may have strong correlations, and some messages do not require real-time delivery. Therefore, one approach to these problems is to form clusters of machines. Instead of communicates with the base station directly, machines talk to nearby cluster head, which in turn pass on to the base station. This will reduce the machine transmission power demand and increase spatial reuse of the spectrum. Another possibility is to fuse information or remove redundancy of the information, e.g., via distributed coding, to further reduce bandwidth usage. Second, many connected devices are mobile, such as sensors install on vehicles. These sensors not only need to communicate with other sensors via intra-vehicle networks, but also inter-vehicle networks. Existing radios most likely underperform in on-road wireless channels. To provide reliable vehicle-to-vehicle communication, we should first study the vehicle mobility model and then develop the optimal communication protocols based on the channel model. Finally, wireless communication consumes large amounts of bandwidth. A recent study shows that up to 70 % of the power used on a mobile device goes through wireless communication [33]. Many connected devices are battery-powered, and current human-to-human communication designs do not consider energy efficiency as the first priority. Yet, energy-efficient machine-to-machine communication is difficult to achieve. In particular, signaling costs are high. Self-organizing hybrid distributed and centralized structure may be one approach to reducing signaling overhead.

3.2. Architecture

As trillions of devices or equipment's are connected to the Internet it is necessary to have an adequate architecture that permits easy connectivity, control, communications, and useful applications. How will these objects interact in and across applications [37]? Many times, things or sets of things must be disjoint and protected from other devices. [2][4] Various standards and automatic checks are made to ensure that an app can execute on a given platform. [12]. A similar architectural approach for IoT would also have similar advantages. However, the underlying platform for IoT is much more complicated than for smartphones. Nevertheless, if IoT is based on an underlying sensor and actuator network that acts as a utility similar to electricity and water, then, different IoT applications can be installed on this utility. Interferences arise from many issues, but primarily when the cyber depends on assumptions about the environment, the hardware platform, requirements, naming, control and various device semantics. Previous work, in general, has considered relatively simple dependencies related to numbers and types of parameters, versions of underlying operating systems, and availability of correct underlying hardware. Research is needed to develop a comprehensive approach to specifying, detecting, and resolving dependencies across applications. This is especially important for safety critical applications or when actuators can cause harm.

3.3. Robustness

If our vision is correct, many IoT applications will be based on a deployed sensing, actuation, and communication platform (connecting a network of things). In these deployments it is common for the devices to know their locations, have synchronized clocks, know their neighbor devices when cooperating, and have a coherent set of parameter settings such as consistent sleep/wake-up schedules, appropriate power levels for communication, and pair-wise security keys. However, over time these conditions can deteriorate. The most common (and simple) example of this deterioration problem is with clock synchronization [18]. Over time, clock drift causes nodes to have different enough times to result in application failures. While it is widely recognized that clock synchronization must re-occur, this principle is much more general. For example, some nodes may be physically moved unexpectedly. More and more nodes may become out of place over time. To make system-wide node locations coherent again, node re-localization needs to occur (albeit at a much slower rate than for clock sync). This issue can be considered a form of entropy where a system will deteriorate (tend towards disorder) unless energy in the form of re-running protocols and other self-healing mechanisms is applied [35]. Note that control of actuators can also deteriorate due to their controlling software and protocols, but also due to physical wear and tear. In other words, how can a long-lived, dynamic, and mobile IoT be maintained?

4. Conclusion

The IoT promises to deliver a step change in individuals‟ quality of life and enterprises‟ productivity. Through a widely distributed, locally intelligent network of smart devices, the IoT has the potential to enable extensions and enhancements to fundamental services in transportation, logistics, security, utilities, education, healthcare and other areas, while providing a new ecosystem for application development. A concerted effort is required to move the industry beyond the early stages of market development towards maturity, driven by common understanding of the distinct nature of the opportunity. This market has distinct characteristics in the areas of service distribution, business and charging models, capabilities required to deliver IoT services, and the differing demands these services will place on mobile networks. Connecting those smart devices (nodes) to the web has also started happening, although at a slower rate. The pieces of the technology puzzle are coming together to accommodate the Internet of Things sooner than most people expect. Just as the Internet phenomenon happened not so long ago and caught like a wildfire, the Internet of Things will touch every aspect of our lives in less than a decade.

Briefly we can say one vision of the future is that IoT becomes a utility with increased sophistication in sensing, actuation, communications, control, and in creating knowledge from vast amounts of data. This will result in qualitatively different lifestyles from today. What the lifestyles would be is anyone’s guess. It would be fair to say that we cannot predict how lives will change. We did not predict the Internet, the Web, social networking, Facebook, Twitter, millions of apps for smartphones, etc., and these have all qualitatively changed societies’ lifestyle. New research problems arise due to the large scale of devices, the connection of the physical and cyber worlds, the openness of the systems of systems, and continuing problems of privacy and security. It is hoped that there is more cooperation between the research communities in order to solve the myriad of problems sooner as well as to avoid re-inventing the wheel when a particular community solves a problem.

References

[1] M. A. Ezechina, K. K. Okwara, C. A. U. Ugboaja. The Internet of Things (Iot): A Scalable Approach to Connecting Everything. The International Journal of Engineering and Science 4(1) (2015) 09-12.
[2] G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (references)
[3] Ron Davies. The Internet of Things Opportunities and challenges. May 2015. [70] Friedemann Mattern and Christian Floerkemeier. From the Internet of Computers to the Internet of Things. https://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdfJ. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
[4] "Values and Principles." Principles. Internet Society, 2015. http://www.internetsociety.org/who-we-are/mission/valuesandprinciples
[5] 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.
[6] G. Schirner, D. Erdogmus, K. Chowdhury, and T. Padir, the Future of Human-in-the-Loop Cyber-Physical Systems. Computer 46, 1, 2013, pp. 36– 45.
[7] 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.
[8] S. Mohammed, P. Fraisse, D. Guiraud, P. Poignet, and H. Makssoud, Towards a Co-contraction Muscle Control strategy for Paraplegics. CDCECC, 2005.
[9] K. Tsui, D. Kim, A. Behal, D. Kontak, and H. Yanco, I Want That : Human-in-the-Loop Control of a Wheelchair-Mounted Robotic Arm. Journal of Applied Bionics and Biomechanics 8, 2011.https://www.linkedin.com/pulse/why-iot-needs-fog-computing-ahmed-banafa?trk=mp-author-card
[10] S. Ravi, A. Raghunathan, S. Chakradhar. Tamper Resistance Mechanisms for Secure, Embedded Systems, Proc. of 17th International Conference on VLSI Design, 2004. p. 605.
[11] 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.
[12] T. Pering, Y. Agarwal, R. Gupta, and R. Want, "Coolspots: reducing the power consumption of wireless mobile devices with multiple radio interfaces," in Proc. of ACM Mobile Systems, Applications and Services, pp. 220–232, 2006.
[13] A. Wood, L. Fang, J. Stankovic, and T. He, SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks, ACM Security of Ad Hoc and Sensor Networks, Best Paper Award, October 31, 2006.
[14] W. Xu, W. Trappe, Y. Zhang, T. Wood, The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks, Proc. of MobiHoc, 2005. pp. 46-57.
[15] M. Balazinska, A. Deshpande, M.J. Franklin, P.B. Gibbons, J. Gray, S. Nath, M. Hansen, M. Liebhold, A. Szalay, V. Tao, "Data Management in the Worldwide Sensor Web," IEEE Pervasive Computing, vol.6, no.2, pp.30-40, April-June 2007
[16] M. Bellis, "The History of the ENIAC Computer," About.com Guide
[17] D. Estrin, "Participatory sensing: applications and architecture [Internet Predictions]," Internet Computing, IEEE, vol.14, no.1, pp.12-42, Jan.-Feb. 2010

*Corresponding author.
E-mail address: sachinupadhyay2010@ yahoo.co.in