IJASRM

International Journal of Advanced Scientific Research and Management, Volume 3 Issue 9, Sept 2018

www.ijasrm.com

ISSN 2455-6378

Legal issues in Internet of Things

Prof. Hetal B. Pandya

Computer Engineering Department, Government Engineering College,
Bhavnagar , India

Abstract

IoT envisions the near future of internet by allowing the interaction between people and things at virtual level and becomes the integral part of human life. It is playing a leading role in various domains per say, IoT brings home automation, security, devices monitoring, and managing of daily routine for individual users. Various enabling technologies are used to fulfill the promising concept of IoT. However, with such technological inventions, many fold challenges will come into the picture, especially legal issues. The paper is divided into three parts. Firstly it provides introduction of IoT, subsequently it gives overview of IoT in India and in third section, understanding of legal issues like privacy and data security, data ownership, intellectual property rights, product liability, and jurisdiction and deciding liability have been discussed.

Keywords: — *IoT, Technologies in IoT, Legal issues of IoT*

1. Introduction

Internet of Things – In simple 3 words it can be explained as “web of things”, allows interconnecting everything which we are using in our day to day life. It’s like every generic thing, communicating to each other and act accordingly. For example: IoT will wake up you in morning through alarm, by referring to calendar. It then turn on greaser 5 minutes before you will go to take your bath, it turn of lights, fans, a/c etc as soon as you leave home and as per the outer atmosphere. When you enter in to your car it shows you the probable and best route to reach your office. This is how a fully automated life can be live with the help of IoT.

According to Cluster of European research Project, in IoT all the devices /things are active participants in the communication by exchanging information through network and the sensors and react to the situation autonomously without the intervention of human being.

“The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service.

The IoT is now a day’s playing leading role in various domains. For individual users, IoT brings home automation, security, devices monitoring, and managing of daily routine. For an organization, automated applications provide easy access to appropriate information which helps in taking major decision quickly. An industry, with all automated machines produces fast and efficient output and hence leads to increase in economy of an industry.

Looking at the statistics at global level, it is expected that the IoT market will grow to 28.1 billion IoT devices by 2020 and revenue growth will be observed to $7.1 trillion in 2020. It is also estimated that IoT will increase $10 to $15 trillion to global GDP in the next 20 years. Further, IoT analytics market is estimated to grow at a CAGR of27.48% from 2015 to 2020 to reach $ 16.35 B by 2020.

2. Overview of Enabling Technologies of IoT

IoT is combination of various empowering technologies such as sensing and communicating technology, middleware and communication protocols. The following section provides overview of these enabling technologies.

2.1 Sensing and Communication Technology

The hardware and sensing elements like wireless sensors, RFID tag/readers, NFC, and various embedded chips play a major role in IoT. We can say that they constitutes lower layer of IoT architecture. Also, some technologies like two dimensional barcode, Radio-frequency identification (RFID), wireless sensor network, RFID Wireless Sensor Network (RSN) and Near Field Communication (NFC) are used for the same.

2.2 Middleware

Middleware is glue that provides interoperability among various hardware/sensing devices and application software which are running under distributed computing environment. Basic functionality of middleware is to integrate heterogeneous devices, provides common semantics and to provide various management and developmental tool for IoT. Middleware provides infrastructure to leverage IoT services. The key components of middleware are interoperation, context awareness, device discovery and management, device abstraction, integration various processes, managing large volume of data and off course security and privacy of those data. The IoT Middleware can be categorized as per their major functionalities like Pervasive computing middleware, Message oriented middleware, Semantic web base middleware, Service oriented architecture and UBIWARE.

Similarly, communication middleware support protocols for transmitting messages or data between two points. It also includes embedded middleware. It comprises of various categories like SCADA based, RFID based, WSN based and RSN based middleware. The communication middleware can be categorized as RFID based middleware; Sensor Network based middleware, Supervisory Control and Data Acquisition – SCADA and LBS and surveillance middleware

2.3 Communication Protocols

IoT needs different protocols for different operations. Like it requires a protocol for collecting the data from sensors, communication protocol to send the data to server infrastructure, protocols for device to people communication, protocol for D2D/M2M communication. It includes message Queue Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Extensible Messaging and Presence Protocol (XMPP), Data Distribution Service (DDS), Advanced Message Queuing Protocol (AMQP), Zigbee, and Zwave.

3. IoT in India

In 2015, Government of India announced that by next five years it has plans to create a $15 billion internet of things market in the country. This created some spike in the interest around IoT. However, IoT is yet to create any major buzz in India as even the mainstream information sources has not taken up to discuss about IoT in big way.

It important to know the Government of India’s IoT announcement. Department of Electronics and Information Technology, has come out with a draft IOT Policy document which focuses on following objectives:

1) 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.
2) To undertake capacity development (Human & Technology) for IoT specific skill-sets for domestic and international markets.
3) To undertake Research & development for all the assisting technologies.

To develop IoT products specific to Indian needs in all possible domains.

Further, under digital India programme and smart cities initiatives, government has started focusing on Smart ways to manage water, environment, healthcare, agriculture, waste management and smart Safety.

4. Overview of legal issues of IoT

There are varieties of challenges in IoT. These challenges can be classified according to (i) various technological aspects of IoT and (ii) legal aspects of IoT. The following section provides overview of legal issues to be aroused out IoT. The main issues in legal domain ranges from privacy & data security, data ownership, intellectual property rights, product liability, and jurisdiction and deciding liability.

4.1 Privacy and data security

Primarily, the IoT system is profoundly reliant on data collection and transmission. This data could comprise of general as well as sensitive personal information of the users such as bank account details, blood group and other important details alike. This type of available data poses the challenge of data leak and privacy could be at risk. Similarly, as IoT sensing devices are low powered, incorporation of security algorithms for the data security are not feasible. Also, the sensing devices are not under surveillance so they can be easily interceding by intruders and eavesdropping can be possible. Adding to it, various network attacks such as spoofing, Distributed denial of service (DDoS), jamming and shielding are also major security concerns. As the devices/person can be easily tracked by the sensing devices, the privacy and the confidentiality for person/object cannot be preserved. To address this issue, it is required to frame legitimate policy beforehand to track the devices.

4.2 Data ownership

As there will be involvement of multiple stakeholders or IoT users, involvement of many third parties will be there including the multitude of sources of the data. The data may come into possession of many data processors, which rises the conflict in terms of data ownership. Also, there will be immense integration of data from various technologies and devices, the question of ownership of data as well as end product (information) will come in the picture. . For example, gadget like wrist watch senses the pulse/body temperature and directs the air conditioner to fine-tune the room temperature according to the level of comfort; or the navigation system in a car could predict to the appliances at home when the individual would be arriving home, the ownership of the data generated regarding that person (his travel route, time, habits, etc.) become a question of concern. It leads to issues like, who own the data, the person (because it relates to him) or do the devices which are used (and because they created it)? Addressing this questions pertaining to ownership of continuously generated data is very much essential in terms of its legal ownership.

4.3 Intellectual Property Rights

In IoT, the system is very much relied upon interconnection among devices requiring various products and technologies. This interconnection will be of different companies' developed products and technologies which raises the issue of claim over intellectual property on the end product or information because IoT facilitates data generation and creation of content including Machine Generated Data. This will also raise questions pertaining to time of original data creation during interaction of various devices. These blurring boundaries create issues as to what extent of rights each party is entitled to in terms of Intellectual Property

4.4 Product Liability

An IoT device generally includes various components such as software, hardware, and other related service elements. And each of these components comes with their own set of warranties and disclaimers. In this situation, any defect or deficiency in the IoT device can create complex issues pertaining to product liability. This will lead to difficulty wherein fixing which component or who is responsible for the defect. And this will lead to the difficulty where in user or consumer will be unable to determine whom he should go for compensation claim or repair. In such situation, it will be impossible for consumer to find out a way if all stakeholders in the transaction disclaim their responsibility for the defect.

4.5 Jurisdiction

It is well evident that the world of information technology has its own jurisdictional issues. The issue pertaining to it cannot be attributed to any limited geographical area. And the evolution of IoT creates more complex scenario. This happens because IoT involves the interconnection of various technologies and services of different companies which may be from different geographical jurisdictions individually. This makes challenging to fix a common jurisdiction for IoT related disputes and requires involvement of various considerations.

4.6 Deciding Product Liability

In IoT, where many devices are interconnected in case of any injury caused to a party, it becomes very much difficult to accurately state which feature of the interconnected devices malfunctioned, and who can be held liable it. This is because, as the flow of information is continuous in IoT device, and it is sometimes practically very difficult to accurately fix where the flaw occurred.

5. Conclusion

The way technological advancements are taking momentum in leaps and bounds, needless to say that the future belongs to IoT. However, it's worth noting the challenges involved in such massive amounts of data. Developed and developing nations are on the track of advancements through IoT but the issues and especially legal issues like privacy and data security, data ownership, intellectual property rights, product liability, and jurisdiction and deciding liability are required to be addressed.

It is advisable for policy makers and the stakeholders to understand and address these legal challenges. It's essential for service providers and consumers to pay attention towards laws and regulations on consumer protection, IPRs, IT Laws, liability relating to such matters, etc .Also, due care has to be taken towards IoT issues especially in case of collaborative projects with other companies, introducing service in the market, addressing customer grievances and using data protection systems etc.

References

[1] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context Aware Computing for The

Internet of Things: A Survey," Commun. Surv. Tutor. IEEE, vol. 16, no. 1, pp. 414–454, First 2014.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787 – 2805, 2010.

[3] "NFC in the Internet of Things (IoT) - ConnecTIng Wirelessly - Blogs - TI E2E Community," 07-Dec-2014. [Online]. Available: http://e2e.ti.com/blogs_/b/connecting_wirelessly/archive/2013/09/17/nfc-in-the-internet-of-things-iot. [Accessed: 07-Dec-2014].

[4] "Middleware for pervasive computing: A survey - Pervasive and Mobile Computing - Tom 9, Numer 2 (2013) - Biblioteka Nauki - Yadda," 07-Dec-2014. [Online]. Available: http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.elsevier-d1fbcfbd-22c6-38a2-a4b3-486e95382ed1. [Accessed: 07-Dec-2014].

[5] Z. H, "The Internet of Things in the Cloud: A Middleware Perspective - CRC Press Book," 07-Dec-2014. [Online]. Available: http://www.crcpress.com/product/isbn/9781439892992. [Accessed: 07-Dec-2014].

[6] M. A. Chaqfeh and N. Mohamed, "Challenges in middleware solutions for the internet of things," in Collaboration Technologies and Systems (CTS), 2012 International Conference on, 2012, pp. 21–26.

[7] "A Triple Space-Based Semantic Distributed Middleware for Internet of …," 07-Dec-2014. [Online]. Available: http://www.slideshare.net/twolf/a-triple-spacebased-semantic-distributed-middleware-for-internet-of-things. [Accessed: 07-Dec-2014].

[8] "iot.eclipse.org — Protocols," 07-Dec-2014. [Online]. Available: http://iot.eclipse.org/protocols.html. [Accessed: 07-Dec-2014].

[9] "Understanding The Protocols Behind The Internet Of Things | Embedded content from Electronic Design," 07-Dec-2014. [Online]. Available: http://electronicdesign.com/embedded/understanding-protocols-behind-internet-things. [Accessed: 07-Dec-2014].

[10] "RFC 7252 - The Constrained Application Protocol (CoAP)," 07-Dec-2014. [Online]. Available: https://tools.ietf.org/html/rfc7252. [Accessed: 07-Dec-2014].

[11] "RFC 4919 - IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," 07-Dec-2014. [Online]. Available: https://tools.ietf.org/html/rfc4919. [Accessed: 07-Dec-2014].

[12] "IBM Bluemix Docs," 07-Dec-2014. [Online]. Available: https://www.ng.bluemix.net/docs/#. [Accessed: 07-Dec-2014].

[13] "ThingWorx - Internet of Things and M2M Application Platform," 07-Dec-2014. [Online]. Available: http://thingworx.com/. [Accessed: 07-Dec-2014].

[14] "Documentation," 07-Dec-2014. [Online]. Available: http://gobot.io/documentation/. [Accessed: 07-Dec-2014].

[15] J. Al-Jaroodi and N. Mohamed, "Service-oriented middleware: A survey," J. Netw. Comput. Appl., vol. 35, no. 1, pp. 211 – 220, 2012.

[16] D. Guinard, I. Ion, and S. Mayer, "In Search of an Internet of Things Service Architecture: REST or WS-*? A Developers' Perspective," in Mobile and Ubiquitous Systems: Computing, Networking, and Services, vol. 104, A. Puiatti and T. Gu, Eds. Springer Berlin Heidelberg, 2012, pp. 326–337.

[17] A. P. Castellani, M. Gheda, N. Bui, M. Rossi, and M. Zorzi, "Web Services for the Internet of Things through CoAP and EXI," in Communications Workshops (ICC), 2011 IEEE International Conference on, 2011, pp. 1–6.

[18] T. A. Alghamdi, A. Lasebae, and M. Aiash, "Security analysis of the constrained application protocol in the Internet of Things," in Future Generation Communication Technology (FGCT), 2013 Second International Conference on, 2013, pp. 163–168.

[19] "iotsys - IoTSyS - Internet of Things integration middleware - Google Project Hosting," 15-Dec-2014. [Online]. Available: https://code.google.com/p/iotsys/. [Accessed: 15-Dec-2014].

[20] "LinkSmart Middleware Portal," 15-Dec-2014. [Online]. Available: https://linksmart.eu/redmine. [Accessed: 15-Dec-2014].

[21] "India: Legal issues pertaining to internet of things (IoT)", 12-April-2018. [Online]. Availablehttp://www.mondaq.com/india/x/691560/Data+Protection+Privacy/Legal+Issues+Pertaining+To+Internet+of+Things+IOT

[22] "Internet of Things: Legal perspective - risk and challenges". Available: https://medium.com/@legalresolved/internet-of-things-legal-perspective-risk-challenges-cd98b7a05bf7

[23] "Internet of Things: Indian perspective". Available: https://www.firstpost.com/business/internet-things-indian-perspective-2057171.html

[24] "IoT: Challenges and Issues in Indian Perspective". [Online]. Available: https://www.researchgate.net/publication/326929378

[25] Akyildiz, I, "Internet of things: trends, directions, opportunities, challenges". Available: https://bwn.ece.gatech.edu/presentations/IoT%20Trends%202017-04.pdf.