Challenges and Concerns of Privacy in Internet of Things

Gousiya Begum [#1], Dr.M.Ramabai[*2], Dr.M.Chandra Mohan[#3]
[#1] Assistant Professor CSE MGIT Hyderabad T.S. India
[#1] Professorand HOD IT MGIT Hyderabad T.S. India
[#1] Professor CSE JNTUH CEH Hyderabad T.S. India

Abstract

Emergence of Social networking and wide range of smart devices and Internet applications has lead to creation of extremely large sets of complex data referred as BIGDATA. IOT is interconnection of physical things using intelligent devices like sensors etc. and operating them with ease[1]. IoT together with the other emerging Internet developments such as Internet of Energy, Media, People, Services, Business/Enterprises are the backbone of the digital economy, the digital society and the foundation for the future knowledge based economy and innovation society. IoT will very soon generate huge amount of gigantic data which will make BIGDATA more and more complex. IoT will optimize our resource utilization, monitor and track anything from a remote location.

Billions of devices are going to be connected to Internet in very near future. IoT and BIGDATA are going to influence our life style in great deal. Apart from the scope and opportunities of IOT there are many concerns for the users of BIGDATA in the form of Data storage and security, Legal issues, location Data etc. As on today lot of private data is stored in a remote place which user does not own and operate. There is no accountability on how the data is accessed. IoT will push lot of personal data to the web leading to one more major issue concerned to individual privacy.

Thus the present study of this paper is concerned primarily to investigate possible options of ensuring privacy for data pertaining to IOT, monitoring, tracing and authorizing access to private data.

Keywords — *IoT(Internet of Things), BIGDATA, privacy.*

I. INTRODUCTION

Internet of Things and Big Data will fundamentally change the world in the next few years. In a nutshell, IoT is concerned with the network of physical entities with embedded technologies to sense, collect, communicate and interact with their internal states and/or the external environment. Big Data is on the subject of extremely large data sets that may not be analyzed computationally via traditional methods to reveal patterns, trends, and associations, especially related to human behavior and interactions.

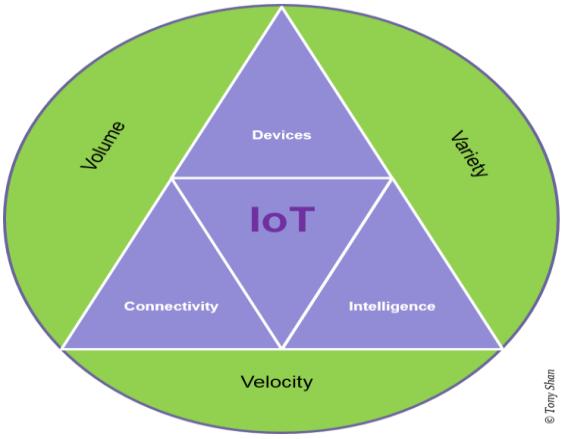

Fig. 1 Big Data and IoT

Processing all of the data from the IoT is an exercise in big data. Various types and formats of data streams from different devices and sensors in IoT are handled and transformed by the "variety" of Big Data collection. The vast amount data influx from IoT are ingested and stored by the "volume" of Big Data loading. The near real-time processing and analysis of explosive data from IoT are performed in a timely manner by the "velocity" of Big Data analytics. To a large extent, IoT and Big Data are two sides of the same coin [2]. Big data becomes the foundational enablers for IoT, providing the building blocks for IoT to operate. On the other hand, IoT becomes the source and channel of massive data, events and signals, and in turn leverages the Big Data to interact, collaborate and correlate with each other to generate tangible results and impacts on consumers, enterprises and the society. They are complimentary when IoT meets Big Data.

We are connecting nearly everything – from cars and buildings to clothing and light bulbs – to the Internet. Network equipment manufacturer Cisco reports that there are 25 billion networked devices in the world today and predicts that there will be 50 billion by 2020 [3].

The sensors, along with our smart phones, tablets, and computers, generate twice as much data today as earlier, and this trend is expected to continue. Sensors that are so small and efficient that they can power themselves with ambient radio waves are becoming a reality. As a result, data is becoming cheaper to collect and keep, it is coming from an

incredibly diverse range of sources – including the physical world around us – and our ability to analyze all of this data is constantly improving. These developments pose difficult challenges for privacy, security and fairness in our society. The data from connected devices will be deeply personal, and big data analytics will make the data more readily actionable. Some of these devices will handle deeply sensitive information about our health, our homes, and our families. Some will be linked to our financial accounts, some to our email accounts. And devices themselves will be more closely connected with our actions in the physical world, making data security and device security critically important.

To help consumers navigate and benefit from this complex, uncertain, and exciting world, the Internet of Things and big data analytics need to meet consumers' expectations and earn their trust. Appropriate privacy and security protection, as well as broader assurances that customers are being treated fairly are the key elements of consumer trust.

Consumers want to know – and should be able easily to find out – what information companies are collecting, where they're sending it, and how they're using it. This kind of information is important to consumers' decisions about whether to use digital products and services in the first place. The FTC (Federal Trade Commission) came to this realization early in the history of the commercial Internet. But many companies, including data brokers, ad networks, and analytics firms, operate in the background with consumer data, and their activities can significantly affect consumers. While consumers might benefit from the activities of some of these "behind the scenes" operators – by receiving more relevant advertising, for example – consumers should have choices about where their data ends up and how it is used. Consumer choice is enhanced by giving consumers "just in time" information, at key moments when it is most relevant to them, such as when they are deciding to download an app or make purchases on a connected device. But companies should also help consumers navigate the complex ecosystem of data, devices, and big data analytics operating behind the scenes, so that consumers understand the practices that can affect them, and exercise choices about the practices. Companies that provide connected devices should recognize that providing transparency will require some creative thinking. Visual and auditory cues, and immersive apps and websites should be employed to describe to consumers, in a meaningful and relatively simple way, the nature of the information being collected. The same signals should be used to provide consumers with choices about whether any of this information can be used by entities or persons who fall outside the context in which the consumer is employing the device, and in which the consumer expects her information to remain private. Another promising tool for providing information to consumers, as well as allowing them to exercise meaningful choices, is the "command center" that companies are now developing to run multiple household connected devices. The driving force here is convenience, but these command centers could also provide an opportunity for consumers to understand the information their devices are generating, and to control where that information goes. After all, if you can have a centralized interface to program your garage door, thermostat, television, refrigerator, and who knows what else, you ought to be able to use that same interface to make meaningful choices about the data your devices will collect and where they will send it.

II. IOT ARCHITECTURE

Internet of Things(IoT) evolves around the central concept : "a world-wide network of interconnected objects", where objects can be addressable through unique identity, accessible through Internet (sometimes via intelligent interface), self organized and repairable.

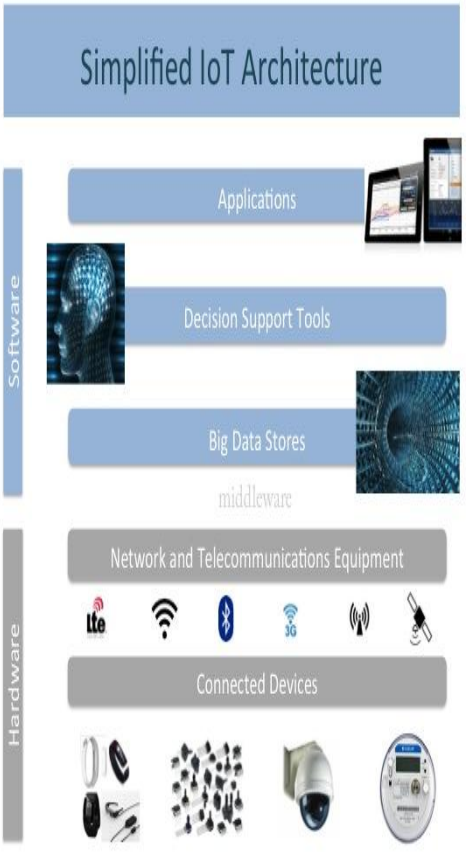

Fig. 2 IoT Architecture

The foundation layer to IoT is the Connected Devices. These devices contain processors, memory and sensors that enable you to discover something about the device, it history, its current operating state

or something about the environment it is located. Sensors include such things gyro / fingerprint reader, / barometer / hall (recognizes whether cover is open/closed) / RGB ambient light / gesture / heart rate / accelerometer / proximity / compass / GPS / temperature/ etc.

These sensors require networks to communicate and become useful. Historically, devices report status via their external display (flashing light, led, screen), then more sophisticated via terminal port, and now, with low-cost reliable networks, via communication protocols, over wi-fi, bluetooth 3G and other networks. This is the Network and Communications layer in the architecture.

The Big Data Stores are the next important layer of the architecture [4]. The plural is intended, as a solution may have more different types of storage requirements, i.e. images, value pairs (time and reading), audio. It is now affordable to store the data that proliferation of sensors produce. The advent of big data solutions like Hadoop, Cassandra, MongoDB and MapR. means that the large amounts of data collected can be captured, stored, analysed, curated, searched, shared, much beyond the capability of traditional relational database systems such as Oracle.

The next layer relates to Decision Support Tools . Without automation the sheer quantity of data is unmanageable and largely unusable. For example, temperature readings from a thermostat can easily be stored and display, but when processed can start to provide some useful information – i.e. average temperature at time of day, variance of current measure to the average, to the last reading, to the last 5 readings, etc.

The Application layer is where the business functionality lives. Whether it is an iphone app that tells you your home alarm has activated or a complex piece of scheduling software that is using multiple data points from sensors to schedule predictive maintenance of large assets.

III.CHALLENGES OF IOT

IoT trends to be unified, seamless, and pervasive. Large scale service deployment needs to be framed within a set of standards [5]. The development of IoT is a step-by-step process. There are still many problems to be solved, such as low power nodes and computing, low cost and low latency communication, identification and positioning technologies, self-organized distributed systems technology, and distributed intelligence.

The IoT provides many new opportunities to the industry and end user in many application fields. Currently, however, the IoT itself lacks theory, technology architecture, and standards that integrate the virtual world and the real physical world in a unified framework [6]. Following key challenges are thus listed.

A. Architecture Challenge:

IoT encompasses an extreme wide range of technologies. IoT involves an increasing number of smart interconnected devices and sensors (e.g., cameras, biometric, physical, and chemical sensors) that are often nonintrusive, transparent, and invisible. As the communications among these devices are expected to happen anytime, anywhere for any related services, generally, these communications are in a wireless, autonomic, and ad hoc manner. In IoT, data integrations over different environments are thus tough and will be supported by modular interoperable components. Infrastructure solutions will require systems to combine volumes of data from various sources and determine relevant features, to interpret data and show their relationships, to compare data to historical useful information, and support decision-making. Single reference architecture thus cannot be a blueprint for all applications. Heterogeneous reference architectures have to coexist in IoT. Architectures should be open, and following standards, they should not restrict users to use fixed, end-to-end solutions. IoT architectures should be flexible to cater for cases such as identification (RFID, tags), intelligent devices, and smart objects (hardware and software solutions).

B. Technical Challenge:

IoT technology can be complex for variety of reasons. First, there are legacy heterogeneous architectures in the existing networking technologies and applications, e.g., different applications and environments need different networking technologies, and the ranges as well as other characteristics of cellular, wireless local area network, and RFID technologies are much different from each other [7]. Second, communication technologies, including fixed and mobile communication systems, power line communications, wireless communication, and short-range wireless communication technologies, for both fixed and mobile devices, either simple or complicated, should be low cost and with reliable connectivity. At last, there are thousands of different applications; it is in natural to have different requirements on what parties need to communicate with each other, what kind of security solutions are appropriate, and so on.

C. Hardware Challenge:

Smart devices with enhanced inter-device communication will lead to smart systems with high degrees of intelligence. Its autonomy enables rapid deployment of IoT applications and creation of new services. Therefore, hardware researches are focusing

on designing wireless identifiable systems with low size, low cost yet sufficient functionality. As the bandwidth of IoT terminals could vary from kbps to mbps from sensing simple value to video stream, requirements on hardware are diverging. However, two requirements have been nevertheless the essentials: one is the extremely low power consumption in sleep mode and the other is ultra low cost. Suppose the sleeping time over active time is one million, the leakage power of an IoT terminal shall at least be one million time less than that of active. It is so far impossible when an IoT terminal is sleeping and receiving RF signals. It will be even difficult when using advanced CMOS silicon with relatively more leakage power. Hardware and protocol code sign for sleeping has been thus the first hardware challenge of IoT. Billions of IoT terminals will be used; the cost of an IoT terminal must be ultra low. However, so far, there is no low cost positioning solution for IoT, especially the positioning precision of a short-range IoT terminal must be high. Low active power is also a challenge for low-cost terminal [8]. Traditionally, low cost equals to lower performance or longer process latency. Longer processing latency ends up to higher energy consumption. As the spectrum resource is very limited at the lower part in L band, IoT may use higher RF such as the frequency bands higher than 5 GHz. The higher the RF, the more power consumption from RF PA will be. In another way, not yet used very narrow spectrum band between two used bands may have to be used by future IoT. To use very narrow band with strong power neighbors, the cost of passive component will not be low and that will definitely be a potential challenge in the future.

D. Privacy and Security Challenge:

Compared with traditional networks, security and privacy issues of IoT become more prominent [9]. Much information includes privacy of users, so that protection of privacy becomes an important security issues in IoT. Because of the combinations of things, services, and networks, security of IoT needs to cover more management objects and levels than traditional network security. Existing security architecture is designed from the perspective of human communication, may not be suitable and directly applied to IoT system. Using existed security mechanisms will block logical relationship between things in IoT. IoT needs low-cost- and M2M-oriented technical solutions to guarantee the privacy and the security. In many use cases, the security of a system has been considered as a general feature. Related research shall focus on privacy control. Low cost, low latency, and energy-efficient cryptography algorithms and related flexible hardware will be essential for sensor or device.

E. Standard Challenge:

Standards play an important role in forming IoT. A standard is essential to allow all actors to equally access and use. Developments and coordination of standards and proposals will promote efficient development of IoT infrastructures and applications, services, and devices. In general, standards developed by cooperated multiparties, and information models and protocols in the standards, shall be open. The standard development process shall also be open to all participants, and the resulting standards shall be publicly and freely available. In today's network world, global standards are typically more relevant than any local agreements.

F. Business Challenge:

For a mature application, its business model and application scenario are clear and easy to be mapped into technical requirements. So the developers do not need to spend much time on business-related aspects. But for IoT, there are too many possibilities and uncertainties in business models and application scenarios. It is thus inefficient in terms of business-technology alignment, and one solution will not fit possibilities for all. The IoT is a challenging traditional business model. Although small-scale applications have been profitable in some industries, it is unsustainable when extended to other industries. In the early stage of IoT development, business aspects should be considered to reduce the risk of failure.

Objective: Primary objective of this paper is to design and develop an ecosystem where privacy preservation can be ensured and even security of the personal data generated from IoT enabled devices.

IV. LITEARTURE SURVEY

Golbeck and Mauriello [10] have shown that the average Facebook users significantly underestimate the amount of data they that they give access to third party applications. Moreover, they also noted that most of us tend to overlook the privacy [11] terms and policies on the Web. In the IoT era, the amount of user data that can be collected can be significantly higher. For example, recent wearable technologies, such as Google Glass, Apple iWatch, Google Fit, Apple Health Kit, and Apple Home Kit may collect very sensitive information about users, ranging from their health conditions to financial status by observing/recording daily activities. It is noteworthy to mention that to succeed in the IoT marketplace, product and service providers need to gain the consumer confidence [12]. We note that privacy issues during the Internet age did receive significant attention over the last few years. For example, 'allegation of governments spying on their citizens' to the new laws such as 'right to be forgotten' [13] has opened up a whole range of debate. Compared to the Web era, the IoT is more

vulnerable to privacy violations. Therefore, researchers as well as IT professionals will pay more attention towards IoT technologies, business models, and potential regulatory efforts to ensure that a more secure and privacy preserved IoT data management techniques are developed.

TRUSTe [14] highlighted the fact that privacy concerns could be a significant barrier to the growth of IoT. According to the TRSUTe survey, about 60% of internet users have basic privacy awareness of IoT and they know that smart devices, such as smart TVs, fitness devices, and in-car navigation systems could collect personal activities data. Moreover, 85% of the Internet users would like to understand more about data collection. Furthermore, 88% of the respondents wanted to control the data collection from the smart devices. Finally, the survey revealed that 87% of internet users were concerned about the type of personal information collected.

The FTC recognized three major privacy concerns: facilitation of the collection of large amounts of consumer data, using that data in ways unexpected by the consumer, and security of data. This ubiquitous data collection makes the Internet of Things a much more data driven economy. With massive quantities of continuous data, new discoveries can be made, but little to no regulation can by harmful to the consumers. Privacy issues are especially hard to discuss because, by nature, privacy is subjective. The FTC aims to promote three best practices: privacy by design, simplifed consumer choice, transparency. Companies have to make an effort to build consumer protection in from the beginning.

V. SCOPE OF PRIVACY IN IoT

As much of the information in an IoT system may be personal data, there is a requirement to support anonymity and restrictive handling of personal information [1]. There are a number of areas where advances are required:

• Cryptographic techniques that enable protected data to be stored processed and shared, without the information content being accessible to other parties. Technologies such as homomorphic and searchable encryption are potential candidates for developing such approaches.

• Techniques to support Privacy by Design concepts, including data minimisation, identification, authentication and anonymity.

• Fine-grain and self-configuring access control mechanism emulating the real world. There are a number of privacy implications arising from the ubiquity and pervasiveness of IoT devices where further research is required, including:

• Preserving location privacy, where location can be inferred from things associated with people.

• Prevention of personal information inference, that individuals would wish to keep private, through the observation of IoT-related exchanges.

• Keeping information as local as possible using decentralised computing and key management.

• Use of soft identities, where the real identity of the user can be used to generate various soft identities for specific applications. Each soft identity can be designed for a specific context or application without revealing unnecessary information, which can lead to privacy breaches.

VI. STATE OF THE ART: ACADEMIC RESEARCH START

Lab of Things (LoT) [15] by Microsoft Research is a flexible platform that uses connected devices in homes. It enables researchers to easily interconnect devices and implement application scenarios, and sharing of data, code and participants, which further lowers the barrier to evaluate ideas in a diverse set of homes. However, the LoT assumes that the privacy concerns must be manually handled where the deployer must sign an agreement with data owners.

Hub of All Things (HAT) (hubofallthings.com), Funded by the EPSRC, is an ongoing project that aims at developing data markets to support trading data generated by the IoT solutions in smart home environments. The HAT does not address privacy issues. Its primary goal is to provide an API so that the home owners can push data to the cloud.

There also are a number of industrial efforts to build IoT platforms. Xively (xively.com) offers a Platform as a Service that allows IoT devices to connect to the cloud. It does not address any privacy issues other than that it will provide secure data storage. In Xively, privacy protection is the responsibility of the person who builds applications and services using the Xively platform.

Datacoup (datacoup.com) is a new start-up that will allow users to sell personal data. Primarily, their focus is on social media data, such as Facebook, Twitter, and YouTube. Currently, Datacoup does not focus on IoT data. Datacoup is among the few initiative that focuses on trading any kind of personal data. Datacoup pays $8 for each user1 that shares data. However, users have to trust Datacoup completely as Datacoup will sell user data through their own servers. Mydex (mydex.org) is a British social-enterprise helping to make it easier and safer for individuals to hold, control, and re-use their personal information in effective and secure ways. Mydex is also a personal data sharing platform.

VII. CONCLUSIONS

Collecting data through IoT solutions and analyse them in large-scale have a significant value to offer for both individual users and businesses. Further, it can also make significant impact towards society in general through increase productivity and reducing wastage. However, existing technologies and regulations are not sufficient to support privacy guaranteed data management life cycle. From the time the data is being captured by the sensors embedded in IoT solutions to the point where knowledge is extracted and raw data is be permanently and securely deleted, user privacy need to be protected and enforced. By doing this only the IoT solutions can gain the confidence of the consumers. Limitation of the technology will need to be mitigated by strict laws and regulation that would include strict and serious penalties for offenders and misusers.

REFERENCES

[1] Dr. Ovidiu Vermesan, Dr. Peter Friess,"Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems", River Publishers

[2] Andrea Molinari, Vincenzo Maltese, Lorenzino Vaccari, Andrea Almi , Eleonora Bassi,"Smart Cities White Papers Big Data and Open Data for a Smart City", IEEE TN

[3] U.S. Federal Trade Commissioner Julie Brill," Privacy and Data Security in the Age of Big Data and the Internet of Things", Washington Governor Jay Inslee's Cyber Security and Privacy Summit, January 5, 2016

[4] "Simplified IoT Architecture", October 2, 2014

[5] Shanzhi Chen, HuiXu, DakeLiu, Bo Hu, and Hucheng Wang, "A Vision of IoT: Applications, Challenges and Opportunities With China Perspective", IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 4, AUGUST 2014

[6] R. Kranenburg and A. Bassi, "IoT challenges," Commun. Mobile Comput.,vol. 1, no. 1, pp. 1–5, 2012.

[7] Y. Chen et al., "Time-reversal wireless paradigm for green Internet of Things: An overview," IEEE Internet Things J., vol. 1, no. 1, pp. 81–98, Feb. 2014.

[8] S. Lanzisera et al., "Communicating power supplies: Bringing the internet to the ubiquitous energy gateways of electronic devices," IEEE Internet Things Journal., vol. 1, no. 2, pp. 153–160, Apr. 2014.

[9] H. Ning et al., "Cyberentity security in the Internet of Things," Computer, vol. 46, no. 4, pp. 46–53, Apr. 2013.

[10] J. Golbeck and M. L. Mauriello, "User Perception of Facebook App Data Access: A Comparison of Methods and Privacy Concerns," University of Maryland, Maryland, 2014.

[11] D. Miorandi, S. Sicari, F. D. Pellegrini and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks , vol. 10, no. 7, pp. 1497-1516, 2012.

[12] H. Sundmaeker, P. Guillemin, P. Friess and S. Woelffle, "Vision and Challenges for Realising the Internet of Things," Cluster of European Research Projects on the Internet of Things, 2010.

[13] European Commission, "Proposal For A Regulation Of The European Parliament And Of The Council," European Commission, Brussels, 2012.

[14] TRUSTe, "Internet of Things Industry Brings Data Explosion, but Growth Could be Impacted by Consumer Privacy Concerns," TRUSTe Research, 29.05.2014. Available:http://www.truste.com/blog/2014/05/29/internet-of-things-industry-brings-data-explosion-but-growth-could-be-impacted-by-consumer-privacy-concerns/.

[15] A. B. Brush, E. Filippov, D. Huang, J. Jung, R. Mahajan, F. Martinez, K. Mazhar, A. Phanishayee, A. Samuel, J. Scott and R. P. Singh, "Lab of Things: A Platform for Conducting Studies with Connected Devices in Multiple Homes," in Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication, New York, NY, USA, 2013.