Volume 5, Issue 4, 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Challenges of Security and Privacy Data Aggregation and Future Vision of Internet on Technologies

Dr. K. Vanitha
Asst.Prof,School of IT and Science
Dr.G.R Damodaran College of Science
Coimbatore, Tamil Nadu,
India

S. Vishnupriya
Research Scholar,School of IT and Science
Dr.G.R Damodaran College of Science
Coimbatore, Tamil Nadu,
India

Abstract-The Internet is a global network system that is interconnected with millions of computers. The Internet have an extensive range of information resources to communicate with worldwide. This paper contains security and privacy challenges and future vision of Internet on Technologies. The vision of the Internet of that individual object of day today life,such as cars, roadways, refrigerators that can equipped with sensor and which can useful to track information from the device.

The Implementation of IOT that require some specifications that are communication like WIFI, NFC, RFID, Hardware, Software, Protocols, and Cloud platform to communicate easily. some of these aspect are discussed in this paper.

Keywords-RFID(Radio-Frequency IDentification),NFC,WIFI

I. INTRODUCTION

Internet of Things (IoT) is a concept and a paradigm that considers pervasive presence in the environment of a variety of things/objects that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications/services and reach common goals. In this context the research and development challenges to create a smart world are enormous. A world where
the real, digital and the virtual are converging to create smart environments that make energy, transport, cities and many other areas more intelligent. The goal of the Internet of Things is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service.

The Internet of Things (IoT) is in a stage of adoption very similar to what we saw in 2008-10 around cloud computing and in 2011-2013 around big data analytics. Those two trends have been fully defined, and enterprises are actively deploying mission-critical enterprise applications utilizing those technologies. In 2015 we will likely see increased hype around IoT, but we will also begin to see some companies take the lead and implement innovative IoT solutions that increase operating efficiencies, improve customer experiences and drive innovation.
One way to think about "things" is by their communication patterns:

- human-to-human (H2H)
- human-to-thing (H2T)
- thing-to-thing (T2T)
- thing-to-things (T2Ts)

- Sensors, microcontrollers, sensor hubs, mobile devices and morehubs take in and compute data to relieve processing required on thesensor's application processor or the microcontroller
- Passive sensors collect and distribute information without the need for a person to activate the sensor each time data are processed

Examples: Proteus ingestible pill sensor, Eldercare in-home sensors, Find My
iPhoneChallenges: more talk about "ransomware"—the ability to threaten someone with
physical or other harm—as well as more conventional concerns unauthorized disclosure and use of data

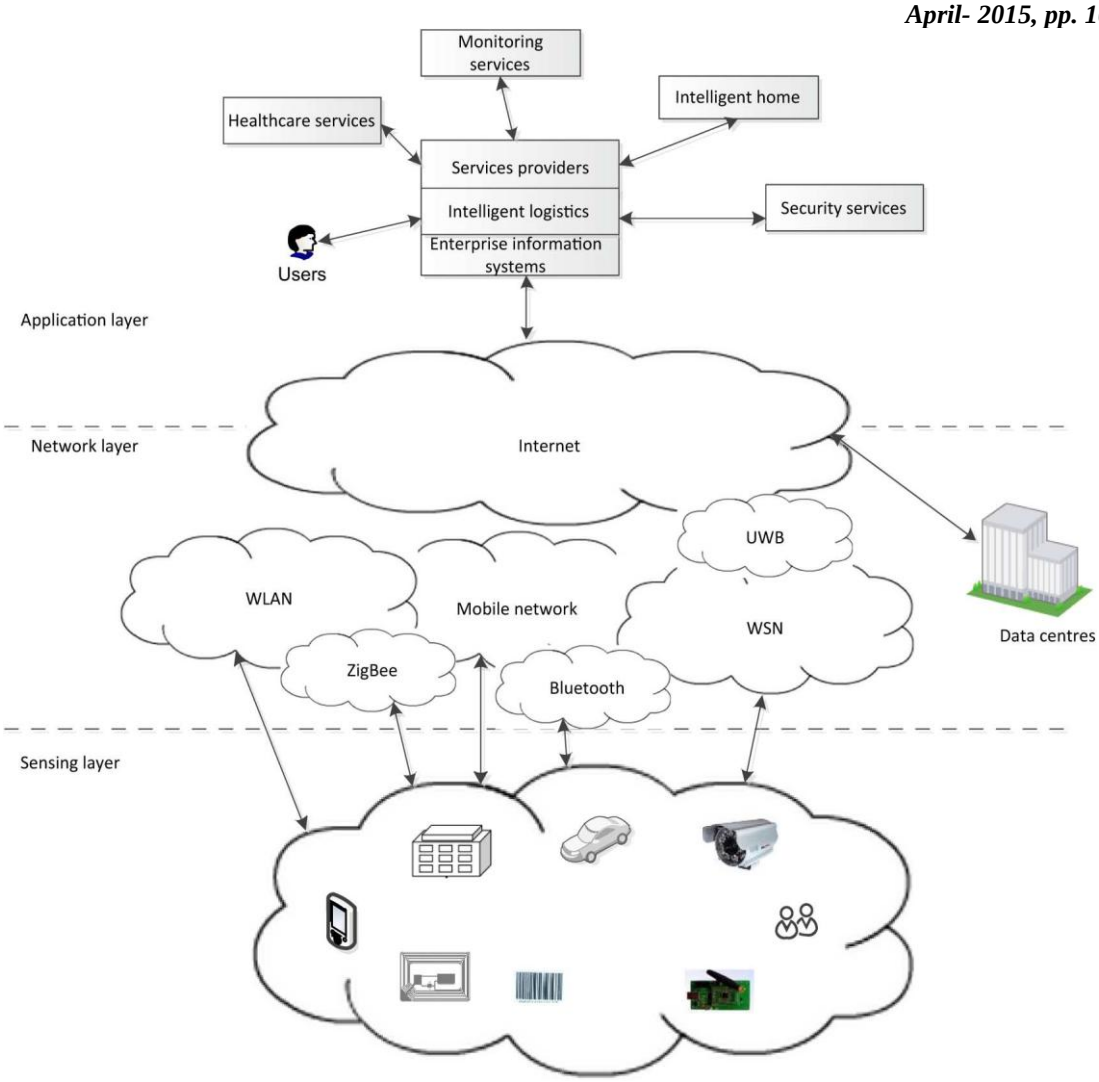

Fig 1.1.Architecture of Internet of Things

II. SECURITY AND PRIVACY CHALLENGES IN IOT

Privacy and security are an important concern in systems, which are as open as the internet of things. The issues of data privacy may arise both during data collection, and during data transmission and sharing. Privacy in data collection issues typically arise because of the widespread use of RFID technology, in which the tags carried by a person may become a unique identifier for that person. Privacy in data sharing and management may arise because much of the information being transmitted (eg. GPS location) can be sensitive, but it may also be required (on an aggregate basis) to enable useful real-time applications such as traffic analysis. In this section, we will discuss both issues. In addition, a number of security issues also arise involving the access control of the managed data.The main concept of IoT is the ability to connect loosely defined smart objects and enable them to interact with other objects, the environment, or more complete and legacy computing devices.

2.a. PRIVACY CHALLENGES ON DATA

As discussed above, the ability to track the RFID data with covert readers is a significant challenge in the data collection process. We have discussed details of methods for reducing the privacy risks in the data collection process in the chapter on RFID processing in this book[2].The tags are encrypted, and the reader is able to decrypt them when they send them to the server, in order to determine the unique metainformation in the tag. The reader also has the capability to re-encrypt the tag with a different key and write it to its memory, so that the (encrypted) tag signal for an eavesdropper is different at different times. Such a scheme provides additional protection because of repeated change in the encrypted representation of the tag, and prevents the eavesdropper from uniquely identifying the tag at different times.

Blocker tags exploit the collision properties of RFID transmission, which are inherent in this technology. The key idea is that when two RFID tags transmit distinct signals to a reader at the same time, a broadcast collision occurs, which prevents the reader from deciphering either response. Such collisions are in fact very likely to occur during the normal operation of the RFID infrastructure. In order to handle this issue, RFID readers typically use anti-collision protocols. The purpose of blocker tags is to emit signals (or spam) which can defeat these anti-collision protocols, thereby causing the reader to stall. The idea is that blocker tags should be implemented in a way, that it will only spam unauthorized readers, thereby allowing the authorized readers to behave normally. Details of the blocking approach are discussed in [2].

2.b. PRIVACY IN DATA SHARING AND MANAGEMENT

The functionality of the internet of things is based on the data communication between different entities, and the underlying data may often be person-centric, the ability to provide privacy during the data transmission and sharing process is critical. For example, in a mobile application, the GPS data for a user may be collected exactly, but may not necessarily be shared exactly. Many applications may require only aggregate information collected by the sensors, rather than exact information about individuals. For example, traffic conditions in a vehicular sensing applications can be inferred with the use of aggregate data.

Privacy preferences enable users to specify what information can be provided to whom in different contexts. They also allow users to specify obfuscation rules, which control the accuracy or inaccuracy of the information provided in response to different queries under different conditions.

III. TECHNOLOGIES USED IN IMPLEMENTATION OF INTERNET ON TECHNOLOGIES

3.a.RFID-ISO/IECStandardslist

A radio-frequency identification system uses tags, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response. The readers generally transmit their observations to a computer system running RFID software
or RFIDmiddleware.

RFID tags can be either passive, active or battery assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery assisted passive (BAP) has a small battery on board and is activated when in the presence of a RFID reader.

Frequency: 120–150 kHz (LF), 13.56 MHz (HF), 433 MHz (UHF), 865-868 MHz (Europe)902-928 MHz (North America) UHF, 2450-5800 MHz (microwave), 3.1–10 GHz (microwave)
Range: 10cm to 200m
Examples: Road tolls, Building Access, Inventory

3.b. NFC - ISO/IEC 18092 and ISO/IEC 14443-2,3,4, JIS X6319-4

NFC is a set of short-range wireless technologies, typically requiring a distance of 10 cm or less. NFC operates at 13.56 MHz on ISO/IEC 18000-3 air interface and at rates ranging from 106 kbit/s to 424 kbit/s. NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target. This enables NFC targets to take very simple form factors such as tags, stickers, key fobs, or cards that do not require batteries. NFC peer-to-peer communication is possible, provided both devices are powered.

Frequency: 13.56 MHz
Range: < 0.2 m
Examples: Smart Wallets/Cards, Action Tags, Access Control

3.c. WiFi (Alliance)

Wi-Fi is a technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed Internet connections. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards

Frequency: 2.4 GHz, 3.6 GHz and 4.9/5.0 GHz bands.
Range: Common range is up to 100m but can be extended.
Applications: Routers, Tablets, etc

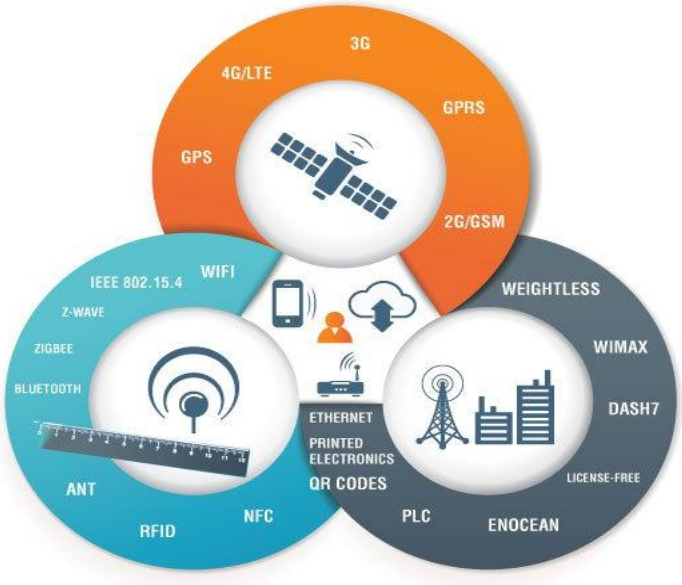

Fig 1.2. Technologies used in IOT

IV. FUTURE VISION OF INTERNET ON TECHNOLOGIES (2014-2015)

IoT has stepped out of its infancy and is on the verge of transforming the current static Internet into a fully integrated Future Internet.A schematic of the interconnection of objects is depicted in fig.1.3., where the application domains are chosen based on the scale of the impact of the data generated. The users span from individual to national level organizations addressing wide ranging issues.A Cloud implementation using *Aneka*, which is based on interaction of private and public Clouds is presented. We conclude our IoT vision by expanding on the need for convergence of WSN, the Internet and distributed computing directed at technological research community.

Our future vision of IoT is to make everything like an autonomous robot. This is a truth, which should be reached, but nowadays, this is not easy to accomplish. Science, there are more things which are passiveTo accomplish these two simple characteristics, we need camera, image processing technique, processor, actuator, and intelligent program to adapt the smart board motion. All of these components are needed for transforming the active thing from static situation (i.e., with human controlled) to smartness.

Fig.1.3. Future of IOT

IoT Visions

- 53 per cent are using IoT projects to optimise existing businesses and 47 percent as a strategic business investment
- Target audiences for IoT solutions include consumers (42 percent), business (54 percent) and internal use by employees (51 percent)
- 96 per cent have faced challenges with their IoT projects

Iot is Not Delivering Full POtential Because of Data Challenge

- Only 8 per cent are fully capturing and analysing IoT data in a timely fashion
- 86 per cent of stakeholders in business roles say data is important to their IoT project
- 94 per cent face challenges collecting and analysing IoT data

Better IoT Data Collection And Analysis would Deliver More Value

- 70 per cent say they would make better, more meaningful decisions with improved data
- 86 per cent report that faster and more flexible analytics would increase the ROI of their IoT investments

4.1. Future Technologies

Internet of things has wide application areas today some of them can be Health and wellness, Transport, Energy, Security, Communication.Some applications that are

4.1.1. Waste Management

Detection of rubbish levels in containers to optimize the trash collection routes. In the field of retail its application includes Supply Chain Control: Monitoring of storage conditions along the supply chain and product tracking for traceability purpose.

4.1.2. Medical and healthcare systems

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers or advanced hearing aids.[4]. Intelligent Shopping ApplicationGetting advice at the point of sale according to customers habits , preferences , presence of allergic components for them.

4.1.3. Environmental monitoring

Environmental monitoring applications of the IoT typically utilize sensors to assist in environmental protection by monitoring air or water quality,atmospheric or soil conditions,and can even include areas like monitoring the movements of wildlife and their habitats.[43] Development of resourceconstrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IoT devices in this application typically span a large geographic area and can also be mobile

V. CONCLUTION

The internet of things is a vision, which is currently being built. It is based on the unique addressability of a large number of objects which may be RFID-based tags, sensors, actuators, or other embedded devices, which can collect and transmit data in an automated way.The consolidation of international initiatives is quite clearly accelerating progress towards an IoT, providing an overarching view for the integration and functional elements that can deliver an operational IoT.

REFERENCES

[1] C. C. Aggarwal, T. Abdelzaher. Social Sensing. Managing and Mining Sensor Data, Springer, 2013

[2] C. C. Aggarwal, J. Han. A Survey of RFID Data Processing, Managing and Mining Sensor Data, Springer, 2013.

[3] http://www.charuaggarwal.net/iot.pdf

[4] Ersue, M; Romascanu, D; Schoenwaelder, J; Sehgal, A (4 July 2014). "Management of Networks with Constrained Devices: Use Cases". IETF Internet Draft < draft-ietf-opsawg-coman-use-cases>

[5] R. Angles, C. Gutierrez. Querying RDF Data from a Graph Database Perspective, ESWC, 2005. [14] K. Ashton. That 'Internet of Things' Thing. In: RFID Journal, 22 July, 2009.

[6] Y. Rogers, Moving on from Weiser's vision of calm computing: engaging ubicomp experiences, in: UbiComp 2006: Ubiquitous Computing, 2006.

[7] Ashton Kevin "That Internet of Things "Things in the real world things matter more than ideas,RFID Journal(2009).

[8] Extracting Value From the Massively Connected World of 2015Online: www.gartner.com/DisplayDocument?id=476440.

[9] R. Caceres, A. Friday, Unicom systems at 20: progress, opportunities, and Challenges, IEEE Pervasive Computing 11 (2012)

[10] Internet of things – Converging Technologies for smart Environments and Integrated Ecosystems-Ovidiu Vermesan, Peter Friess,2013.

[11] Analysys Mason, "Imagine an M2M world with 2.1 billion connected Things", online at http://www.analysysmason.com/aboutUs/news/insight/M2M_forecast_Jan2011/

[12] E. Savitz, "Gartner: Top 10 Strategic Technology Trends For 2013" online at http://www.forbes.com/sites/ericsavitz/2012/10/23/gartner-top-10-strategictechnology-trends-for-2011

[13] The Internet of Things: A survey Luigi Atzori a, Antonio Iera b, Giacomo Morabito,Elvisier(2010)

[14] Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions ,Jayavardhana Gubbi,a Rajkumar Buyya,b* Sla ven Marusic,a Marimuthu Palaniswamia, Elvisier (2013).

[15] The Internet of Things,How the Next Evolution of the Internet Is Changing Everything ,Dave Evans(2011), Cisco IBSG ,2011

[15] M. Atre, V. Chaoji, M. J. Zaki, J. Hendler. Matrix "Bit" loaded: A Scalable Lightweight Join Query Processor for RDF Data, WWW Conference, 2010.

[16] L. Atzori, A. Iera, G. Morabito, The Internet of Things: A Survey, Computer networks, 54(16), pp. 2787–2805, 2010

[17] M. Balazinska et al. Data Management in the World Wide Sensor Web, Pervasive Computing, April–June, 2007.

[18] D. Beckett. The Design and Implementation of the Redland RDF Application Framework. WWW Conference, 2001.

[19] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, M. Szydylo. Security Analysis of a Cryptographically Enabled RFID Device, USENIX Security, 2005. [20] V. Bonstrom, A. Hinze, H. Schweppe. Storing RDF as a graph. LA-WEB, 2003.

[21] A. Broring et al. New Generation Sensor Web Enablement, Sensors, 11(3), 2011.

[22] M. Buettner, B. Greenstein, A. Sample, J.R. Smith, D. Wetherall. Revisiting smart dust with RFID sensor networks, Proceedings of ACM HotNets, 2008.

[23] C. Bornhovd, T. Lin, S. Haller, J. Schaper. Integrating Automatic Data Acquisition with Business Processes Experiences with SAP's Auto-Id Infrastructure, VLDB Conference, 2004.

[24] J. Broekstra, A. Kampman, and F. van Harmelen. Sesame: A generic architecture for storing and querying RDF and RDF Schema. ISWC, 2002.

[25] V. Bychkovskiy, S. Megerian, D. Estrin, M. A. Potkonjak. collaborative approach to in-place sensor calibration. IPSN Conference, 2003

