International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Social Networking and Securing the IoT

Neha[1], Amit Jain[2]

[1]Student, Poornima Institute of Engineering and Technology, ISI-2, Sitapura, 302022, Jaipur
neha.sinha1805@gmail.com

[2]Asst. Prof., Poornima Institute of Engineering and Technology, ISI-2, Sitapura, 302022, Jaipur
amit.jain@poonima.org

Abstract: ***The development of internet of things needs issues related to things' service discovery and composition to be addressed. The novel paradigm of "social network of intelligent objects" based on the notion of "social relationships" among objects. The objects are capable of establishing social relationships in an autonomous way with respect to their owners with the benefits of improving the network scalability in information/service discovery because of theintegration of social networking concepts into the internet of things leading to the social internet of things paradigm.Through Internet Protocol (IP) connectivity, devices can now beconnected to the Internet, thus allowing them to be read, controlled,and managed at any time and at any place, but formulating a coherent security vision to enableIoT devices to securely communicate with each other in an interoperable manner is an important concern.***

Keywords: Internet of things, social networks, communication security.

1. Introduction

A complex architecture is required for the realization of an effective, efficient and reliable IoT that takes into account the issues of sensing the real world, transmitting data, and managing the relevant services to build applications [1]. The Internet of the Future is expected to have huge content-oriented traffic, intensive interactions between billions of persons, heterogeneous communications among hosts and smart objects, and provisioning of millions of services, with strict real-time requirements and flexibility in connecting everyone and everything. Key component of the Internet of Future is the Internet of Service, which is aimed at making every possible service widely and easily available through the Internet yielding to higher productivity. Strictly linked to the IoS is the Internet of Things, which is aimed at embodying into the Internet a large number of objects that through standard communication protocols and unique addressing schemes provide services to the final users.

IoTis envisioned to bring together billions of devices, also denoted as smart objects, by connecting them in an Internet-like structure, allowing them to communicate and exchange information and to enable new forms of interaction among things and people. Smart objects are typically equipped with a microcontroller, a radio interface for communication, sensors and/or actuators. Smart objects are constrained devices, with limited capabilities in terms of computational power and memory. They are typically battery-powered, thus introducing even more constraints on energy consumption: this motivates the quest for energy-efficient technologies, communication/networking protocols and mechanisms. The Internet Protocol (IP) has been widely envisaged as the true IoT enabler, as it allows to bring the full interoperability among heterogeneous objects [3].

2. Social IoT and Service Search

The Internet of Things (IoT) integrates a large number of heterogeneous and pervasive objects that continuously generate information about the physical world [4]. A SIoT network is based on the idea that every object can autonomously establish a connection for the desired service by using its relationships, queryinits friends and the friends of its friends in a distributed manner, guaranteeing an efficient and scalable discovery of objects and services following the same principles of social networks for humans.

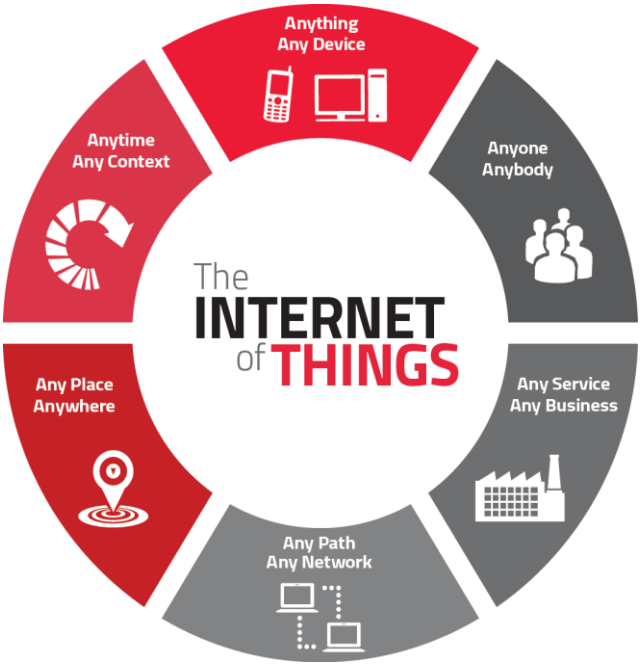

Figure 1: Connectivity in Internet of Things

The search of each specific service provided by the devices in the IoT represents a crucial challenge: the number of objects connected to the network is increasing exponentially, leading to an enormous searching space.A centralized system has been proposed in [5] where objects are contacted based on a prediction model that calculates the probability of matching the query. In this way, the search engine does not need to contact all the sensors leading to goods calability with the number of objects; nevertheless, it is not scalable with the network traffic, since the number of possible results

is significantly larger than the number of actual results, so a lot of sensors are contacted for no reason.

Like for human beings, one way of socialization among objects can be a *parental object relationship*, defined among similar objects, built in the same period by the same manufacturer. This relationship is easily implemented during the item production, will not change overtime and is only updated by events of disruption/obsolescence of a given device.

Moreover, objects can establish *co-location object relationship* and *co-work object relationship*, like humans do when they share personal or public experiences. These relations are determined whenever objects(e.g., sensors, actuators, RFID Tags, etc.) constantly reside in the same place (e.g., to offer home/industrial automation services) or periodically cooperate to provide a common IoT application, such as emergency response and telemedicine [6].A further type of relationship is *ownership object relationship*, defined for objects owned by the same user (mobile phones, game consoles, etc.). The last relationship is *social object relationship*, established when objects come into contact, sporadically or continuously, for reasons purely related to relations among their owners (e.g., devices/sensors belonging to friends).

Similarly to people exchanging their contacts (phone numbers, e-mail addresses, etc.), the device, if properly authorized, autonomously exchanges its social profile. The driving idea isthat devices with similar characteristics and profile can sharebest practice to solve problems already faced by "friends".

3. Security and Privacy

Inadequate security on Internet of Things devices could enable intruders to access and misuse sensitive information collected and transmitted by the device. In a complex system of Iot, introducing objects into the active control processes without human intervention, makes IoT security very difficult to address.

The confidentiality of private data and information is of utmost importance in order to ensure the privacy of users. The device authenticity can be easily achieved in network-dependent communication. However, in an autonomous network, device authentication is still an issue [7].The integrity of the data transmitted in huge amount of traffic that will be generated in the IoT environment needs to be ensured on an end-to-end basis on every link on a multi-hop route.
There are two types of security attacks in device-to-device communication in IoT:

1) *Inference attack*: This is an attack on privacy, which is carried out by logically or statistically studying data transmission patterns between devices.
2) *Distributed denial-of-service attack*:This can be carried out by jamming autonomous device-to-device communications to disable the operation of devices.

The general network architecture is divided into three layers: sensing layer, transport layer and application layer. The threat of RFID and Wireless sensor network's security are the major security problems of sensing layer . There are many security problems in the sensor network, such as external attack and link layer security, Witch attack, HELLO flooding attack, wormhole and sewage pool, selective forwarding attack, broadcast authentication and flooding etc.

The transport layer is composed of a variety of networks, including the internet, 3G communication network and the cloud computing platform, it is the centre of the whole network, it is in charge of the transmission and processing of information which is obtained by perception layer. Key technologies of the transport layer include long distance wired and wireless communication protocol, network integration technology and magnanimous intelligent information processing technology etc. There are many security problems in the transport layer, such as DOS attack, DDOS attack, impersonation attack, middleman attacks, cross heterogeneous network attacks etc. [8].

The application layer is interface between the Internet of things and users, which uses data mining, cloud computing, fuzzy recognition and other intelligent computing technologies to process magnanimous data and provide effective information.

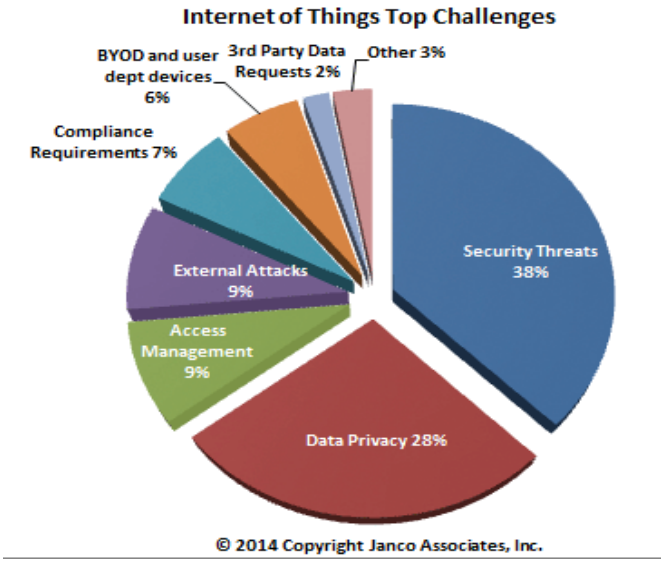

Figure 2: Challenges in IoT

Following are the measures to be taken to reduce security threats:
1. Quick and decisive actions need to be taken to manage and protect the label identity, to use communication technology and biological recognition technology, to protect RFID security and privacy better. Wireless sensor network is an important part of the sensing layer. The password and key technology, secure routing, secure data aggregation, security and privacy protection should be studied more comprehensive.
2. Transport layer security mechanism can be comprehensive utilization of point to point encryption and end-to-end encryption mechanism. In addition, we should strengthen the transport layer of the cross domain authentication and cross network authentication.

3. Strengthen the database access control policy, Strengthen authentication mechanism and encryption mechanism of different scenarios, strengthen the data tracing ability and network forensics capability and improve the network crime forensics mechanism, then establish a comprehensive, unified efficient safety management platform.

4. Conclusion

In this paper, we introduced the novel concept of social networking in Internet of Things, based on social relationship among objects, analogously to what happens for human beings. We also presented the issue of service search done by the objects in the complex network of IoT. The various types of relationship among objects in Iota and their contribution in search of service has been provided. The IoT has gained significant attention over the last few years. With the advances in sensor hardware technology and cheap materials, sensors are expected to be attached to all the objects around us, so these can communicate with each other with minimum human intervention. Finally, this paper presented the problems and solution of the Internet of things security problems. The communication between devices in Social Internet of Things has the ability to revolutionize every aspect of present day life by creating smart homes, smart grids, smart transportation, smart buildings, and smart cities. The Internet of things will bring a new round of development of the information industry, it will have a far-reaching impact on the economic development and social life.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of things: a survey,"*Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[2] P. Mendes, "Social-driven Internet of connected devices," *Proc. Interconn. Smart Objects with the Internet Workshop*, Lisbon,Portugal, 2011.
[3] Z. Shelby, K. Hartke, and C. Bormann. (Jun. 2013). *ConstrainedApplication Protocol (CoAP)*. RFC 7252 (Proposed Standard), InternetEngineering Task Force [Online]. Available: http://tools.ietf.org/html/rfc7252.
[4] D. Zhang, L. Yang, and H. Huang, "Searching in internet of things:Vision and challenges," in *Parallel and Distributed Processing with Applications (ISPA), 2011 IEEE 9th International Symposium on*, 2011,pp. 201–206.
[5] B. Ostermaier, K. Romer, F. Mattern, M. Fahrmair, and W. Kellerer, "Areal-time searchengineforthe web of things," in *Internet of Things(IOT), 2010*, 2010, pp. 1–8.
[6] H. Ning and Z. Wang;, "Future Internet of things architecture: likemankind neural system or social organization framework?" IEEE *Commun.Lett.*, vol. 15, no. 4, pp. 461–463, 2011.
[7] R. Laroia, "Future of wireless? The proximate Internet," presented at theCOMSNETS, Bangalore, India, Jan. 5–9, 2010.
[8] Wu Chuankun. A Preliminary Investigation on the Security Architectureof the Internet of things[J]. Strategy & Policy Decision Research, 2010, 25(4):411-419.

Author Profile

Nehais currently pursuing her B.Tech in Electronics and Communication stream from Poornima Institute of Engineering and Technology, Jaipur since 2011 and is in her final year (8th semester) right now. Her areas of interests are Internet of Things, Home Automation and Robotics.