ADCAIJ: Advances in Distributed Computing and Articial Intelligence Journal
Regular Issue, Vol. 6 N. 4 (2017), 35-40
eISSN: 2255-2863
DOI: http://dx.doi.org/10.14201/ADCAIJ2017643540

An Indian Perspective on the adverse impact of Internet of Things (IoT)

V. Kethareswaran

Department of Computer Science and Engineering, Anna University - BIT Campus, Tiruchirappalli - 620 024, TamilNadu, India. kethar4111997@gmail.co

KEYWORD

Internet of Things (IoT); Indian Society Impacts; Indian Policies & Laws

ABSTRACT

The **Internet of Things (IoT)** *has opened up a new era of computing where by every imaginable object is equipped with, or connected to a smart device allowing data collection and communication through the Internet. The IoT challenges individual privacy in terms of the* collection and use *of individuals' personal data. This study assesses the extent to which the IoT has an adverse effects on Indian Society. A review of various policies and laws formulated and enacted by the Govt. Of India where taken into account and various conclusions were derived based on the analyzed facts. Findings indicate that (1) the Indian policies and Laws pertaining to IoT and cyber issues are not enough to provide stiff opposition to the current pretext of fear and mishappenings and (2) future legislations must consider the implications of* global reach *of IoT services with respect to its citizen's well-being.*

1. Introduction

The **Internet of things** is the internetworking of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as «the infrastructure of the information society». The IoT allows objects to be sensed and/or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure.. The number of Internet-connected devices (12.5 billion) surpassed the number of human beings (7 billion) on the planet in 2011, and experts estimate that the IoT will consist of almost 50 billion objects by 2020. The Indian Government's plan of developing 100 smart cities in the country, for which Rs. 7,060 crores has been allocated in the current budget could lead to a massive and quick expansion of IoT in the country. Also, the launch of the Digital India Program of the Government, which aims at 'transforming India into digital empowered society and knowledge economy' will provide the required impetus for development of the IoT industry in the country. The various initiatives proposed to be taken under the Smart City concept and the Digital India Program to set-up Digital Infrastructure in the country would help boost the IoT industry. IoT will be critical in making these

cities smarter. Among other things, IoT can help automate solutions to problems faced by various industries like agriculture, health services, energy, security, disaster management etc. through remotely connected devices.

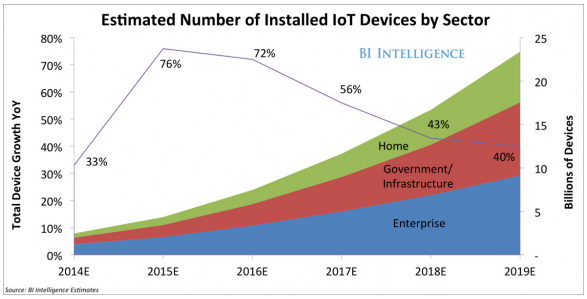

Figure 1: Future of IoT globally

IoT offers avenues for telecom operators & system integrators to significantly boost their revenues and this has resulted in their taking lead in adoption of IoT applications and services being offered by the technology. Apart from direct IoT applications, the IT industry also has an opportunity to provide services, analytics and applications related to IoT. Internet of Things (IoT) is one of the hottest technologies. But, privacy and network issues need to be overcome before it can become mainstream. Thus this assessed research poses this question: ***To what extent does the Indian Privacy Policy protect an Indian's privacy with respect to data collected via the Internet of Things?*** and ***How far are the issues pertaining to IoT are being answered by the Indian laws and regulations?*** In answering this question, this paper does not offer a legal analysis, but verifies whether the current Indian Privacy Policy of data protection effectively secures an individual's privacy from an IoT perspective. The research involved the assessment of current data protection laws in our country and the newly framed and yet to be implemented ***Policy on Internet of Things.***

2. Data protection laws in India

Data Protection laws may be defined as the laws which are enacted for safeguarding and protecting the data present on the internet. India has witnessed various high profile data theft cases off lately. India does not have any separate law which is designed exclusively for the data protection. However, the courts on numeral instances have interpreted «data protection» within the ambits of «Right to Privacy» as implicit in Article 19 and 21 of the Constitution of India. Apart from this, the laws which are presently dealing with the subject of data protection are «The Indian Contracts Act» and «The Information Technology Act». Section 43 A of the Information technology Act explicitly provides that «*Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected».* Further Section 72 A provides that «*Punishment for disclosure of information in breach of lawful contract.»* It is apparent that both the sections mentioned above are not dealing with data security directly. Prior to 2011 the situation of the laws related to data protection was very vague and ambiguous, as there was no law which dealt directly and explicitly with this issue. Later in 2011, after the enactment of the European Union's strict and stringent Data Protection Laws, the Government of India also felt the need for the same in our country. Consequently, a new set of rules named the «**Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**» came into picture. These rules have provisions for three groups- Body Incorporates, Information Providers (Data Subjects) and the Government. The key features of the Rules are as follows-

- *Rule 3* mentions the list of things which will be treated as «sensitive personal data «under the Act. It includes passwords, credit or debits card information, medical and biometric records etc.
- *Rule 4* casts a duty upon the Body Corporate to provide a privacy policy for dealing with personal information and sensitive data and it also requires that the policy should be available on the website of the body corporate. The policy shall include all the necessary details for e.g. type of personal data collected, statements of practices, purpose of collection, provisions related to disclosure and security practices etc.
- *Rule 5* states various provisions which govern the collection of information by the Body Corporate.
- *Rule 6* requires that the Body Corporate shall seek the consent of the concerned provider before disclosing the sensitive data to a third party, unless such disclosure was agreed by the parties through any contract. However, such information can be shared without any prior consent with government agencies mandated under law or any other third party by an order under the law, who shall be under a duty not to disclose it further.
- *Rule 8* clarifies that a body corporate shall be considered to have complied with reasonable security practices if they have implemented and documented the standards of these security practices.

3. Policy on Internet of Things

3.1. Objectives

- To create an IoT industry in India of USD 15 billion by 2020. It has been assumed that India would have a share of 5-6% of global IoT industry.
- To undertake capacity development (Human & Technology) for IoT specific skill-sets for domestic and international markets.
- To undertake Research & development for all the assisting technologies.
- To develop IoT products specific to Indian needs in all possible domains.

3.2. Strategy

The Policy framework of the IoT Policy has been proposed to be implemented via a multi-pillar approach. The approach comprises of five vertical pillars (Demonstration Centers, Capacity Building & Incubation, R&D and Innovation, Incentives and Engagements, Human Resource Development) and 2 horizontal supports (Standards & Governance structure).

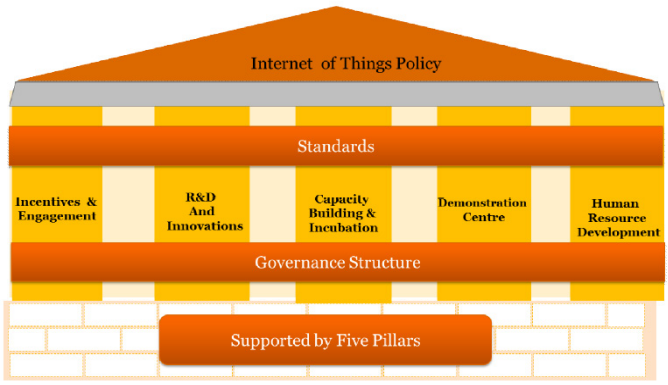

Figure 2: IoT approaches in Indian society

4. Analysis of the Protection act and Policy

Internet of things (IoT) has received a very positive response from Indian government and Indian entrepreneurs. Although everybody is very enthusiastic about IoT and its usage in India yet nobody is aware about its usage policies and regulatory framework. This situation has arisen as we have neither a dedicated e-commerce law nor a law governing IoT and its uses in India. As a result everybody is just deploying IoT based systems and devices in India without knowing the seriousness of their actions and omissions. IoT usage and deployment can give rise to IoT privacy, data protection, cyber security and civil liberty issues in India. However, world over these techno legal issues of IoT are still in infancy stage. India has also been trying to bring a policy and regulatory framework for use of IoT in India by various stakeholders. Issuance of draft IoT Policy of India and Revised Draft IoT Policy of India are instances of such efforts but they are not sufficient to cover the areas and operations of innovative technology like IoT. It is obvious that we need techno legal framework for successful and wide scale use of IoT in India. However, this is a difficult task to manage as we have very few techno legal professionals in India and other jurisdictions that can assist in this regard. This is the reason why India is still struggling to enact privacy, data protection and cyber security laws in India. As a result, India has a very poor track record of civil liberties protection in cyberspace and surveillance and censorship issues of Digital India and Aadhaar projects are in active violation of provisions of Indian Constitution. It is largely believed that as we would start mass deployment of IoT making it omnipresent, all stakeholders would be apprehensive as the cross linking nature of IoT would offer new possibilities and methods to influence and to exchange data and information. This leads to a variety of existing and new potential risks concerning data security, privacy and data protection, which must be considered in advance. The severity and likeliness of each risk will depend on the circumstances in which each IoT application / system is deployed. Naturally privacy, data protection and cyber security are complementary requirements for IoT services in India. In particular, data security and data protection are regarded as preserving the confidentiality, integrity and availability of information provided by Indian citizens. It is also believed that cyber security is an essential and basic requirement while providing of IoT related services by the industry or government. This is required not only to ensure information security for the organisation itself but also for the benefit of Indian citizens at large. For instance, IoT presents a variety of potential security risks that could be exploited to harm consumers by: (a) having unauthorized access and misuse of personal information; (b) facilitating attacks on other systems; and (c) creating risks to personal safety. Similarly, privacy risks may flow from the collection of personal information, habits, locations, and physical conditions over time. These days behavioral targeting is very common among companies who rely upon historical and real time data to analyze and influence consumer's interests and choices. Companies might use this data to make credit, insurance, and employment decisions. Even if companies are prevented by law for not taking such a course of action still these risks to privacy and security could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption.

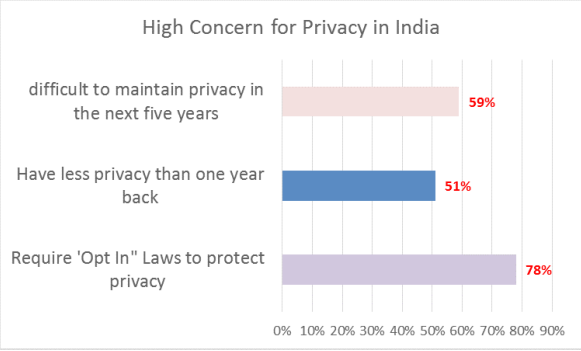

Figure 3: The netizens of India felt privacy is an area of huge concern for them today and expect to be so over the next five years

5. Conclusion to the analyses

This paper analyses the impact of data collected through the IoT by highlighting its impact on the legal framework of India. From the analyzed data's it is strongly recommended that companies developing IoT products and services in India should implement reasonable security practices and procedures. These must include cyber security best practices, e-discovery best practices, cyber law due diligence , Internet intermediary liability law compliances, etc. Similarly, there must be a dedicated crisis management plan for cyber-attacks against IoT in India so that IoT and critical infrastructures can recover from sophisticated cyber-attacks as soon as possible.

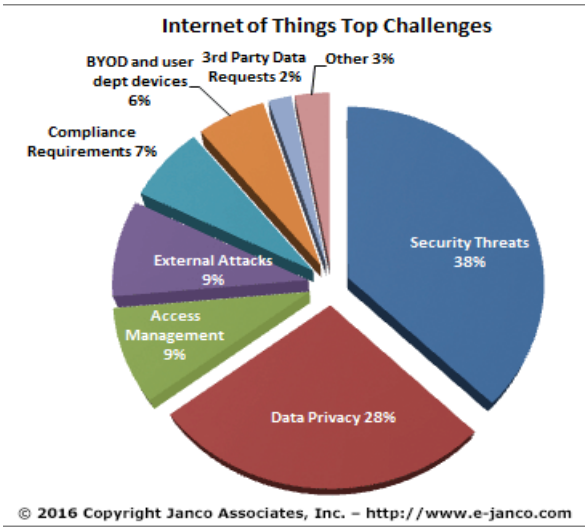

Figure 4: IoT concerns in India

The above graph also shows that the security threats and data protection laws are a huge concern for IoT in India. India must also develop robust and resilient cyber so that systems dependent upon Information and Communication Technology (ICT) can come online as soon as possible. There are some long-standing Fair Information Practice Principles («FIPPs») like notice, choice, access, accuracy, data minimization, security, and accountability that should apply to the IoT segment. Indian IoT stakeholders must also follow these principle and privacy and data protection best practices so that IoT services can be provided in a legal and law abiding manner not only in India but also in other jurisdictions. Hence, IoT stakeholders from India must be aware of and comply with laws of different jurisdictions if their products and services are also offered in those jurisdictions. Thus we conclude that the present context to which the analysis were made are not promising enough to face the situation of crisis. Thus the legal framework must be further enhanced to meet the current requirements.

6. References

Abowd, G.D., Mynatt, E.D. Charting past, present, and future research in ubiquitous computing. *ACM Trans Comput Hum Interact* 2000; *7*(1): 29-58.

Atzori, L., Iera, A., Morabito, G. The internet of things: a survey. *Comput Netw* 2010; (54): 2787-805.

Baldauf, M., Dustdar, S., Rosenberg, F. A survey on contextaware systems. *Int J Ad Hoc Ubiquitous Comput* 2007; *2*(4): 263-77.

Barnaghi, P., Wang, W., Henson, C., Taylor, K. Semantics for the internet of things: early progress and back to the future. *Int J SemanticWeb Inf Syst* 2012; 8(1): 1-21.

Bauer, S., Burkitt, F., Curran, C., Gioia, L. Digital IQ snapshot - sensor technology. <http://www.pwc.com/us/en/advisory/digital-iq -survey/assets/sensor-technology.pdf>; 2014 [accessed 15.08.14].

Chen, Y.K. 2012. Challenges and opportunities of internet of things. Asia and South Pacific design automation conference (ASP-DAC), Issue 17, pp. 383-8.

Coetzee, L., Eksteen, J. 2011. The internet of things-promise for the future? An introduction. IST-Africa conference proceedings, pp. 1-9.

European Commission (ISM). Vision and challenges for realizing the internet of things. In: *CERP-IoT - cluster of European research projects on the internet of things*. Luxembourg: Publications Office of the European Union; 2010. pp. 1-230.

Ferber, S. How the internet of things changes everything. <http://blogs.hbr.org/2013/05/how-the-internet-of-things-cha/>; 2013 [accessed 15.10.14].

Haller, S., Karnouskos, S., Schroth, C. *The internet of things in an enterprise context. s.l.* Berlin and Heidelberg: Springer; 2009.

Jara, A.J., Zamora, M.A., Skarmeta, A.F. 2012. Knowledge acquisition and management architecture for mobile and personal health environments based on the internet of things. IEEE 11th international conference on trust, security and privacy in computing and communications (TrustCom), pp. 1811-18.

Mayer-Schönberger, V., Cukier, K. *Big data: a revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt; 2013.

Nissenbaum, H. Protecting privacy in an information age: the problem of privacy in public. *Law Philos* 1998; *17*(5): 559-96.

Ministry Of Electronics and Information Technology, Govt Of India. http://meity.gov.in/content/revised-draft-internet-thingsiot-policy.