IJCSN International Journal of Computer Science and Network, Volume 5, Issue 4, August 2016
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 1.02

Internet of Things: Hindrance or Help

Parth Desai

Symbiosis Centre for Information Technology,
Pune, India – 411 057

Abstract - Internet of Things has (IoT) been promisingly making its way in the world market. According Gartner-a research firm report, 6.4 billion connected "Things" will be in use in 2016 which is 30% more than 2015. With the increasing horizon of IoT, there has been an increased concern over privacy. IoT systems have delivered positive results in many fields such as Healthcare, Insurance, Retail, Banking etc. but still large numbers of people are reluctant about the adoption of IoT. The major reason behind it is the amount of private data that they have to give away in order to get reward from it. In this paper, I have proposed to develop "Privacy versus Benefit Model" classifying the IoT product based on the degree of sensitive data they are collecting. Furthermore, suggestion on combating privacy concerns of the consumers has also been defined for the companies developing IoT systems.

Keywords – *IoT, Big Data, Data Classification, Personally Identifiable Information, Privacy Concern.*

1. Introduction

Organizations have been discussing the Internet of Things for a considerable length of time. There are numerous conceivable dreams of it. Some believe it's about your smartwatch communicating with your car, while your smart refrigerator autonomously converses with the supermarket to request you to order some more curd. Gartner-a research firm anticipated 26 billion gadgets will be introduced by 2020.

IoT is emerging as a promising technology in recent times. Still, many are reluctant to use IoT because of the security concerns associated with it such as insecure cloud interface, insecure mobile interface, privacy concerns etc. Companies should have to take a more pro-active role in embedding security in their products if they want their products to be accepted by wide range of users. In this paper, I am presenting a model which can address privacy concerns. In addition to that, suggestion on building an ideal system which addresses all privacy concerns is also specified.

2. Related Works

As identified by Atzori et al. [1], Internet of Things can be realized in three paradigms—internet-oriented (middleware), things oriented (sensors) and semantic-oriented (knowledge). Although this type of delineation is required due to the interdisciplinary nature of the subject, the usefulness of IoT can be unleashed only in an application domain where the three paradigms intersect.

There are several application domains which will be impacted by the emerging Internet of Things. We categorize the applications into four application domains:

(1) Personal and Home;
(2) Enterprize;
(3) Utilities; and
(4) Mobile.

This is depicted in Fig. 1, which represents Personal and Home IoT at the scale of an individual or home, Enterprize IoT at the scale of a community, Utility IoT at a national or regional scale and Mobile IoT which is usually spread across other domains mainly due to the nature of connectivity and scalability. There is a huge crossover in applications and the use of data between domains. For instance, the Personal and Home IoT produces electricity usage data in the house and makes it available to the electricity (utility) company which can in turn optimize the supply and demand in the Utility IoT.

The internet enables sharing of data between different service providers in a seamless manner creating multiple business opportunities. A few typical applications in each domain are given [2].

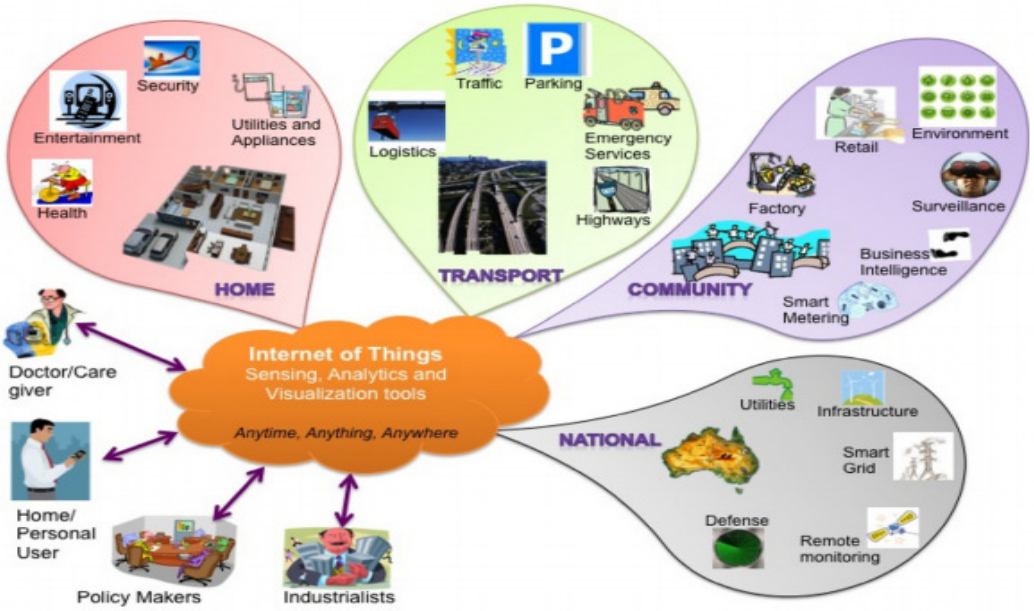

Figure 1 Internet of Things schematic showing the end users and application areas based on data [2]

There are many benefits of implementing IoT which can help individuals and businesses on a daily basis. Incorporating IoT into the healthcare will track individual's health remotely and can take mitigating steps when medication is needed. IoT also can be handy in person's household activity such as asset tracking, optimal utilization of electricity and house inventory management etc. It can also be very useful in different businesses such as banks can keep track of assets that are on loan, vehicle insurance company can decide premium based on users driving habits, manufacturing company can automate their inventory management etc.

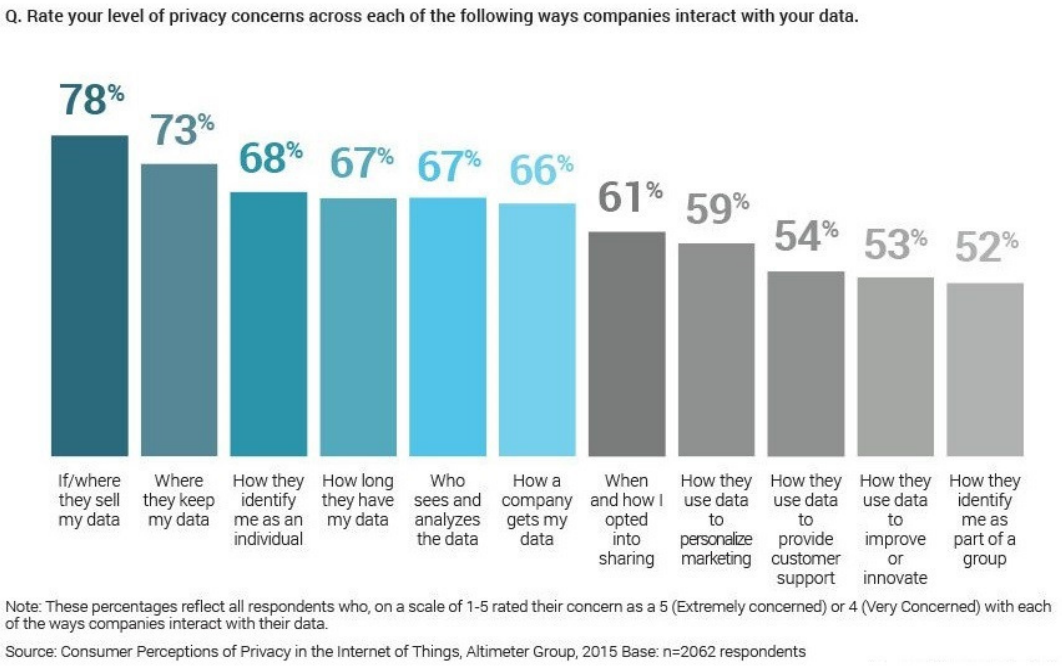

Figure 2 Consumers' top privacy concerns

IoT technology is being used in many domains right from healthcare to retail. To make things smarter around user, data of every move is collected and it is accessible to respective companies. Take an example of precise location collection through different applications, it may seem simple but these precise data can reveal user's all activities. Furthermore, sensors used in smart home helps user to monitor the activities of daily living can also give information about your private activities in home. Hence, it is proved that with the benefits of IoT, the privacy risks associated therein is the major bottleneck in adopting the IoT.

Privacy in IoT means protection of information of an individual from exposure in the IoT environment. Every individual has its own definition of privacy. For example, somebody might find it offensive if supermarket owner get to know the amount of milk left in smart fridge at the same time somebody find it quite useful as they are getting milk every day without bothering about its availability. Therefore, company should have to consider such scenario while designing a system which can give more benefits at the cost of confidentiality.

3. The Proposed Privacy versus Benefit Model

Privacy concern is the one of the major road block of IoT's success. Large number of consumers doesn't know how their personal data is being used and up to which level data is being accessed by the third party software. To increase the market demand, Companies need to develop a better way to communicate how data is used and shared.

As defined above, every individual has different level of concerns over IoT privacy. Hence, it will be prudent if IoT products classified based on their degree of privacy exposure so that the stage-wise mitigation policies can be made depending upon the quality of data. In this paper, we proposed to have a model called "Privacy versus Benefits Model" which can classify the IoT products regardless of the domain it belongs to. We tried to bring all IoT product to a same platform in the said model based on the quality of data being collected so that common policy can be drawn out.

For an instance; smart refrigerator and smart health monitoring fall in different domain as, utilities and healthcare respectively, but both uses the user's personal data. In which person may not mind if someone comes to know about the milk quantity in refrigerator as long as he/she is getting automating milk through stock maintenance facility, but the data received from the smart health monitoring is of related to person's health which have higher degree of sensitivity. Therefore, the consideration of degree of sensitivity of collected data.

If companies understand degree of sensitivity and focuses more on the lower degree of sensitive data to build the system then there shouldn't be any issue as long as consumers are getting benefits against the cost. Customers are more reluctant to accept the system which focuses on higher sensitive personal data. The figure 2 states consumers' top privacy concerns and it shows that most of the concerns can be solved by better communication with them. For example, if manufacturer assured them by

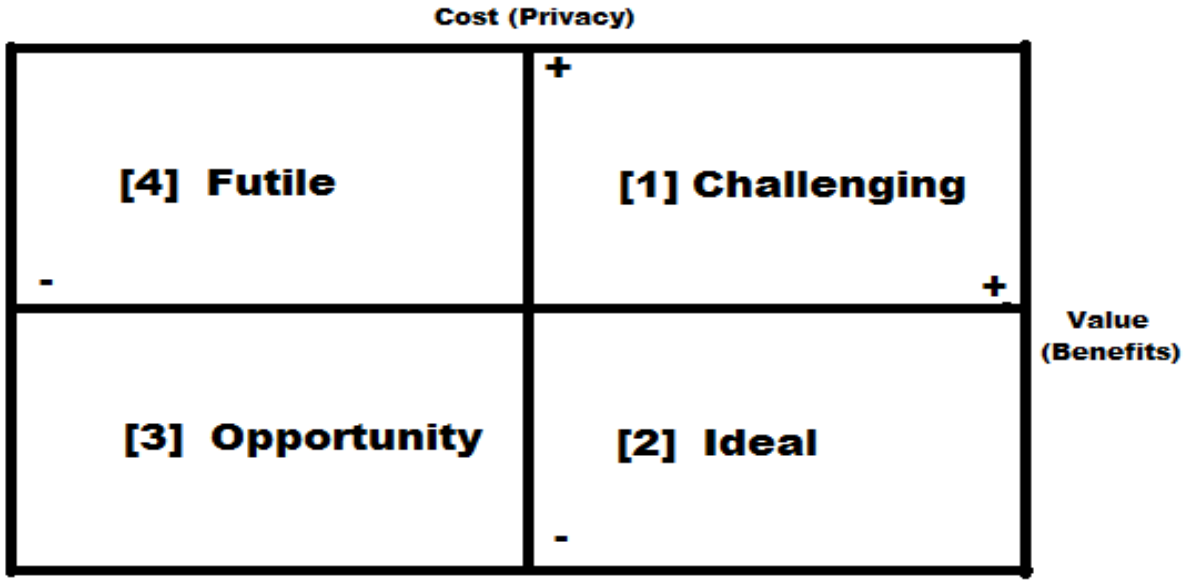

Figure 3 Privacy versus Benefit model

stating that they are not in favour of selling consumer's personal data as majority are in doubt that what if these personal data got sold to other vendor.
We focus to develop a model to classify the IoT product based on data sensitivity. This model helps company to manufacture better product and also company can make consumer carefree for their privacy through better communication.

In the proposed "Privacy versus Benefit Model", we classify IoT products in to four categories.

3.1 Challenging

This class of products use sensitive information about the consumer to give benefits in the returns. For instance, smart health reports, it takes data related to consumer's health as an input, keeps track of his/her health in reward. To resolve their concerns over privacy as it is an individual's Personally Identifiable Information (PII), company should have to make consumers less concern about their privacy by giving assurance for the following things:

- Consumer data is not being sold to other vendors,
- Only concern employees of the company has privileged to access their data,
- Data is been keep encrypted to make it confidential,
- Unwanted data is being destroyed on regular basis.

Many companies fail to communicate properly to their consumers so that fail to get their trust. We suggest to improve the communication with the consumer so that their concerns can be reduce up to some level and product can be categorize as Ideal product.

3.2 Ideal

This type of products gives high advantages in return of low sensitive data. It would be ideal product if consumers can get maximum rewards at minimum risk. For example, smart refrigerator – it can maintain the stock of daily household without human interference. This feature can give consumer daily availability of household item in return they just have to give away the quantity details to the supermarket system so that can supply the required items once safety stock is reached. Any IoT product can not fall into Ideal stage overnight it's a time consuming process. After improvising a few initial versions company can get mature product which falls into this category.

3.3 Opportunity

The group of product which gives very less benefits and same time uses less sensitive personal data falls into opportunity zone. As the name suggest these products have opportunity to be popular among consumers if they work on their offerings. Initial versions of most of the new product falls into this category as it provide only a few new benefits to consumers. They have to design more features so that consumers can get more benefits and product can fall into Ideal category where benefits can exceeds cost (privacy concern).

3.4 Futile

This class of product provide many limited benefits in return of high amount of sensitive personal data. It is very tough for any company to recover from this situation as it may cost them very hugely as they have to entirely start from the square to the power one. Many products fall into this category unknowingly as they fail to improve after being in challenging or opportunity zone in their initial versions.

As explained above every company's prime objective should be placing their product in Ideal class as it gives maximum benefit at the risk of minimum privacy. Most of the privacy apprehensions can be addressed if company wants to address it by placing strong privacy policy. So this model can be used as a guide for company developing IoT products so they can correctly provide optimal mixture of benefits and secrecy.

4. Conclusion

The proposed privacy versus benefit model helps organization in addressing consumers' privacy concerns by giving some simple suggestions and ponders on improving communication between consumers and organization. As discussed in paper privacy concerns of consumers can prove hindrance if these concerns are not properly addressed. But manufacture has to come up with strong privacy policy, data collection and sharing policy, data disposal policy in order to get trust of the consumers. Companies should focus on delivering optimal mixture of risk and rewards so that IoT can be helpful to consumers rather than being hindrance in their life.

References

[1] L. Atzori, A. Iera, G. Morabito, The Internet of Things: a survey, Computer Networks 54 (2010) 2787–2805.

[2] Jayavardhana Gubbi , Rajkumar Buyya , Slaven Marusic , Marimuthu Palaniswami , 'Internet of Things (IoT): A vision, architectural elements, and future directions', Future Generation Computer Systems 29 (2013) 1645–1660

[3] Chow C, Mokbel M. Privacy in location-based services: a system architecture perspective. Sigspatial Special 2009; 1(2):23–27

[4] Juels A. RFID security and privacy: a research survey. Selected Areas in Communications, IEEE Journal on 2006; 24(2):381 – 394, doi:10.1109/ JSAC.2005.861395.

[5] Renaud K, Ga andlvez Cruz D. Privacy: Aspects, ´ definitions and a multi-faceted privacy preservation approach. Information Security for South Africa (ISSA), 2010, 2010; 1 –8, doi:10.1109/ISSA.2010. 5588297.

Author Profile

Parth Desai is a student in Symbiosis Centre for Information Technology, Symbiosis International University. He is currently doing his Masters of Business Administration in Information Technology with Information Security as a major. His research interests are Information security, Product design, Business process management, Internet of Things e