Rethinking Security of the Ultimate Panopticon: The Internet of Things

Sridipta Misra

School of Computer Science
McGill University
Montreal, Canada

December 2014

A thesis submitted to McGill University in partial fulfillment of the requirements for the degree of Master of Science.

Dedication

Dedicated to Ma-Baba, Dada, Didun, and the love of my life, Reetica, for their unconditional and unceasing love, belief and support. Also, to the entire research community, who with their hard work, make this world a better place!

Acknowledgements

Foremost, I would like to express my heartfelt gratitude to my adviser Prof. Muthucumaru Maheswaran for his patience, motivation, enthusiasm, and profound knowledge. His continuous guidance and feedback helped me to improve the quality of my research and thesis writing.

I thank my fellow lab-mates in *Advanced Network Research Lab*: Fan Jin, Debashish Ghosh, Vaibhav Somani, Bhaskar Pilania, Feier Chen, Mariam Nouh and Peter Henderson for their insightful inputs and stimulating discussions, and for all the fun we have had together. I am thankful to the *School of Computer Science, McGill University* for all the facilities and resources that they provided to make my learning and research effective and interesting.

Last but not the least, I would like to thank my family for supporting me through my thicks and thins. Many thanks to Reetica Nag for proofreading my thesis. Thanks to Laetitia Sabatier and Ismail Badawi for translating my thesis's abstract to French.

Abstract

The Internet has quickly evolved from being merely a medium for accessing interlinked hypertext documents across computers to the mighty Internet of Things (IoT). The IoT is still in its infancy and is yielding impressive benefits through unprecedented associations of real world problems and technological solutions. This is impairing our ability to perceive novel vulnerabilities that the IoT presents. With the enormous amount of data and control that the cyber space would possess in the future, extending security and privacy solutions of the Internet, to the IoT might prove to be a catastrophic decision. Hence, it is best to rethink the security and privacy of the IoT.

This thesis attempts to comprehensively recognize and analyze the vulnerable features of the IoT, which could be exploited to pose various forms of threats to the IoT ecosystem. The thesis also presents a threat taxonomy for the IoT. Three broad classes of threats have been established: *System Security Threats*, *Privacy Threats*, and *Reflective Trust and Reputation Threats*. Under each class, threats have been specialized based on relevant factors. The taxonomy is designed to create specialized *threat spaces*. This would refine threat recognition and safeguarding during the device and application design and deployment phases, and detection, isolation and containment of attacks during the operational phase. This thesis organizes the available and developing solutions to mitigate these threats, and discusses some directions of future works.

Finally the thesis proposes the novel philosophy of *Social Governance*, which recognizes the service and device manufacturers, the policy makers, and the users of the devices and services, as the three pivotal drivers of a networked society. It endorses development of a new framework to facilitate the free flow of information among the drivers to foster an expeditious, organized and secure IoT development. The framework would optimize policy formulation, enforcement (through *Hierarchical Distributed Policy Management System*) and adherence (through *Policy Compliant Smart Devices*). Formulating comprehensive threat taxonomies for the IoT, like the one proposed in this thesis and designing an exclusive framework for the IoT to promote adequate information flow and effective implementation of security and privacy would contribute in building a robust networked society.

Résumé

L'Internet a rapidement évolué de sa position originale en tant que série de documents hypertextes interreliés entre ordinateurs vers un réseau comprenant une multitude d'appareils et d'objets communiquant à travers divers protocoles; l'Internet des Objets (idO). Encore sous sa phase de développement, cet idO prodigue des résultats impressionnants par son application de solutions technologiques à des problémes bien réels. Ces résultats masquent les vulnérabilités potentielles présentées par cet idO. Dans un futur proche, appliquer les méthodes de sécurité et de confidentialité courantes utilisées par l'Internet pour contrôler les quantités massives d'information gérées dans le cyberespace à l'idO pourrait prouver catastrophique. Il serait plus logique de repenser ces méthodes de sécurité et de confidentialité de l'information.

Cette thèse tente de reconnaître et d'analyser les vulnérabilités de l'idO qui pourraient être exploitées afin de compromettre son écosystéme. Elle présente aussi une taxonomie des menaces pour l'idO. Trois classes de menaces sont établies: *les menaces à la sécurité du systéme*, *les menaces à la confidentialité*, et *les menaces réfléchissantes à la confiance et la réputation*. Sous chaque classe, les différentes menaces ont été spécialisées selon différents facteurs. La taxonomie est créée pour définir des espaces spécialisés de menaces; ceci permettrait d'affiner la reconnaissance des menaces et d'offrir de la protection durant la phase de conception et de déploiement des appareils, ainsi que de détecter, d'isoler et de contrer les attaques durant la phase opérationnelle. Cette thése organise les solutions disponibles et en développement pour atténuer ces menaces et examine les directions futures.

Finalement, cette thèse propose la nouvelle philosophie de *Gouvernance Sociale*, philosophie qui reconnaît comme les trois pivots du réseau; le manufacturier, les gestionnaires et les usagers. Elle recommande le développement d'un nouveau cadre pour faciliter le transfert d'information entre les pivots pour encourager un développement rapide, organisé et sécure de l'idO. Ce cadre optimiserait la formulation, la gérance (utilisant le *Système Hiérarchique Distribué de Gestion de la Politique*) et l'adhérence (utilisant des *Appareils Intelligents Conformant à la Politique*) aux politiques d'utilisation. La formulation de taxonomies des menaces pour l'idO, comme celles proposées dans cette thèse et la création d'un cadre

exclusif pour l'idO pour promouvoir la circulation adéquate de l'information et l'implémentation efficace de mesures de sécurité et de confidentialité contribuerait à bâtir une réseautique robuste.

Contents

List of Figures

Chapter 1

Introduction

1.1 Motivation

"In a few decades time, computers will be interwoven into almost every industrial product."
-Karl Steinbuch, German computer science pioneer, 1966.

Not only has this vision of Karl Steinbuch been realized for decades now, the term *'connectivity'* is being redefined with the Internet of Things (IoT). With smartphones, tablets and ultra portable laptops having already revolutionized how, when and where people get connected, makers of sensors and other networked endpoints are looking to take things to the next level with an even more sophisticated ecosystem of devices. The vision of 50 billion connected devices by 2020 [3], suggests that anything that can benefit from being connected, will be connected. This rapid evolution of the traditional Internet into the IoT is empowering the exploration of countless domains of utilities that were previously unimaginable. At the same time, it is also making the society vulnerable to newer forms of threats and attacks in many more ways than any precursor network forms. This is because the gamut of application of the IoT is much richer. With the IoT, computing and connectivity is becoming much more pervasive and ubiquitous. The IoT's cybersecurity and privacy implications are as popular a topic as its business impact [4].

The evolution of the IoT and the advancement of computing capabilities in general, would set off an arms race between the security community and the cy-

bercriminals [4]. The productivity achieved through equipping a large number of environments with Wi-Fi, Bluetooth or radio devices cannot be ignored, but the security and management of the unprecedented volume of data captured by these smart environments is still highly uncertain and unclear.

Protection of data has been an issue ever since the first two computers were connected. With commercialization of the Internet, security concerns expanded to encompass user privacy, financial transactions, and cybertheft threats. In the IoT, security is inseparable from safety. Whether accidental or malicious, interference with the controls of a pacemaker, a car, or a nuclear reactor could be catastrophic.

The IoT is criticized for being developed rapidly without appropriate consideration of the profound security challenges involved and the necessary regulatory changes [5]. As the IoT spreads widely, cyber attacks are likely to become increasingly physical (and not simply virtual) [6]. In January 2014, Forbes listed many Internet-connected appliances like televisions, kitchen appliances, cameras, and thermostats that can already "spy on people in their own homes" [7]. Computer-controlled devices in automobiles such as brakes, engine, locks, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the onboard network. These devices are currently not connected to external computer networks, and so are still not vulnerable to Internet attacks [8, 9]. The possibility of an intruder being able to remotely regulate the refrigerator, start the heater, unlock the doors, deploy airbags while you are driving without any crash, or turn a running car's steering wheel is frightening.

The U.S. National Intelligence Council realized the severity of the situation and stated that it would be hard to deny "access to networks of sensors and remotely-controlled objects by enemies of the United States, criminals, and mischief makers. An open market for aggregated sensor data could serve the interests of commerce and security no less than it helps criminals and spies identify vulnerable targets" [10].

A comprehensive security for the IoT would encompass securing the devices/sensors, securing the data, and securing that across an open network, which is a massive challenge. The access to personal data is probably one of the biggest changes in the future, and unless managed and secured adequately, it can result in severe personal, industrial or societal destruction. Hence, it is very critical to understand

what the security model for the IoT would look like [4].

Another challenge, that we recognize, in order to ensure systematic and secure application of the IoT is strict definition and limitation of the roles of each actors in the functioning of the system. The IoT is bringing the cyber space and the physical space even closer. The physical world is being directly interfaced, through the machines/things, to the virtual world. Although human intervention still exists in the forms of traditional communication and user control/manipulation over *things* (refer Section 2.2).

Human intervention increases the scope of undesired deviations in the system's behaviour due to malicious or accidental interferences. The machines should be able to operate as per the relevant policies with minimal of human mediation. The policies in turn should be highly context-specific and consensus-based. This would require maximum involvement of the users in policy formulation.

The thesis proposes a *"consensus-based dynamic policy formulation framework"* called *Social Governance*, which strives to:

- Maximize active participation of users in the *"dynamic policy formulation* and hence in the governance. Facilitate formulation of highly context-specific policies by considering the local consensus.
- Minimize the users' role in *"policy adherence"* to maximize policy compliance. Make the machines "smart" enough to obey the policies autonomously.

To ensure the evolution of the IoT into a robust and secure infrastructure in the future, all its proponents and stakeholders must align themselves towards a synergistic development of the IoT technologies, while upholding the stability, security and privacy of the society. As a part of these efforts, it is indispensable to exhaustively study the characteristics of the IoT, and recognize those which could potentially be exploited to pose any form of threat to either the IoT infrastructure or any of its stakeholders. Moreover, for a robust future of the IoT, a framework for the structured development and governance of the IoT is highly desirable. Despite the strong association, it is crucial to detach the development framework of the IoT from that of the traditional Internet [11].

1.2 Thesis Contribution

This thesis makes the following six major contributions:

- Presents a new system model for the IoT, recognizing the three layers of organization which comprises a composite IoT operation.
- Studies the potentially vulnerable features of the IoT from the viewpoint of security and privacy, and proposes a comprehensive *Threat Taxonomy*, which comprises the contribution of some previously established research works as well as several novel components proposed by this thesis.
- As part of the taxonomy, the thesis identifies a new genre of threats: *Reflective Trust and Reputation Threats*.
- Maps existing work into the threat space.
- Recognizes the required solutions for securing the IoT and discusses relevant ongoing works.
- Proposes the novel concept of *Social Governance*, which envisions a specialized framework to facilitate structured and stable development of the IoT. Social Governance recognizes the service and device manufacturers, the policy-making bodies, and the users of the devices and services, as the primary drivers of a networked society, and strives to establish a framework which allows active (and passive) participation of each of the drivers in all the activities throughout the life-cycle of an IoT service, i.e. in the development and implementation of the technologies, as well as their sound governance in the society. Social Governance Framework can be a solution to many of the threats discussed in the taxonomy, especially the privacy threats and some of the reflective trust and reputation threats.

1.3 Thesis Organization

Chapter 2 presents the background of the IoT: the system model, evolution of networks, its vision, applications and challenges. Chapter 3 discusses the vulnerable features of the IoT and presents the threat taxonomy. Chapter 4 attempts to

recognize and organize the solutions for holistically securing the IoT. Chapter 5 proposes Social Governance and the framework. Finally, Chapter 6 concludes the thesis and discusses the possible directions for future research work.

Chapter 2

System Model for the Internet of Things

2.1 The Concept of the "Internet of Things"

The phrase "Internet of Things" was coined about 10 years ago by the founders of the original MIT Auto-ID Center, Kevin Ashton in 1999 and David L. Brock in 2001 [12], who envisioned "a world in which all electronic devices are networked and every object, whether it is physical or electronic, is electronically tagged with information pertinent to that object." They envisioned use of physical tags that allow remote, contactless interrogation of their contents; thus, enabling all physical objects to act as nodes in a networked physical world. Realization of this vision will yield benefits in diverse areas including supply chain management and inventory control, product tracking and location identification, and human-computer and human-object interfaces [13]. Several technologies drive the IoT's vision. [12] comprehensively lists those technologies. The IoT's broad vision and the infancy of the research on it results in lack of standard definitions for the IoT. Few standard definitions provided by different researchers are:

- Definition by [14]: "Things have identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environment, and user contexts."
- Definition by [15]: "The semantic origin of the expression is composed by

two words and concepts: Internet and Thing, where Internet can be defined as the world-wide network of interconnected computer networks, based on a standard communication protocol, the Internet suite (TCP/IP), while Thing is an object not precisely identifiable. Therefore, semantically, the Internet of Things means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols."

- Definition by [16]: "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."

Considering these definitions, the IoT can be defined as a paradigm that considers pervasive presence in the environment of various things that through wireless and wired connections are able to interact and cooperate with other connected things to create seamless communication and contextual services, and reach common goals. An interconnection of highly heterogeneous networked entities, the IoT follows a number of communication patterns: human-to-human (H2H), human-to-thing (H2T), thing-to-thing (T2T), or thing-to-things (T2Ts) [17].

The IoT, a global network infrastructure, links uniquely identified physical and virtual objects, things and devices through the exploitation of data capture (sensing), communication and actuation capabilities [18]. The underlying infrastructure of virtually represented "things" in an Internet-like structure includes existing and evolving Internet and network developments [19]. Emerging services and applications will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability [19].

2.2 Evolution of the Networks

It is critical to look at the evolution of the composition and nature of networks over the years to be able to analyse the new areas of vulnerabilities that the IoT might introduce.

In the late 1960s, communication between two computers was made possible through a **basic computer network** [20]. In the early 1980s the TCP/IP stack was introduced. Then, commercial use of **the Internet** started in the late 1980s.

At this point the networks were all about pure peer-to-peer connections. You had networks and then you were connecting the networks together using IP protocols so that the machines could communicate with each other. Later, the **World Wide Web** (**WWW** or **the Web**) became available in 1991 which made the Internet more popular and stimulated its rapid growth. The pure Web started as a hub and spoke network model superimposed on top of the Internet. People (enterprises/institutions or exclusive web content developers) were setting up web servers (hubs) onto the existing Internet, and then people were just connecting to these hubs to access the content.

Later, with the emergence of services like the social networks, blogs and the microblogs, where people could actively access the web services to create their own content in the Web space, the people became a major source of content creation for the Web, and hence an active part of the network. Here, by content we mean the data in the Web, which is not meant to be private to a few users, but is publicly accessible to the Internet users, and can be mined by anyone. This form of the Web can be addressed at the **"Web of People (WoP)"**. The WoP modified the hub-spoke structure to introduce a more distributed and fine-grained network structures. Now the "hub" transformed into mostly service providers for the Internet users to create their own content, than simply accessing content at the hub. For example, Google's Blogger [21] or WordPress [22], which run services on their servers (the hubs), which people can access to create their own blog sites.

Over the years, the WoP underwent further transformations. The vision of making the Internet services more intuitive, accurate, context-aware and automated (less dependent on human mediation), has lead to a weaker association (or even complete exclusion) of the "people" from the loop, and inclusion of "things" into the networks [15]. From inanimate things like cars, lamps, gadgets etc., to animate things like plants and cattle, all those physical entities which directly affect or get affected by the virtual world are being included into the Web. This form of Web can be called the **"Web of Things (WoT)"** or the **"Internet of Things (IoT)"**. In case of the WoP, actions like blogging, did not affect the physical world right away. The people were the sensors, as they sensed the information and put it into the Web, or they received the information from the Web to act on it. The IoT strives for minimizing the human mediation in the sensing and feed-

ing of information into the virtual world, and/or associated actions carried out in the physical world based on the information in the virtual world [23]. With the IoT, the command and control plane is going to be embedded into the networking plane, which was actually human mediated up till this point. Figure 2.1 illustrates the five phases in the evolution of the Internet.

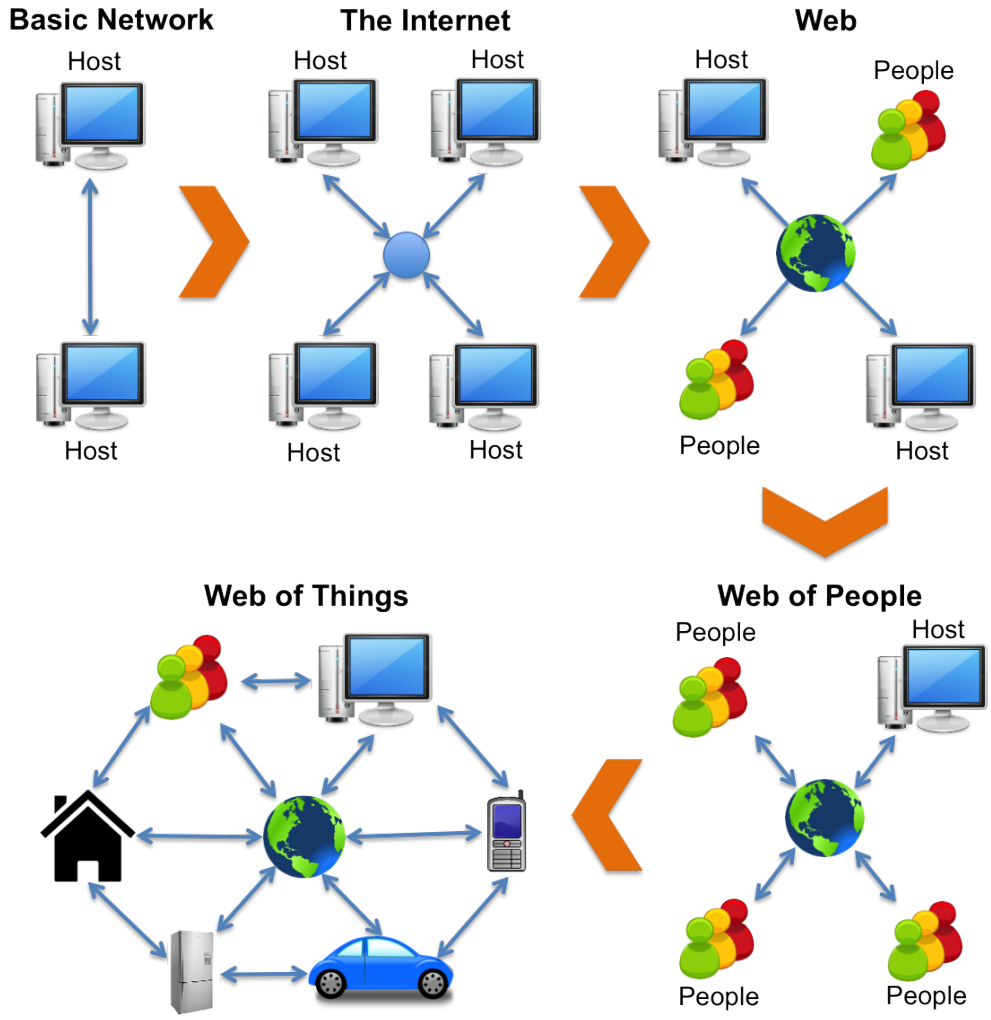

Fig. 2.1 Evolution of the Internet

We specialize these five network forms based on operations of the networks and the kinds of data managed by the network forms. The composite operation of an internet system can be organized into three layers: *perceptual layer*, *network and transport layer*, and *application layer* [24, 1]. The **Application Layer** rep-

Evolution of Networks ➔ / *Involved Components* ↓		***Internet***	***Web***	***Web of People***	***Web of Things (IoT)***
Content	***Machine Generated Content***	✖	✖	✖	✔
	User Generated Content	✖	✖	✔	✔
Operations	***Application Layer***	✔	✔	✔	✔
	Network & Transport Layer	✔	✔	✔	✔
	Perceptual Layer	✖	✖	✖	✔

Fig. 2.2 Network Forms and Operations and Data Types Supported

resents the intelligence for processing the data for achieving desired functionality. The **Network and Transport Layer** comprises infrastructure and technologies enabling wired/wireless connections, unique addressing schemes, and reliable and secure transmission and storage of the collected data. The **Perceptual Layer** comprises elements and technologies which help collect data from the real physical world and make it available to the virtual world. **User Generated Content** is the data that is actively contributed by the users of the Internet. **Machine Generated Content** is the data contributed in to system by the connected "things" as a result of their perception of the physical environment and/or processing of data. Figure 2.2 illustrates the operations and data supported by the different network forms.

Before the advent of the Internet, the physical world was manipulated by the actions of the people. Then came the Internet, the Web and the Web of People, where people were able to influence events in the physical world, though with the aid of the network technologies, but with much required human mediation. For example, a person on one part of the planet could perceive an event, and could communicate the information over the networks to another person/machine on the other side of the planet, who/which could then take certain actions accordingly.

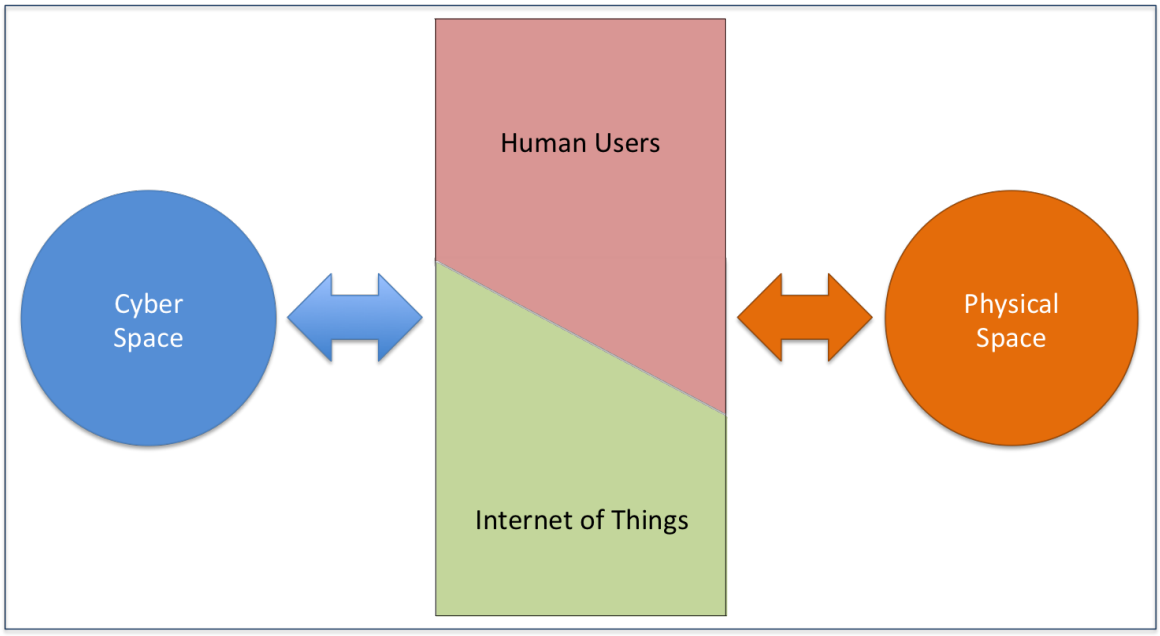

Fig. 2.3 Interaction of Cyber-Physical Spaces Through the IoT

With the IoT, the physical world is being directly interfaced, through the machines/things, to the virtual world (refer Fig. 2.3). However, it would not remove human intervention completely, as traditional communication forms are still valid. Also the things are controlled/manipulated by the users.

In an IoT-interfaced system, we can have three forms of interactions between the cyber-physical spaces:

- Interactions purely sensed and actuated by the users.
- Interactions sensed and actuated by machines controlled by local users.
- Interactions sensed and actuated purely by machines with remote user involvement.

If the human intervention is completely removed from the usage/execution cycle of the machines then the behaviour of the network systems would be much more predictable and secure as the machines would probably work according to a program and the program would be following a policy. It would help in avoiding

deviation from the expected behavior of the systems by minimizing the scope of malicious or accidental interferences due to human factors.

Moreover, it is desirable that the policies which govern the behaviour of technologies in any region should be highly context-specific and should be consensus-based. This could mean that the policies for a certain technology may change not only spatially, but maybe also temporally. For making the policies consensus-based, it is imperative to maximize the involvement of the users in the process of policy formulation.

Hence, an ideal framework for the IoT should be *"consensus-based dynamic policy formulation framework"*, which would consider an inter-play of two aspect:

1. Maximize active participation of human factors in the *"dynamic policy formulation"* and hence the governance. Facilitate formulation of highly context-specific policies by considering the local consensus.

2. Minimize the role of human factors in the *"policy adherence"* to maximize policy compliance. Make the machines "smart" enough to obey the policies and refuse any deviation from those.

2.3 Vision of the Internet of Things

2.3.1 Large scale ubiquitous and Pervasive Connectivity

The underlining vision of the IoT is to create a world where the real and the virtual are converging to create smart environments that makes energy, transport, cities and many other areas more intelligent [25]. Proponents of the IoT envision enablement of things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service [26]. It means enablement of communication via Internet to all the things that surround us. The IoT is much more than M2M communication, wireless sensor networks, 2G/3G/4G, RFID, etc. These are the enabling technologies for IoT applications.

Future storage and communication services will be highly pervasive and distributed: people, smart objects, machines, platforms and the surrounding space which is getting smart due to technologies like wireless/wired sensors, M2M de-

vices, RFID tags will create highly decentralized common pool of resources interconnected by a dynamic inter-networks. The "communication language" will be based on interoperable protocols, operating in heterogeneous environments and platforms. The IoT would use synergies generated by the convergence of consumers, businesses and industrial Internet [26], creating an open, global network of people, data, and things. This convergence leverages the cloud to connect intelligent things that sense and transmit a broad array of data, helping create services that would not be obvious without this level of connectivity and analytical intelligence.

2.3.2 Context-Aware Computing

A fundamental motivation behind the increasing popularity of the IoT has been the desired context-awareness of the computing elements to optimize their performance and to enable services customization according to the current situation with minimal human intervention. Although context-aware systems have been in the research epicenter for almost two decades now [27, 28], the ability to convey and select the most appropriate information to achieve non-intrusive behavior on multiuser-converged service platforms in mobile and heterogeneous environments remains a significant management challenge. Creation of smarter environments, entertainent and busincess applications, which are more supportive and suited to the user, would require acquiring, analyzing, and interpreting relevant context information [29] regarding the user [30].

2.3.3 Seamless Connectivity and Interoperability

Interoperability at the scale of the IoT must go beyond syntactical interfaces and requires the sharing of common semantics across all software architectures. It also demands a seamless integration of existing computational artifacts (hardware and software) and communication infrastructures. Only then can context information be successfully shared between highly adaptive services across heterogeneous devices on large-scale networks that consider this information relevant.

2.3.4 Network Neutrality

The IoT has remained on the periphery of the network neutrality battle because it is primarily comprised of small, power-efficient devices generating a small amount of traffic. However, with the creation of smart environments through integration of multiple smart and intercommunicating devices, the bandwidth consumption has become much substantial. This, along with the explosion of connected devices, means the IoT will not be able to escape the implications of the network neutrality debate for too long.

As a part of the IoT vision, [31] emphasizes on the significance of network neutrality. It states,"no bit of information should be prioritized over another so the principle of connecting anything from/to anybody located anywhere at anytime using the most appropriate physical path from any-path available between the sender and the recipient is applied in practice. For respecting these principles, the Internet service providers and the governments need to treat all data on the Internet equally, not discriminating or charging differentially by user, content, site, platform, application, type of attached equipment, and modes of communication."

Though advocates against net neutrality have valid arguments supporting their stance, for example, when networks are overloaded, say at sporting events or during disasters, being able to shed non-critical traffic may be important for emergency services and the devices they may depend upon, there is a downside should network neutrality be overturned. The risk of vendor lock in is high and it is quite possible to see situation where, for instance, AT&T enters into an agreement with Google to provide the public network capabilities for Nest home automation devices, and this could result in Nest customers suffering a substandard service if they choose another provider.

2.4 Applications of the Internet of Things

The 2010 Internet of Things Strategic Research Agenda (SRA) [16] identified and described the main IoT applications, which span numerous diverse applications, into six vertical domains: *smart energy, smart health, smart buildings, smart transport, smart living* and *smart city*. Successful realization of the vision of a pervasive

IoT would require unification of these diverse vertical application domains into a single, unified, horizontal domain, often referred to as *"smart life"* [26].

Based on inputs from experts, surveys [32] and reports [33], the European Research Cluster on the Internet of Things identified the IoT application domains [16, 34]. [26] presents an updated enumeration of the application domains.

- **Cities**
  - **Smart Parking:** Monitoring parking spaces availability in the city.
  - **Structural health:** Monitoring vibrations and material conditions in buildings, bridges and historical monuments.
  - **Noise Urban Maps:** Real time sound monitoring in centric zones.
  - **Traffic Congestion:** Monitoring vehicles and pedestrian levels to optimize driving and walking routes.
  - **Smart Lightning:** Intelligent and weather adaptive street lighting.
  - **Waste Management:** Detection of rubbish levels in containers to optimize the trash collection routes.
  - **Intelligent Transportation Systems:** Smart Roads and Intelligent Highways with warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.
- **Environment and Water**
  - **Forest Fire Detection:** Monitoring combustion gases and preemptive fire conditions to define alert zones.
  - **Air Pollution:** Control of carbon dioxide emissions of factories, pollution emitted by cars and toxic gases generated in farms.
  - **Landslide and Avalanche Prevention:** Monitor soil moisture, vibrations and earth density to detect dangerous patterns in land conditions.
  - **Earthquake Early Detection:** Distributed control in specific places of tremors.

  - **Water Quality:** Study water suitability in rivers and the sea for fauna and eligibility for drinkable use.
  - **Water Leakages:** Detection of liquid presence outside tanks and pressure variations along pipes.
  - **River Floods:** Monitoring water level variations in rivers, dams and reservoirs.

- **Energy Smart Grid, Smart Metering**
  - **Tank level:** Monitoring water, oil and gas levels in storage tanks and cisterns.
  - **Smart Grid:** Energy consumption monitoring and management.
  - **Photovoltaic Installations:** Monitoring and optimization of performance in solar energy plants.
  - **Water Flow:** Measuring water pressure in water transportation systems.
  - **Silos Stock Calculation:** Measuring emptiness level and weight of the goods.

- **Security and Emergencies**
  - **Perimeter Access Control:** Access control to restricted areas and detection of people in non-authorized areas.
  - **Liquid Presence:** Liquid detection in data centres, warehouses and sensitive building grounds to prevent break downs and corrosion.
  - **Radiation Levels:** Distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts.
  - **Explosive and Hazardous Gases:** Detecting gas levels and leakages in industrial environments, around chemical factories and inside mines.

- **Retail and Logistics**
  - **Supply Chain Control:** Monitoring storage conditions along the supply chain and product tracking for traceability purposes.

  - **NFC Payment:** Payment processing based in location or activity duration for public transport, gyms, theme parks, etc.
  - **Intelligent Shopping Applications:** Getting advice at the point of sale according to customer habits, preferences, presence of allergic components for them or expiring dates.
  - **Smart Product Management:** Control rotation of products in shelves and warehouses to automate restocking processes.
  - **Quality of Shipment Conditions:** Monitoring vibrations, strokes, container openings or cold chain maintenance for insurance purposes.
  - **Item Location:** Search of individual items in big surfaces like warehouses or harbours.
  - **Storage Incompatibility Detection:** Warning emission on containers storing inflammable goods close to others containing explosives.
  - **Fleet Tracking:** Control of routes followed for delicate goods like medical drugs, jewels or dangerous merchandises.

- **Industrial Control**
  - **M2M Applications:** Machine auto-diagnosis and assets control.
  - **Indoor Air Quality:** Monitoring toxic gas and oxygen levels inside chemical plants to ensure workers and goods safety.
  - **Temperature Monitoring:** Control temperature inside industrial and medical fridges with sensitive merchandise.
  - **Ozone Presence:** Monitoring ozone levels during the drying meat process in food factories.
  - **Indoor Location:** Asset indoor location by using active (ZigBee, UWB) and passive tags (RFID/NFC).
  - **Vehicle Auto-diagnosis:** Information collection from CAN Bus to send real time alarms to emergencies or provide advice to drivers.

- **Agriculture and Animal Farming**

  - **Wine Quality Enhancing:** Monitor soil moisture and trunk diameter in vineyards to control sugar content in grapes and grapevine health.
  - **Green Houses:** Control micro-climate conditions to maximize the production of fruits and vegetables and its quality.
  - **Golf Courses:** Selective irrigation in dry zones to reduce the water resources required in the green.
  - **Meteorological Station Network:** Study weather conditions in fields to forecast ice formation, rain, drought, snow or wind changes.
  - **Compost:** Control humidity and temperature levels in alfalfa, hay, straw, etc. to prevent fungus and other microbial contaminants.
  - **Offspring Care:** Control growing conditions of the offspring in animal farms to ensure its survival and health.
  - **Animal Tracking:** Location and identification of animals grazing in open pastures or location in big stables.
  - **Toxic Gas Levels:** Study ventilation and air quality in farms and detection of harmful gases from excrements.

- **Domotic and Home Automation**
  - **Energy and Water Use:** Energy and water supply consumption monitoring to obtain advice on how to save cost and resources.
  - **Remote Control Appliances:** Switching on and off remotely appliances to avoid accidents and save energy.
  - **Intrusion Detection Systems:** Detection of window and door openings and violations to prevent intruders.
  - **Art and Goods Preservation:** Monitoring conditions inside museums and art warehouses.

- **eHealth**
  - **Fall Detection:** Assisting elderly/disabled people living independently.

- **Medical Fridges:** Control conditions inside freezers storing vaccines, medicines and organic elements.
- **Sportsmen Care:** Vital signs monitoring in high performance centres and fields.
- **Patients Surveillance:** Monitoring conditions of patients inside hospitals and in old peoples home.
- **Ultraviolet Radiation:** Measuring UV sun rays to warn people not to be exposed in certain hours.

Furthermore, [26] identifies the research challenges in the applications of the IoT which have been prioritized by the IERC for the coming years.

2.5 Challenges

The challenges toward fulfilling the visions for the IoT include at least the following four aspects:

- **Cost:** The prices of WSN components should be low to support their large-scale deployment. This requirement dictates resource constraints in these devices. Existing network security protocols do not consider these constraints.
- **Data Management:** The IoT will be a major source of big data, contributing massive amounts of streamed information from billions of inter-connected objects. Typical IoT applications producing big data include meteorology, experimental physics, astronomy, biology, and environmental science. For eg., as per [35] a Boeing jet generates 10 TB of data per engine every 30 minutes. A single six-hour flight would thus generate some 240 TB of data, and there are about 28,537 commercial flights in the US skies on any given day. An A380 has more than 300,000 sensors on board constantly generating data streams. Clearly, M2M communications will generate enormous Internet traffic leading to Zettabyte science [36].
- **Security:** Compared to traditional networks, the IoT comprises more number and forms of networks and connected things. Also it is designed to

foster newer forms of interactions. These and few more factors (discussed in Chapter 3), gives rise to newer security issues.

- **Privacy:** The devices of WSN may be unable to defend all forms (physical and cyber) of attacks. Sensitive information may be leaked.

Strengthening the IoT's security is a major challenge. Being still an immature technology, a major issue affecting the acceptance and applicability of the IoT is the lack of a mature and comprehensive security model and standards.

Figure 2.4 illustrates the risks and threats faced by the three operational layers of the IoT. Major security challenges to the Perceptual Layer are physical damage to the nodes, channel blocking, forgery attacks, fake attacks, copy attacks, replay attacks, and information tampering. The Transport Layer is majorly threatened by attacks like DoS/DDoS attacks, counterfeiting/middleman attacks, heterogeneous network attacks, application risks of IPv6, conflicts of WLAN application, and the traditional network security threats. For the Application Layer, information disclosure, illegal human intervention, unstable platform, and authentication are major challenges.

Since the IoT merged the traditional Internet, wireless communication networks, WSN and other networks, the existing security technologies can provide some security for the IoT, such as the deployment of the user authentication, access control and security audits in the application layer and VPN, firewall and other security policies in the network layer. However, the existing security solutions cannot provide comprehensive security to the three layers. To design a security model for the IoT which would comprise reusable existing security solutions for the Internet and other existing network forms, and novel solutions exclusively for the IoT, is a major research challenge. Figure 2.5 depicts the three categories in which [37] identifies the IoT security issues.

- **Internet's own security issues:** Inherited from traditional Internet environment. Can be solved by using traditional security solutions. Example: data eavesdropping, tampering, forgery, denial of service attacks, man-in-the-middle attacks and other common Internet attacks.

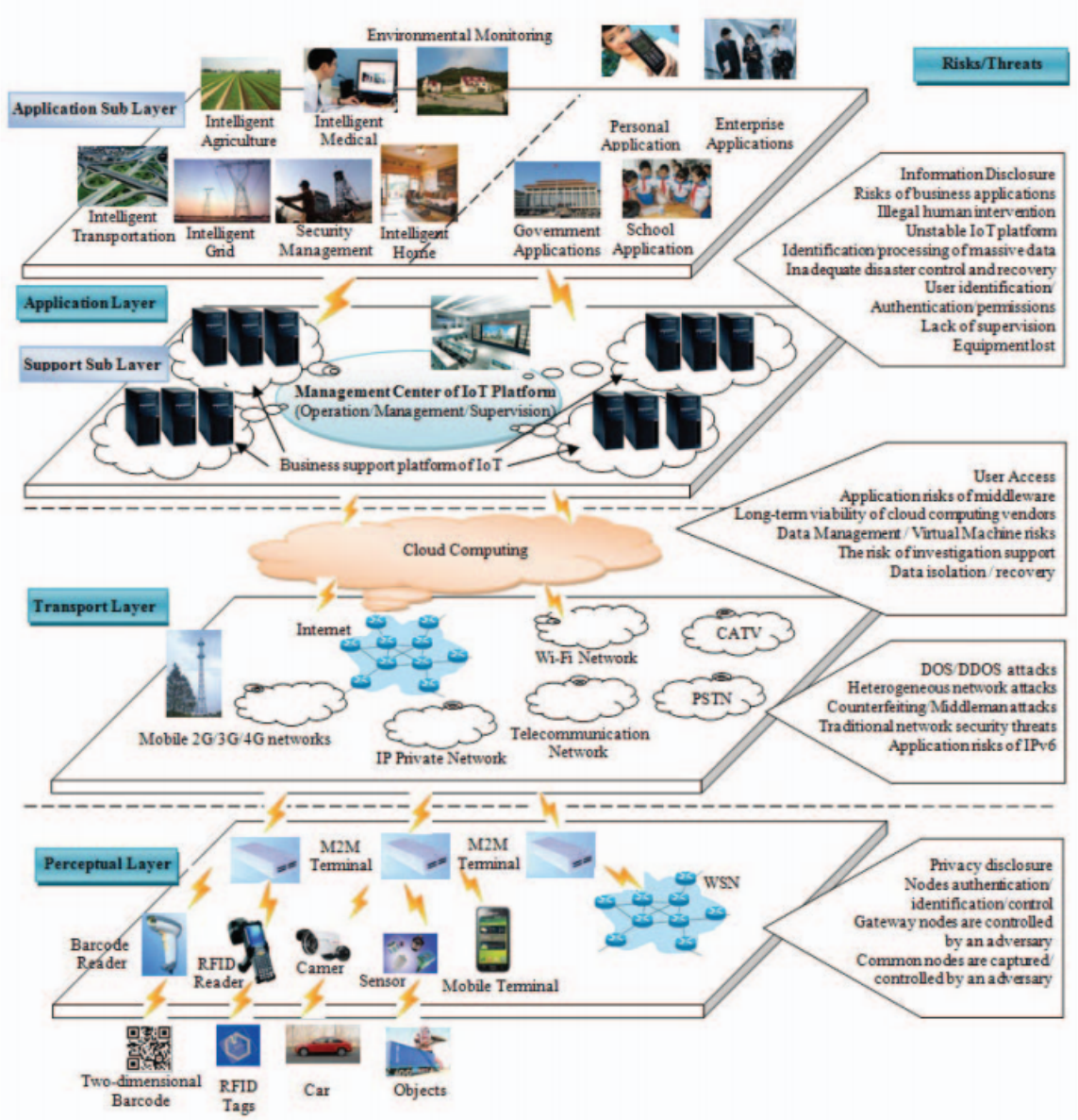

Fig. 2.4 Security problems of IoT s all layers are facing [1].

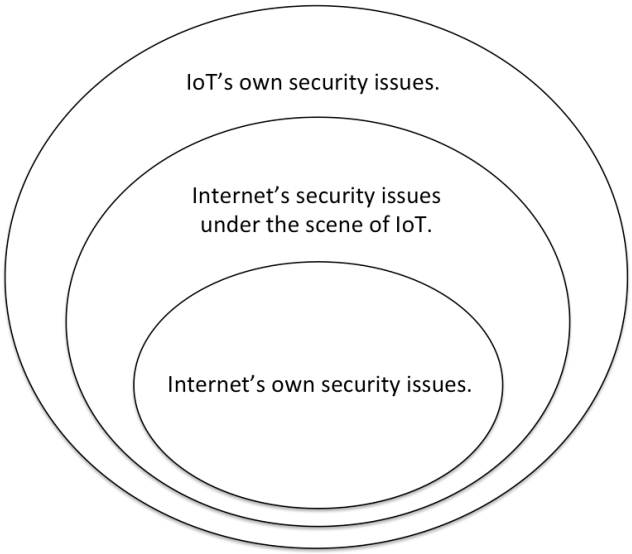

Fig. 2.5 Categories of IoT security issues.

- **Internet's security issues under the scene of the IoT:** Security issues already solved by some security technologies in the Internet environment. However given to the special scene of the IoT, they form some new security issues. These issues cannot be simply solved by continuing using the security technology for the Internet. The characteristics of the IoT needs to be considered. Appropriately modifying the Internet security architectures or designing a new architecture is required. Example: DNS not authenticating requester. In the IoT it will cause leakage of object privacy.

- **IoTs own security issues:** Security issues caused by the new network structure, equipments and other factors of the IoT. They cannot be solved with traditional Internet security architectures. New solutions are required. Example: authentication protocols, key agreement and privacy protection of WSN devices.

Chapter 3

Vulnerable Features and Threats

To ensure evolution of the IoT into a secure infrastructure, it is indispensable to exhaustively identify the features of the IoT which could be exploited to pose threat to either the infrastructure or its stakeholders. This chapter presents an in-depth analysis of the vulnerability space of the IoT, and attempts to create specialized *"threat spaces"* by providing an exhaustive threat taxonomy. We identify a new genre of threats: *Reflective Trust and Reputation Threats*.

3.1 Vulnerable Features of the Internet of Things

The IoT inherits most of the defining features of the Internet. In addition, the IoT has many distinct features as well. This section analyzes the potential vulnerable features from the viewpoint of IoT security and privacy.

[38] measures the security of dynamic networks, in terms of the vulnerable features of the IoT. It also identifies characteristics of the IoT which the authors find most relevant while using the attack surface metric for dynamic networks. We borrow the vulnerable features mentioned in [38] and extend the list to exhaustively enumerate all possible vulnerable characteristics of the IoT. Following are the recognized vulnerable characteristics (refer to Figure 3.1):

- **Integrated Cyber-Physical Space**
  [39] states, "The Internet of Things refers to a virtual representation of a broad variety of objects on the Internet and their integration into Internet

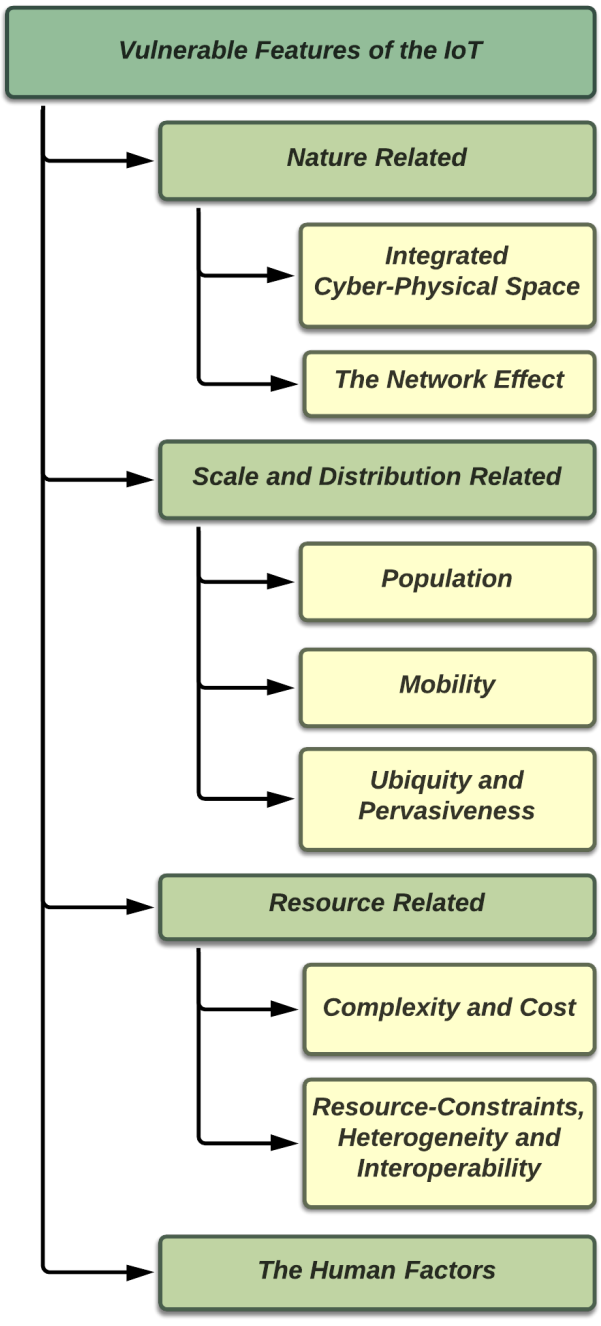

Fig. 3.1 Vulnerable Features of the Internet of Things

or Web based systems and services". The most significant feature of the IoT is its ability to integrate computing and communication capabilities with monitoring and control of entities in the physical world [40, 41]. This feature has enabled the actions of real, physical entities, or events in real environment to influence the events in the virtual world, and vice versa. Many of such associations are safety-critical: their failure can cause irreparable harm to the associated physical systems or people. Supervisory Control and Data Acquisition systems, for example, perform vital functions in national critical infrastructures, such as electric power distribution, oil and natural gas, water and waste-water distribution systems, and transportation systems. Disruption of these control systems could dreadfully impact on public health, safety and economic standings. While most of the effort for protecting Cyber-Physical Systems are towards reliability, there is a growing concern for the protection against malicious cyber attacks. [42, 43, 44, 45] are few of the researches that have raised and discussed this concern.

- **The Network Effect**

  The IoT is the largest network infrastructure ever deployed. T2T communications have resulted in the modern day super-complex, interconnected mesh of communicating nodes of varied level of complexity. It has exacerbated the challenges of maintaining the stability and security of the Internet. As per the Amplification Principle [46], in large networks, even small events can cause huge events; small perturbations on the input to a process can destabilize the system's output. Moreover, as per the Coupling Principle [46], as a system gets larger, it often exhibits more interdependence between components.

  Most IoT services are realized through high degree of intercommunication among the multiple component devices. Hence, the state of the entire system depends on the state of each component. For e.g., if a single sensor in a central heating system for a home is compromised or senses incorrect data, the decision cycle of the central controller would be influenced, leading to an abnormal temperature change of the entire home, unless, of course, fault tolerance techniques are used, such as replicated sensors. In that case, an

incorrectly working sensor can be tolerated. The direct/indirect dependency of things/contexts on some other things/contexts make it critical to carefully define the dependencies and nature of communications among the system components. Appropriate network segmentation should be implemented to limit the effect of an attack within a small segment of the larger system.

- **Population**
  The number of connected devices has exploded in recent years. According to the Cisco Internet Business Solutions Group [3], in 2003 the ratio of approximate human population in the planet to the number of Internet-connected devices was 6.3 billion to 500 million (0.08 device/person). The ratio rapidly changed to 6.8 billion to 12.5 billion in 2010 (1.84 devices/person). Cisco predicts 25 billion connected devices by 2015 and 50 billion connected devices by 2020 [3]. This unprecedented growth-rate of smart entities may raise major data management, security and privacy challenges. The explosion of participating entities is resulting in generation of tremendous amount of data. According to [47] in 2012, 90% of the world's data was created in the last 2 years. The Big Data explosion would raise data storage, data security and information processing concerns. Moreover, as more devices get connected, more sensors are deployed, and more objects are embedded with information. Each entity carries an associated set of channels, methods, and data items, each of which is subject to potential abuse, if it is not properly secured [38]. According to [38], the population explosion would expand the attack surface of the IoT.

- **Mobility**
  With all the smartphones, laptops and tablet, personal computers, cars, wearable technologies like smartwatches and Google Glass, mobile sensors, and even connected livestock [48], extreme dynamicity is becoming a major challenge to the IoT security and privacy.

  All the mobile devices create a dynamic operating environments for the IoT wherein systems and data shift rapidly between environments, exacerbating the challenges of access control, identity management, and device monitoring, and automated decision-making within limited domains of visibility and

control [38]. Mobile devices in order to transparently provide the user with their service, locally connects to other objects or gateways. They have to manage both situations in which they can access the IoT infrastructure and relative services, and contexts in which they will only be able to communicate with nearby devices. Managing mutual authentication, policy enforcement, and basic communication security are challenges [49].

- **Ubiquity and Pervasiveness: Anything, Anywhere, Anytime Could be a Smart Thing**
  The inexpensiveness of the enabling technologies, has led to much widespread physical distribution of IoT systems. The ubiquity, pervasiveness, and the increasing invisibility of the IoT element exacerbates the identity management, monitoring, security as well as privacy protection concerns. Deployment of IoT systems and information in less populated or not easily accessible geographies complicate their physical administration. Insecure physical distribution of constrained systems increase the risk of them getting compromised. Due to network effect, corruption of a simple node of an information/control system may jeopardise the integrity of the entire system. Moreover, the pervasiveness and invisibility of IoT systems complicate their physical surveillance, raising chances of privacy intrusion.

- **Complexity and Cost**
  Device complexity is determined by the device's processing capability, storage capacity and other available resources. The higher the resources, the higher the complexity. The IoT comprises a variety of connected devices with diverse complexities, ranging from high complexity systems like servers and personal computers, to low complexity, specialized devices like sensors, to highly constrained devices like RFIDs. Table 3.2 of [38] summarizes the classification of smart devices based on complexity.

  Table 3.2 shows the dominance of low complexity devices in terms of quantity. Entities with lower complexity also have smaller attack surface as the number of channels, methods, and data items to consider per entity is small [50]. However, the aggregate number of attack vectors of tier 1 and 2 entities is still large. Attack Surface describes all of the different points from where an

Tier	2020 Population	Examples	Characteristics
3	50 billion	Desktop, Laptop, Smartphone	Entity has channel(s) and method(s) for interactions with users.
2	1 trillion	Sensor, Controller	Entity has channel(s) and method(s) for interactions with entities. Entity has channel(s) and method(s) for interacting with its environment.
1	No estimate	Barcode, RFID	Entity contains data item(s) that may be consumed by other entities via an automated method. Entity has an unique identity.

Fig. 3.2 Smart Devices Classification Tiers

attacker could get into a system, and from where they could get data out [50]. A single attack vector for each tier 2 system, compared with 14 attack vectors for a tier 3 Linux system, still results in tier 2 systems presenting 42% more attack vectors in aggregate than tier 3 systems [50]. As a low complexity device (with high resource constraints) cannot support advanced security mechanisms, it is vulnerable to attacks which either exploits its weak defense mechanisms or resources scarcity.

The vision of a "connected world" would require the cost of connectivity to be as low as possible. Peter Middleton, research director at Gartner, Inc. predicts connectivity becoming a standard feature by 2020 with processors costing less then $1 [51]. The low prices of computing devices would impact the resources available for system security, encryption methods, key size and distribution, and software updates [38, 41].

- **Resource-Constraints, Heterogeneity and Interoperability**
  According to [17, 52, 53], the resource constrained members of the IoT are a major vulnerability. Achieving interoperability among the resource constrained networks and other network forms like the Internet is a challenge, as the resulting heterogeneity complicates protocol design and system oper-

ations [54, 55].

The IoT relies on lossy and low-bandwidth channels for communication between nodes with constrained CPU, memory, and energy resources. This poses challenge to the design of security protocols for the IoT. First, the use of small packets (e.g., IEEE 802.15.4 supports 127-byte sized packets at the physical layer) may cause fragmentation of larger security protocols packets. This may open new attack vectors for state exhaustion attacks on constrained nodes or communication channel bandwidth exhaustion attack on the 6LoWPAN [56, 57]. Packet fragmentation also downgrades the overall system performance due to fragment losses and retransmissions.

Low processing power impairs the constrained devices from using of resource-instensive cryptoprimitives, such as public-key cryptography as used in most Internet security standards. Lack of adequate in-built defence mechanisms, coupled with extensive and unsecured physical distribution of these devices make them easy victim to attacks like resource exhaustion attacks, firmware replacement attacks, extraction of security parameters, and malicious substitution of things [17]. Once the attackers capture the constrained smart objects, they can easily exploit the in-built services of the devices to affect the IoT ecosystem.

Protocol translation and end-to-end security are other concerns in supporting interoperability. Though 6LoWPAN [58] and CoAP [59] progress towards reducing the gap between the Internet and the IoT, they do not target protocol specifications that are identical to their Internet pendants for performance reasons. Hence, subtle differences between the IoT protocols and the Internet protocols will remain. While these differences can be bridged with protocol translators at gateways, they compromise the end-to-end security measures between IoT devices and Internet hosts [56].

- **The Human Factor**
  The human factor of the IoT plays a vital role in shaping up its security and privacy. Human errors are among the major IoT security vulnerabilities. The user base of the IoT systems are a major contributor of vulnerabilities

in the IoT. We recognize two ways in which the user base may become a venerability to the security or privacy of an IoT system.

1. Users could be vulnerable to security or privacy intrusion either due to exploitations by malicious manufacturers or service providers, or due to their own irresponsible, insecure or ignorant actions.
2. Users themselves could turn malicious and manipulate the smart environment to compromise the system.

The user base is a soft target of IoT security and privacy attacks, due to the user unawareness and irresponsible/insecure user practices. Most of the times the users of smart devices and services are unaware of the relevant security and privacy policies, the usage policies of the manufacturers/service providers, or the complete capabilities of the products. This could result in compromising of user privacy and/or security. For example, one might install a smart meter expecting it to periodically record the consumption of electric energy and communicate the information back to the utility for monitoring and billing purposes. But, the manufacturer of the smart meter might have added an additional feature into the meter, which also reported the information to a third party (maybe the manufacturer itself), which may use the information for malicious purpose, like analysing the data to predict the presence of people in the house based on energy consumption patterns. Many a times, users fall prey to attacks due to being unaware of secure and insecure practices. For example, it is common for users (even system administrators) to not change the factory setting default password of their network equipments. Also, at times they lack the knowledge of how much information is safe to divulge, and how to control the amount of released information. Users should demand complete transparency from the manufacturers'/service providers' side on where and how the user data is sent and used.

An example of the second type of human factor vulnerabilities in the IoT are the *"hackers"* or the malicious users of the systems who through their intentional actions attempt to exploit the vulnerabilities of the system to

either to gain undesired positional or intelligence advantage, or confers harm to the system by manipulating, disrupting or degrading the target system.

3.2 Threat Taxonomy

The IoT is coupled with new security threats and alters the overall information security risk profile. Although the implementation of technological solutions may respond to the IoT threats and vulnerabilities, IoT security is primarily a management issue. Effective management of the threats associated with the IoT requires thorough assessment of risk given the environment and development of a plan to mitigate identified threats. This section attempts to present a comprehensive taxonomy, creating specialized threat spaces.

3.2.1 Definition of Threat

In the context of the Internet, *threat* (or *cyberthreat*) is defined as, "the possibility of a malicious attempt to damage or disrupt a computer network or system" [60]. The definition of threat for the IoT would be an extension of this definition. The integrated cyber-physical space confers the implications of IoT threats even more severe, as their realization might impact the physical world as well. For e.g., if the network of a smart home is compromised, the attacker might gain control over critical systems of the household, like manipulating the thermostats of the heating system, or control the lock of the *"smart doors"*.

3.2.1.1 Difference Between Threat and Attack

While a threat basically implies a potential harm, an attack means an active act of causing harm. From the information and system security viewpoint, a threat is an entity (object, person or circumstance), which intentionally or unintentionally posses a danger to the system. An attack is always an intentional act of exploitation of at least one of the vulnerabilities of the system to inflict harm to the system, or any of its stakeholders (the users, the enterprise, etc).

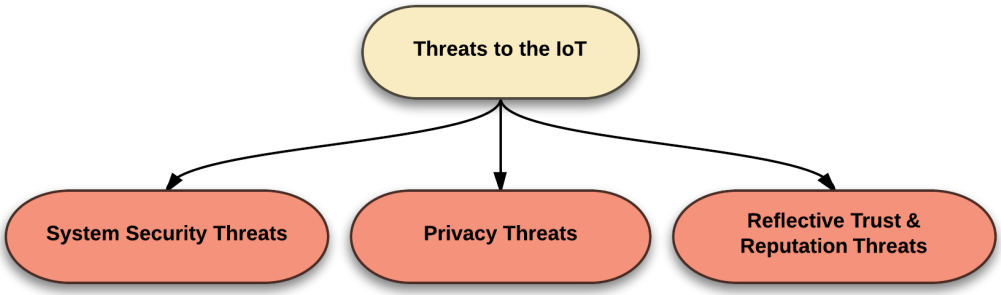

Fig. 3.3 IoT Threat Taxonomy

3.2.2 Proposed Taxonomy

This thesis proposes a novel taxonomy for the threats related to the IoT with the intent of being as exhaustive as possible. As the nature of computing is evolving, especially with the advent of the IoT, the natures of cyber threats are also ever changing. The threats are classified based on the intended motives of the possible attacks, and the type of harm inflicted on the victim. We propose three broad threat categories for the IoT, namely, *System Security Threats*, *Privacy Threats*, and *Reflective Trust and Reputation Threats* (refer Figure 3.3). Futher specialzed *threat spaces* have been developed under each category based on various factors.

3.2.3 System Security Threats

In the context of the IoT, the term *security* encompasses a wide variety of concepts, essentially including the basic elements of confidentiality, authenticity, integrity, authorization, non-repudiation, and possibly even availability of information and system. It also subsumes some augmented concepts like duplicate detection and timeliness [17]. Any potential activity that might intentionally or unintentionally violate these provisions, and in turn compromise individual thing(s), or a network as a whole, should be considered as a *System Security Threat* to the IoT.

[61] defines cyber maneuvers as "the application of force to capture, disrupt, deny, degrade, destroy, or manipulate computing and information resources". Inspired by [38], we classify system security threats into three categories based on the objectives of cyber maneuver. The first category pertains to *capture attacks*,

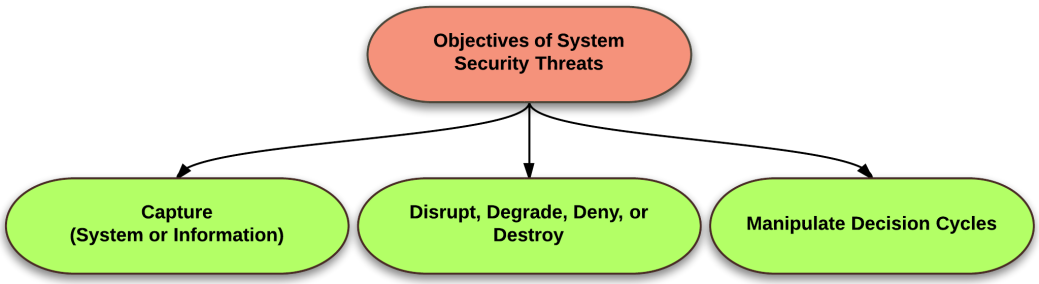

Fig. 3.4 Objectives Behind System Security Threats

designed to gain control over (physical or virtual) systems to gain positional advantage, or to gain access to information to have exploitative intelligence advantage [61]. The second category is of *attacks intended to disrupt, degrade, deny, or destroy the service*. Such attacks confer competitive disadvantage on the victim. Third category comprises *manipulation attacks*, intended to influence the decision cycles of the victims [61]. Such classification can aid assessing the threat implications in the IoT. Figure 3.4 depicts this classification.

To define clearer threat spaces, we further identify which of the following basic *security provisions* could be violated by the threats belonging to these three classes (this approach is inspired by [62]).

- ***Availability:*** Property assuring that data or services of the system are available at all times.
- ***Confidentiality:*** Property requiring all communications be intelligible by authorized principals only [63].
- ***Integrity:*** Property assuring that the resources (systems/information) are consistent, accurate, and trustworthy over their entire life cycle. Systems must not be accessed and modified and data must not be changed in transit, by unauthorized entities [64].
- ***Authenticity:*** Property assuring that the data, transactions, communications or documents (electronic or physical) are genuine, and all the entities in the system are who they claim to be [65].

- ***Authorization:*** Property assuring that each entity in and related to the system are doing what they are authorized to do [66].
- ***Accountability/Non-repudiation/Traceability:*** The ability to uniquely trace actions to its causing entity. Accountability supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action [67, 66].

3.2.3.1 Capture Threats

This category comprises threats which confer the attacker control over a physical or logical segment of the IoT infrastructure, or access to some information stored in the system. Hence, the attacker gains a positional/intelligence advantage to control the affected segment of the infrastructure, or even a greater part in it, or it gains access to some business/control critical information. Capture attacks might not bear an immediate/direct disadvantage upon the victim. However, it violates requisite security provisions, i.e. (business and control) data confidentiality, and *"authorized access only"*. Moreover, such unauthorized control/access facilitates the chances of more severe and active threats, like disruption, degradation, denial or destruction of functioning of the target. Features of the IoT allowing such threats include ubiquity, extensive physical distribution, weak defence mechanisms of constrained devices, mobility and interoperability.

For example, if an attacker captures a smart grid controller, it could be able to observe the power consumption information of any locality or even of individual households. Revelation of private information like the power consumption patterns of any household positions the malicious intruder to be able to easily use the information for malicious purpose.

3.2.3.2 Disruption Threats

This category comprises direct threats posing harm to the system and stakeholders through attacks intended to disrupt, degrade, deny service of, and destroy the target system, hence conferring a competitive disadvantage on the target. The opportunity to capture a system also affords attackers the opportunity to disrupt it. However, realisation of a capture threat does not imply a disruption threat.

While considering disruption threats, we must evaluate attacker opportunity, as well as target resistance, resiliency, and assurance. Features of the IoT allowing such threats include resource-constrained elements of the IoT, insecure physical distribution, mobility [38].

Extending the scenario discussed for capture threats, an example of disruption threats would be if the smart grid controller captured by an attacker is being maliciously used to alter the behaviour of the smart grid to disrupt the power distribution or charging system, or degrade the power supply service, or even shut-down the entire system.

3.2.3.3 Manipulation Threats

This final category of system security threats include threats of influencing the decision cycles [61] of the target. There are several possible ways of influencing the decision making capabilities of the target systems.

The decision cycle starts with the data generation. A possible manipulation threat is the corruption of the data before it enters the IoT system. In this case, even though the internal environment of the IoT is secured and functioning properly, security concerns still might rise due to the actions of the *"correct system"* based on *"incorrect information"*. For example, in a central heating system for a home, the thermostats have sensors which senses the temperature of its locality, and periodically reports the data to the central controller, which based on the information received, regulates the temperature of the home. Someone can manipulate the decision cycles of the controller by simply holding a burning lighter in-front of the thermostats for the sensors to detect and report abnormal temperature rise. Based on the incorrect information received from that sensor the controller may drop the temperature of the home drastically to maintain the required temperature!

Further, the system decision cycles can be influenced by compromising the low-complexity elements of the IoT, like the RFID tags or QR codes. The attacker could manipulate the embedded data, either by malicious substituting of the tags or by modifying the tag information.

Even further in the decision cycles, more aggressive attacks might take place to

influence the decision making of the system. For instance, maliciously substitute or use the devices that are the *"entry points"* of data into the system, like the sensors. Even the controllers of the *"entry point"* devices could be compromised to influence their behaviour.

A final form of manipulation threats would be when the integrity of the data being transmitted between two entities is tampered due to unauthorized intervention. Attacks like Man-in-the-Middle, Replaying and Spoofing pose such threat to data integrity.

Such threats are extremely hard to mitigate, especially due to the features of the IoT like population, widespread physical distribution, and mobility of the things, which *may* increase the chances of attacks without being detected, and features like heterogeneity and interoperability, which along with the highly distributed population of devices, demand great amount of inter-communication among devices, which increases the chances for attacks like Man-in-the-Middle, Spoofing and Replaying.

3.2.3.4 System Security Threat Space Specialization

Figure 3.5 indicates the basic security provisions which might be violated by the realization a particular threat type.

- **Specialization of Capture Threats**
  Capture threats are majorly passive in nature. Unlike the other two threat types, capture threats do not influence the functioning of the target system, but confers a positional advantage to the attacker. It would primarily violate the *confidentiality*, *authenticity*, and *authorization*. Capture threats might also be caused by *accountability/non-repudiation* issues.

  Confidentiality: When an attacker gains control over a system, it gains access to the stored data. If the data is not properly secured, the unauthorized attacker might learn some critical information. For e.g., in an eavesdropping attack, even if the intruder receives data packets being transmitted in the channel, it would be an issue of confidentiality loss only if the intruder can decrypt the protected data. Generally, violation of authentication/authorization increases the probability of violation of confidentiality.

Key Security Elements → / Threat types ↓	Availability	Confidentiality	Integrity	Authenticity	Authorization	Accountability/ Non-repudiation/ Traceability
Capture Threats	✖	✔	✔	✔	✔	✔
Disruption Threats	✔	✔	✔	✔	✔	✔
Manipulation Threats	✔	✔	✔	✔	✔	✔

✖	Never compromised
✔	May be compromised
✔	Always compromised

Fig. 3.5 System Threats Specialization

Integrity: Depending on the form of capture attack, integrity may or may not be compromised. In case of system capture attacks (gaining control of physical/logical systems), the attacker is in the position to influence the system's behavior, and hence its consistency, accuracy and trustworthiness. Hence, system capture implies system integrity violation. In case of information capture attacks like eavesdropping attack, though in possession of critical information, the attacker may not be able to create/tamper/replay messages. Hence, the integrity of the information remains intact.

Authenticity: It is crucial to ensure the authenticity of every *"entity"* in a system (users, devices, or data). In cases of capture attacks where the intruder gains control over the system, or access to the information by misusing the identity of an authorized entity, authenticity violation occurs. Since capture attacks do not involve any active disruption/manipulation of the system, data authenticity remains intact. Example of user/device authenticity

violation would be an Identity Theft or Identity Spoofing attack where the intruder gains access to system/information using some authorized entity's identity. Instances of capture threat without violation of authenticity are possible in cases where the intruder does not gain access to the system by pretending to be someone authorized for the action, but exploits loopholes in the mechanism (like SQL Injection attack on data driven applications [68]) or in user practices (like using the default username/password of the system).

Authorization: Though authorization and authentication are two separate concepts, they are highly coherent. Any form of capture threats would always incorporate a violation of authorization. Any attempt of an *"unwanted"* entity to gain access to a system/information, which they are unauthorized for, is a breach of authorization policy [66].

Accountability/Non-repudiation: Capture threats may involve accountability or non-repudiation violation. In cases of authenticity (and authorization) violation in capture attacks, i.e. when the attacker steals/spoofs an authorized entity's identity, the actions of the attacker while in possession of the system/information, cannot be traced back to the actual actor.

- **Specialization of Disruption Threats**

  Disruption threats are primarily intended to disrupt/degrade the expected performance of the system, or to completely destroy the system or deny its service. A disruption attack may or may not succeed a capture attack [38]. Disruption attacks can cause violation of any/all of the security elements: *availability*, *confidentiality*, *integrity*, *authenticity*, *authorization*, and *accountability/non-repudiation*.

  Availability: Disruption attacks are easy to accomplish in the IoT systems, especially due to the population, and dispersed and unprotected physical location of the resource constrained entities. For any information network to function properly, device availability is a critical factor. Any form of Denial-of-Service attacks [69] target network availability by preventing communications between network devices from accessing the services provided. Large quantity of the peripheral devices of the IoT have constrained

processing, storage and power supply capabilities. Actions engaging such devices to use their resources for purposes other than what they are meant to be used for, would jeopardise the devices' availability to their legitimate co-operating systems. Resource exhaustion attacks can be in the form of processor exhaustion attack, where the devices are kept occupied with processing much of deliberately generated request/tasks. Another form could be the actions to minimize the lifetime of the power constrained devices by constantly overworking them, and not allowing them to enter the energy-saving mode. (Sleep Deprivation Attack [70]). System availability will also be violated in cases where the target system remains active, but the behavior of the system is changed. For example, misconfiguration of network equipments like gateways, routers, DNS server in the enterprise network or the Internet by authorized persons (by mistake), or by attackers.

Confidentiality: Disruption threats which also require capturing of system/information (capture attacks) can possibly have violation of confidentiality if the data captured by the attacker is not efficiently encrypted, and the attacker is able to extract some confidential information from the data.

Integrity: As in case of a disruption attack, the attacker influences the target system with a definite intention of deteriorating its performance. Hence these attacks certainly compromises the consistency, accuracy and trustworthiness of the behavior of the system and the data generated/controlled by it. Thus the system as well as information integrity is violated.

Authenticity: Similar to capture threats, if a disruption threat involves an unauthorized intruder gaining control of system/information by using some other authorized entity's identity, user/device authenticity violation occurs. But unlike capture threats, in case of disruption threats, there are also chances of data authenticity loss. For example, a replay attack, in which a valid data transmission is repeated. It is possible to have disruption attacks without any authenticity violation (e.g. a DoS attack).

Authorization: An authorization policy may be infringed in attacks where the attacker assumes some capabilities which it is unauthorized for. For example, incidents where an attacker misconfigures an enterprise/Inter-

net network element like gateways, routers, or DNS server, to manipulate network traffic, the attacker needs to gain access into those entities. This would mean infringement of authorization. On the other hand, attacks like Denial-of-Service on some device in the IoT infrastructure, by exhausting its processing/storing capabilities or power source by engaging it into excessive workload, may not involve a breach of authority.

Accountability/Non-repudiation: Accountability/non-repudiation may be breached in instances of disruption threats. In cases of authenticity (and authorization) violation, i.e. when the attacker steals/spoofs an authorized entity's identity, the attacker's actions while in possession of the system/information, cannot be traced back to the actual actor. Hence, accountability and non-repudiation is lost. A suitable example would be a replay attack. Presence of numerous mobile smart devices in today's world, poses huge challenge towards deploying efficient access control mechanisms. Absence of a strong access control and a secure bootstrapping mechanism for devices entering and exiting an IoT domain, may cause device identity issues, leading to possible accountability/non-repudiation breaches.

- **Specialization of Manipulation Threats**

  In some cases, manipulation threats can be achieved by some form of active intrusion, while in others it can even be accomplished without any system intrusion. In all its forms, a manipulation threat can infringe *confidentiality*, *integrity*, *authenticity*, *authorization*, and/or *accountability/non-repudiation*.

  Confidentiality and Integrity: In cases of active manipulation of data during transfer on the Internet, or the intranet (the enterprise network and the Low-Power and Lossy Networks [71]), or of data stored on devices, data confidentiality and data integrity are compromised. In instances of manipulation of the embedded data, either by malicious substituting of the tags or by modifying tagging information, or malicious substitution of the devices that are the *"entry points"* of data into the system, like the sensors, device integrity is also compromised.

  Authenticity: In manipulation attacks, authenticity of data is always in-

fringed, as the motive of influencing the decision cycle of the IoT system is achieved by either feeding incorrect information to the IoT environment (refer Section 3.2.3.3), or by manipulating the data existing in the system (e.g. Man-in-the-Middle attacks). Manipulation attacks can also be accomplished by using original data at an *"incorrect"* time (e.g. replay attacks).

Authorization: Unlike capture threats, manipulation threats do not involve authorization infringement every time. Only the situations where the attacker is trying to manipulate data by actively intervening into the communication channel (e.g. Man-in-the-Middle attack) or compromising the integrity of some device(s), does the concern of authority breach arise.

Accountability/Non-repudiation: Manipulation attack may cause loss of accountability/non-repudiation. For example, manipulation of logged data or data logging configuration by the intruder. Such attacks will not impact on the performance of the target system directly, but would jeopardise the ability to trace the original actor(s) of certain activities in the infrastructure.

3.2.4 Privacy Threats

Privacy is a major concern associated with the IoT. With all the ubiquity offered by the IoT, privacy becomes a challenge. In 1890 Warren and Brandeis [72] defined privacy as *"the right to be let alone"*. Though this time-tested definition still holds validity, a lot has changed since 1890! The changing perspective about public and private in the last few decades can be attributed to several factors, but no single factor has influenced the transformation of privacy as has the introduction of the Internet and mobile-communication devices. And now, with the evolution of the Internet into the IoT, there is a need to broaden the concept of privacy to accommodate not only personal privacy but information and physical privacy as well [73].

The growing popularity and utility of the IoT has fostered a Big Data explosion [74, 75]. Generation of such huge quantity of data has created severe data management issues. Efficient data management methodologies [26] are required to contain the IoT environment from turning into a dystopia. Social networking sites like the Facebook are already impacting users' personal interactions and em-

ployability [76, 77]. Consequences of such exposure opportunities being amplified many times could be dire.

To understand the premise of privacy first we must clarify its distinction from security. Our tendency to focus on the outcome of an event and its impact on our lives, makes the distinction between privacy and security concerns non-trivial. For example, people tend not to consider providing their credit card number to a third party as a threat. But when this information is misused by the third party by stealing and using the credit card, people start treating it as security *and* privacy threats, and look for a solution to the situation [78]. The difference between security and privacy must be identified, and it must be realized that security threats and privacy threats can be caused due to each other. The disclosure of credit card details to an unauthorized third party should be considered a privacy breach. Security threats would arise if the third party uses the acquired information to capture/disrupt/manipulate the authorized user's virtual/physical activities. Similarly, an intrusion into an enterprise's database server should be considered a security breach. Privacy threats would arise only if the intruder gains access to sensitive data, like employee details or customer profiles. While, privacy violation actions like social engineering [79], wherein through psychological manipulation people are made to divulge confidential information, there might not be any security threats involved, such compromise of user privacy may culminate in some security threats. For example, theft of login credentials of a user through social engineering may lead to system capture, or even disruption and manipulation attacks.

Privacy includes the concealment of personal information as well as the ability to control what happens with this information [80]. Based on the definitions of privacy in [81, 78], this thesis defines a privacy threat as *a possible event of exposure of sensitive data to entities (person, enterprise, or artificial intelligence) which are not authorized to or required to possess those data. It can either be in the form of wrong data in the wrong entity's hand, or too much data in the hands of the right entity. Privacy threats might not actively impact the actual owner of the data.*

Based on the motive of exploitation, all privacy threats are found to be comprising of the following *fundamental threat elements*.

- ***Action Prediction Threats:*** Data acquired by the *privacy intruder* is used to determine/predict the data owner's future actions. For example, a household's power usage data can be analysed to estimate the presence/absence of members at home at different times of the day.

- ***Association Threats:*** These threats comprise the association of specific smart devices with an individual. For example, when a customer purchases an item with an EPC tag, an association is established between the customer's identity and the item's electronic serial number. This association can be exploited in a lot of ways, like clandestinely tracking the owner of the device.

- ***Preference Threats:*** Based on the identity of the devices owned/carried by an individual, predictions can be made about the taste/preferences and even financial status of the person.

- ***Location Privacy Threats:*** Location based services offer numerous benefits to users as well as financial benefits. However, the possibility of unauthorized disclosure of location information is a major concern, and poses a serious threat to user privacy [82, 83].

- ***Digital Shadowing Threats:*** Digital Shadow means an implicit visibility of a person, business, enterprise or object that can be found within the IoT and other digital records [84]. The unique digital shadow is formed by the smart devices associated to an entity (individual/enterprise/object). Digital Shadowing uses the association property to infer identity/capabilities of an unknown entity [52]. Adversaries can use this digital shadow to identify/-track the entity, without necessarily knowing its real identity/capabilities.

- ***Transaction Monitoring Threats:*** When tagged objects are moved from one entity to another, a transaction between the two individuals associated entities can be inferred.

These *fundamental threats* elements combine to form he following more complex, real life *compound threats*.

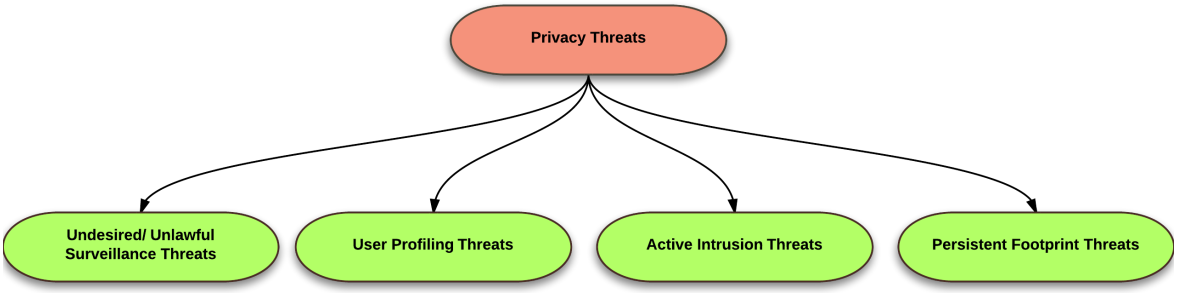

Fig. 3.6 Types of Privacy Threats

- *Undesired/Unlawful Surveillance Threats*
- *User Profiling Threats*
- *Active Intrusion Threats*
- *Persistent Footprint Threats*

3.2.4.1 Undesired/Unlawful Surveillance Threats

The IoT can easily be exploited by a malicious party for unlawful surveillance. In the future these smart, Internet-connected modules may allow an unauthorized party to receive far more information than they should or currently can. For example, a malicious entity may be able to monitor children through cameras installed in their toys, monitor people's motion through the embedded system in their *"smart shoes"*, and monitor when the members of a household enter and leave the home by connecting to an Internet-connected door lock and the electric power usage through their smart meters.

Researchers have successfully demonstrated how many of these vulnerabilities can be exploited to carry out malicious activities on connected automobiles [8], medical devices and smart homes [85, 86]. As per a complaint filed by the Federal Trade Commission [81] against TRENDnet Inc., a producer of wireless cameras which can send motion-captured videos to computing devices, nearly 700 wireless cameras were hacked into and compromised feeds were provided online. The feeds

included unauthorized recordings of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities [87].

Undesired/Unlawful Surveillance Threats can be realized through one or many of the following threats, *association threats, location threats, digital shadowing threats,* and *transaction monitoring threats.*

3.2.4.2 User Profiling Threats

User profiling can be defined as the collection, collation and analysis of user data which facilitates identification, segregation, categorization and decision making about the user. It is a powerful tool from the marketing and research view point. It can prove to be instrumental even for security and law enforcement. The anonymized information submitted by IoT-connected devices can be used to create a detailed profile of the device owner. These profiles can be used/sold for placing targeted advertisements based on various behavioral, demographic, and psychographic attributes. Such target advertisements can be an excellent medium for sellers to reach out to the *"ideal"* consumer, and for the consumers to find the *"perfect"* product. But, it can also be an intrusion into the user's personal space. Dr. John Barrett furnishes an example in his talk [88]. Suppose a heart patient has a Bluetooth enabled pacemaker installed. When the pacemaker detects an Arrhythmia, it informs your cell phone. The cell phone suggest the patient to sit down, informs the hospital and calls an ambulance. These are the benefits of the technology. But trying to relax, the patient receives an advertisement of some "wonder drug" for heart problems on his phone! Even further, if the health insurer has an access to the patient's health data at real time, while waiting for the ambulance, the patient might receive another message informing that the health insurance premium has increased by 25 percent!

User Profiling Threats can be realized through one or many of the following threats, *action threats, association threats, location threats, preference threats,* and *transaction monitoring threats.*

3.2.4.3 Active Intrusion Threats

The involvement of the IoT in our daily lives is reaching a point where a security or privacy breach in an enterprise, or on an individual could result in catastrophic consequences. This notion is corroborated by incidents like [8], where hackers are able to penetrate the operating system of a smart car and manipulate the information displayed on the dashboard to indicate a speed which is lower/higher than the actual speed of the car, manipulate the fuel information, or even worse, deploy airbags without any crash, or turn a running car's steering wheel, while you are driving! Many more such instances can be found where the vulnerabilities in the smart, connected devices have been misused to launch active intrusion into smart cars, smart homes, etc. [87, 89, 85]. The possibilities of an intruder remotely regulating the refrigerator, starting the heater, unlocking the doors, manipulating a running car are frightening.

3.2.4.4 Persistent Footprint Threats

Persistent Footprints refer to the idea that as individuals collect smart objects, they build an items database associated with their identity in corporate information systems. The association may persists even after an object is discarded. The Persistent Footprint threat considers the possible misuse of the discarded smart object to conduct some malicious act. The only identity associated with the misused object is that of the original owner. This weakens accountability and law enforcement [90].

3.2.5 Reflective Trust and Reputation Threats

The thesis introduces a new genre of IoT threats which has not been previously investigated. This genre considers the possible impacts of certain malicious activities external to a service provider's authentic IoT system, which could harm the service provider's reputation, or cause loss of customers' trust. Here the term service provider represents both device/technology manufacturers and the enterprises which provide services using the IoT infrastructure. These activities may also impact the service provider's financial market [91]. Though the previous two threat genres also harm the reputation of the service provider whose services are affected

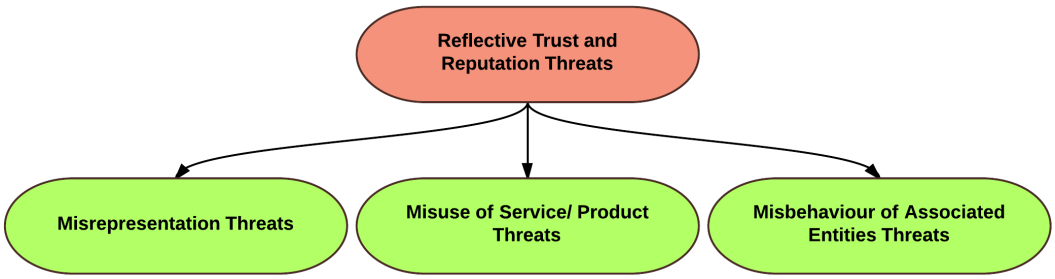

Fig. 3.7 Types of Reflective Trust and Reputation Threats

or of the manufacturer whose devices are compromised, these threats are unique due to the nature of the activities undertaken to realise them. These threats do not involve any active intrusion into the original system, which remains secured. In fact, there might not be any interaction between the attacker and the original infrastructure at all. These threats exploit the inadequacies in the interface between the IoT system and the users and the dependencies of a service provider on other agents to provide their service to the users.

There are three possible types of activities which could pose reflective trust and reputational threats on the stakeholders of the IoT infrastructure (Figure 3.7):

- **Misrepresentation Threats**

  Analogous to such threats are the classic *Phishing Attacks* in web based interactions [92]. In a phishing attack, attacker attempts to acquire sensitive information (e.g. login credentials, credit card details) by masquerading as a trustworthy entity. Unsuspecting users are often deceived into frauds through communications claiming to be from reputed social web sites, financial institutions, or online payment portals. In a similar manner, scenarios may arise in the IoT ecosystem where users are misguided by entities which are unlawfully and incorrectly representing an enterprise, service provider, or a device manufacturer, to gain personal benefits, infringe user privacy, or at the least give an unpleasant experience to the user. In all cases, reputation of the genuine entity which has been wrongly represented is tarnished. Following are two such scenarios.

  The Aberdeenshire Council has started providing smart-phone access to

timetable information at the bus stops [93]. The customers can now interact with their bus stops by scanning a QR code or 'tapping' their NFC (Near Field Communication) [94, 95] enabled smart phones on the timetable display. This exemplifies the ease of access to information and services that the IoT has bestowed on us. Such technologies can make information circulation and updates more effective and economical. But such applications raise a number of issues as well. How would a user know about the authority of the provisioner of such services which can be made available anytime, anywhere? How would the user know if the QR code is authentic? With their location in public sites like bus stands, malicious replacement of the original *"things"* (in this case, a QR code) is certainly possible. This might result in the users being redirected to some malicious services masquerading as the original one, and either causing harm to the visitors (like privacy intrusion), or damage the reputation of the Public Transport Unit [96] by providing bogus information to the users. The users may also remain uninformed about the kind and usage of data collected from the user while using the application, and how and to whom the data is transmitted [97].

Another relevant example would be the cloning of the physical features, firmware or software, or security configuration of *"things"* by untrusted manufacturers to gain financial benefits by selling them at cheaper prices in the market [17]. Such devices might seem to work perfectly fine to the users, but in fact they might be providing inferior service, or even have added malicious features like a backdoor. Such cloned substitutes may inflict reputational damage on the original manufacturer.

- **Misuse of Service or Product Threats**
  The reputation of a service provider can also be tarnished by the use of its services/products by any external entity to perform actions which violates others' security, privacy, or even reputation. These threats might negatively affect the reputational and financial standing of the service provider in spite of the possible absence of any inadequacies in the service/product. For e.g., malicious users may misuse devices like Google Glasses or smart watches to stealthily collect information at locations where such activities are either il-

legal/undesired. Such privacy violations can possibly culminate into security and/or reputational threats as well. Though such incidents do not involve the compromise of the integrity of the service/product, they certainly corrode the reputation of the service/product and affects the user trust, due to the association of the service/product with the incidents. These also lead to formation of prejudiced opinions and even very harsh policies for the service/product [98, 99]. The Social Governance Framework proposed in Chapter 5 can prove to be an effective solution in minimizing such threats and protecting interests of the users and the service providers.

- **Misbehaviour of Associated Entities Threats**
  The IoT is a composite system. Many a times a service provider does not own the end-to-end infrastructure required to provide a service, and hence collaborates with other enterprises and equipment manufacturers. In such setups, the robustness of the security and privacy of the service provider is influenced by the performance of the associated entities. The quality of security or privacy safeguards of the associated entities might not be under the service provider. If the behavior of these entities is substandard/malicious, it would ultimately tarnish the service provider's performance and reputation.

The factors that make this genre of threats possible are:

- ***Detachment from Original Infrastructure:*** The fact that these attacks may not engage in any active interaction of the attacker with the genuine infrastructure makes even the most sophisticated and secured IoT systems vulnerable to such threats.

- ***User Unawareness:*** The dearth of sound understanding among the users, of the IoT technologies (services, devices and their capabilities), the secure usage practices, and the consequences of their actions, results in more and more users falling pray to such malicious traps.

- ***Ubiquity and Pervasiveness of IoT Services:*** The intent of the enterprises to make their services available to a greater mass of people has resulted in a large population of smart devices of highly varying complexity

and extensive physical distribution. This makes the assurance of physical security of these devices highly impractical.

- ***Ease of Launching Attack:*** The requisite for launching such attacks is to simply succeed in deceiving a user to use the malicious service instead of the original one. Hence the technical sophistication required is minimal. As explained in the example above, an element as common and simple as a QR code might be enough to circumvent the advanced security mechanisms of a bank and exploit the customers' trust on the reputation of the institution.

Chapter 4

Securing the Internet of Things

Security and privacy are the prime constraints to the popularity and acceptance of the IoT. Figure 4.1 from [2] indicates the opinions of security personnel active in the IT space on security in the IoT. According to [14], as we go back in time, the need of security and privacy in the Internet would keep decreasing. Hence security and privacy were not parts of the design of the Internet. With the evolution of the Internet into the IoT, many security and privacy issues came up, which we generally resolved by building patches. Security and privacy are generally treated as augmented features. The nature of the vulnerabilities of the IoT, as discussed in the Section 3.1, dictates integration of security and privacy into the design of the IoT. Also, along with a technological model for security and privacy, a foolproof IoT ecosystem would also require reconsideration of the related governance, economics, and social-ethics.

This thesis recognizes the following four broad domains of actions to be vital for the development of an effective, secure, reliable, robust, and safe IoT ecosystem.

- *Making the IoT more secure and private.*
- *Standardizations*
- *Governance*
- *Social Awareness*

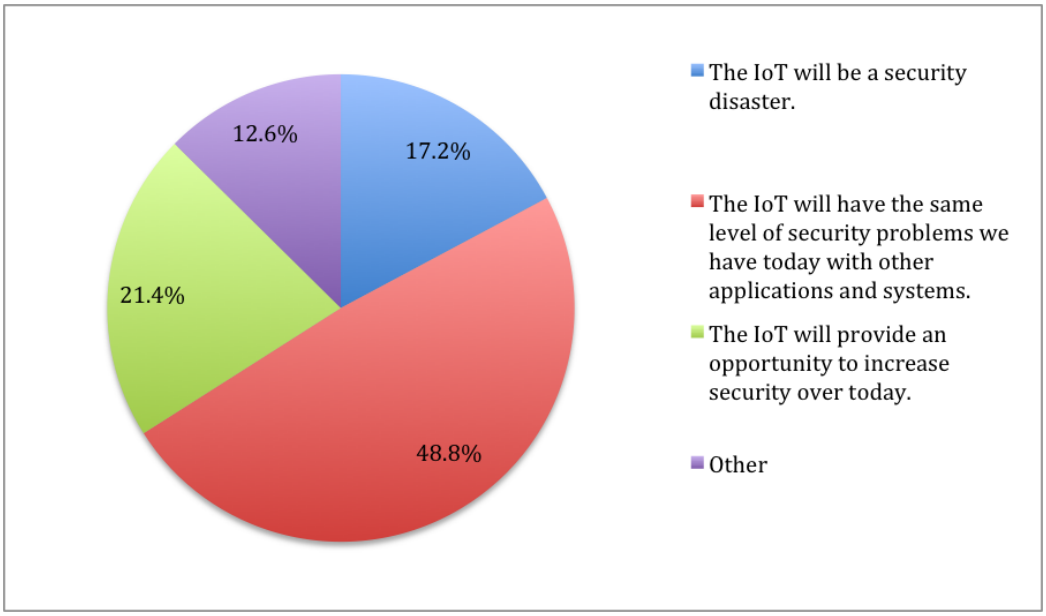

Fig. 4.1 Opinions about the IoT and Security [2]

4.1 Making the IoT More Secure and Private

Based on [52], this thesis recognizes the following requisite domains of actions for preservation of security and privacy in the IoT:

- *Protocol and Network Security*
- *Data and Privacy*
- *Identity Management*
- *Trust Management*
- *Fault Tolerance*

4.1.1 Protocol and network security

One of the biggest challenges to protection of IoT infrastructure is posed by heterogeneity. The highly constrained devices operating in low-power and lossy network standards like IEEE 802.15.4 [100], are required to open secure communication

channels with more powerful devices in the Internet using standard Internet protocols (refer Section 3.1). As per [52], the prime ingredients for securing such communications are,

- *Lightweight Cryptographic Algorithms*
- *Efficient Key Management*
- *Standardized Security Protocols*

The presence of resource-constrained devices in the IoT makes the implementation of highly resource intensive existing standards of cryptographic algorithms, like AES infeasible [101, 102]. The cryptographic mechanisms for the IoT are required to be less resource intensive, faster, and at the same time providing the same level of security. These mechanisms may include symmetric algorithms, hash functions, and random number generators [52].

Key Management is an indispensable element of a secure network infrastructure [103, 104]. An "efficient" key management mechanism for the IoT would consider its heterogeneity and the resource-constrained members. It should support the management of a large device population and high dynamicity in the IoT environment. As per [52], manual configuration of the cryptographic keys in the devices, and the traditional public-key infrastructures would not scale up to accommodate the heterogeneity, population, and diversity of contexts in the IoT environment.

Finally, there is a requirement of establishing *Standardised Security and Communication Protocols*. All the communication protocols in the traditional Internet and the IoT should be standardised to ensure consistent communication standards and to avoid usage of communication and security protocols which are not optimal for some resource-constrained members of the system, or to avoid any intermediate protocol translation which endangers end-to-end security [57, 17] (also refer Section 4.2). The standardised communication and security protocols are required to not only fulfill the IoT's performance goals but also provide the protocol's original security properties in the context of the Internet architecture [17].

[105] presented the first fully-implemented end-to-end security architecture for highly constrained embedded devices. It used Elliptic Curve Cryptography

to demonstrate feasibility of public-key cryptography on the resource-constrained embedded devices, and efficient implementation of a complete secure web server stack including SSL, HTTP and user application.

- *IP-based Security Solutions*
  According to [17], a number of IETF working groups are designing all-IP based solutions for resource constrained networks in the IoT. For example, the 6LoWPAN working group are working towards defining methods and protocols for efficient transmission and adaptation of IPv6 packets over IEEE 802.15.4 networks [106]. A framework for resource-oriented applications which run on 6LoWPAN, is provided by the CoRE working group. The CoRE working group provides the Constrained Application Protocol (CoAP) [59], which is a lightweight version of the HTTP and runs over UDP.

  Some of the major IP-based security protocols and procedures for the IoT are the Internet Key Exchange/Internet Protocol Security (IKEv2/IPsec) [107], Transport Layer Security/Secure Sockets Layer (TLS/SSL) [108], Datagram Transport Layer Security (DTLS) [109], Host Identity Protocol (HIP) [110], Protocol for Carrying Authentication for Network Access (PANA) [111], and Extensible Authentication Protocol (EAP) [112]. [17] discusses the implementation of these protocols and procedures. The IKEv2/IPsec and the Host Identity protocol (HIP) operating at/above the network layer perform authenticated key exchange and set up the IPsec transforms for secure payload delivery. The IETF working groups are currently working on the creation of Diet HIP, a variation of HIP especially designed for facilitating authentication and key exchange in low-power and lossy networks [17]. The Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) are designed to secure the TCP and UDP connections at the transport layer, respectively. The EAP provides an authentication framework supporting multiple authentication methods. It runs over the data link layer and does not require the deployment of IP. EAP supports duplicate detection and retransmission, but does not allow for packet fragmentation. Whereas, PANA that runs between the EAP peer and the EAP authenticator, supports net-

works access authentication between clients and the network infrastructure.

- *Wireless Sensor Network Security Solutions*
  [17] summarizes the variety of key agreement and privacy protections protocols that have been designed for wireless sensor networks. The random key pre-distribution schemes for sensor networks [113] or the more centralized solutions like SPINS [114], have been proposed. In the ZigBee standard [115] for sensor networks the security relationships between the communicating devices of a ZigBee network are maintained through an online trust center.

4.1.2 Data and Privacy

The significance of privacy and the implications of privacy violations in the IoT ecosystem are discussed in Section 3.2.4. [116] discusses privacy implications of the IoT focusing on RFID technology as one of its main enablers and suggest possible solutions to developing IoT systems in a privacy-respecting and secure manner. In order to approach privacy issues in the IoT ecosystem, [52] suggests three key consideration:

- *Privacy by Design*
- *Transparency*
- *Data Management*

Privacy by Design (PbD) is a philosophy which endorses empowering users with tools to control the data produced by them [117, 118]. [117] provides three complimentary definitions of PbD.

- Firstly, PbD means making data security provisions an integrated part of the design of an information system.
- Secondly, PbD means collecting and processing minimal personal data (*principle of data minimization*).
- Finally, PbD means thoroughly analysing and assessing the future vulnerability of originally secure technology.

PbD is being implemented in many areas. According to PbD, any data produced by users can be controlled by them using a dynamic consent tool , which permits/restricts services to access as little or as much of that data as desired by the producer of the data. Hence, users can control the quantity and granularity of the data they produce, that is divulged to any service. For example, a user located in Central Park in New York could use a location-based IoT service, while divulging a less precise location information, such as he is in New York City. Also, smart home appliances, like a refrigerator or a smart heater, should be transparent about what type of information they are collecting, to whom it is being sent, and what purposes those information are used for. Moreover, the appliances and the services should be programmable for the users to be able to set the amount of data that the appliances may collect and to whom those information should be sent.

In October 2010, a landmark resolution was approved by the International Privacy and Data Protection Commissioners at their annual conference recognizing Privacy by Design as an essential component of fundamental privacy protection, and encouraging the adoption of the principles of PbD as part of an organization's default mode of operation [119].

Transparency is another essential element in privacy protection. [120] defines *transparency tools* as privacy enhancement technologies which attempt to improve the data subject's understanding and control of its data profile. Current ubiquity and pervasiveness of the IoT proves high dependency of users on technological solutions in every spheres of life. The ever-increasing sophistication of IoT services and devices entails scopes of lack of comprehensive knowledge to the users about the entities managing their data and how and when those entities are using it. Service providers are required to cater complete transparency of their services to the users. The enterprises should be able to adjust their services according to the quantity and granularity of data that the users agree to provide.

An instance of transparency tools is the *Privacy Coach* [121], a mobile phone application that supports its users in learning about the RFID tags in the ambiance they are in and in making privacy decisions. Unlike the mainstream efforts of focusing on implementing privacy enhancing technologies on the RFID tags themselves, the Privacy Coach functions as a mediator between customer privacy preferences and corporate privacy policies, trying to find a match between the two,

and informing the user of the outcome. Privacy Coach also realizes PbD, as it provides the users control over the data that is absorbed by the surrounding RFID tags In totality, Privacy Coach enables users to make informed privacy decisions in a user-friendly manner. Another apt example of transparency and trustworthiness enhancing tools for the IoT is the *Trusted Tiny Things* project [97] which proposes an infrastructural solution to enable users to interrogate IoT systems to discover critical information about the generation, collection, handling and the handlers of the data produced by the users. The solution is based upon additional metadata describing the context of surrounding devices. The authors also argue that this can be provided by publishing information about devices or services according to the linked data principles [122]. As 'things' become more interconnected this context should also include provenance information: a record of the entities (devices or services) and processes (data transmission, data analysis, decision making) involved in the creation and use of data [123, 124, 125]. A formal representation of provenance has been identified as essential to support users (and machines) to better understand and trust data [126].

Data Management pertains to the critical issue of delegating and restricting management of data throughout its life cycle, to rightful and authorized entities [52]. The characteristic resource-constrained entities of the IoT might not be able to implement the standard data management policies, i.e. cryptographic mechanisms and protocols designed to protect data. As stated in [52], there must be policies on how to manage various kinds of data as well as some policy-enforcement mechanism. Development and enforcement of such data management policies is non-trivial, as it requires interpreting, translating, and optimally reconciling a series of rules, each of which might be in a different language. Also the policies must comply with the legislation on data protection, which itself could evolve.

4.1.3 Identity management

The IoT architecture which comprises existing networks and services, and several new and unique devices (such as remote health monitoring devices, sensors, etc. in the healthcare industry) faces a series of important technical challenges, one

of them being the management of diverse user and object identities and their relationship types [127]. Although the concept of *"Identity"* in the IoT is similar to that in classic web, the identity mechanisms in the IoT are required to be a little different from those in the classic web [128]. Classic identity management (IdM) dealt with longer living identities. For example, in applications like e-mail, user identities are long term, i.e., they could exists for months or years. In the IoT, an identity may exist for months or years, to even days or minutes. For example: A parcel being shipped over a long distance gets an RFID tag associated with an identifier. It moves from one logistic center to another, it is tracked, controlled and routed. As soon as it arrives the identity of the parcel is terminated.

Things in the IoT often have a relationship to real persons (owners, manufacturers, users, administrators, etc.). As the identity relationships may change over time, identity managements processes like authentication, authorization are also impacted.

In the classic IdM certain established methods are used to manage identities. Authentication methods validates identities, identity attributes are transmitted over secure channels and critical data like passwords are encrypted and stored. Security elements like integrity, availability, authenticity, non-repudiation are integrated in classic identity protocols. Whereas in the IoT, many communication protocols are not standardized and may not be IP-based. The resource constrained members of the system lack processing power, bandwidth, or energy to support sophisticated encryption, challenge response procedures or other security mechanisms.

The classic authentication mechanisms may not directly apply to the IoT. In the IoT, objects have to provide some lightweight token or certificate for an authentication where no human mediation is required (for tasks like providing a password). For stronger authentication of individuals in classic IdM, usually multiple factors are combined. These factors are based on the following proofs:

- Something that you have (like a token or certificate).
- Something that you know (like a password).
- Something that you are (like biometry).

In the IoT the last two proofs are not applicable to objects anymore. [52] states certain object identity principles for the IoT:

- An object's identity is separate from the identity of its underlying mechanisms. A computer in a network has an IP address, but it also has a MAC address which makes it uniquely identifiable.
- An object can have one core identity and several temporary identities.
- An object can identify itself using its identity or its specific features. Digital Shadowing [84] projects the virtual identity of a user on the identity of the user's objects, hence only implicitly indicating the user's identity.
- Objects know their owner's identity. A device controlling a user's glucose level should know how that information fits in that user's overall health.

A group of objects can also have an identity, which is also required to be managed. Proving identity is an important part of IdM. The IoT would require an infrastructure that allows mutual object authentication. Also, a balance between centralized and distributed identity management [17] is required. Other important techniques for IdM are anonymization and pseudonym creation. In the IoT an entity could possibly operate in different contexts and might not want to reveal its identity every time. As a result of this, these identity masking technologies are fast gaining popularity. For example, [129] proposes a technique for improving the privacy of Smart Grids through secure anonymization of frequent (for example, every few minutes) electrical metering data sent by a smart meter. Although such frequent metering data may be required by a utility or electrical energy distribution network, it is enough to securely attribute the data to a specific locality, and not to a specific smart meter.

Other IdM issues discussed in [52] are: human and machine authentication, authorization, and granularity. High system security requires combining authentication methods like bioidentification and objects like passport, identity card, or smartphones. Such combinations typically take the form of (what I am + what I know) or (what I have + what I know). Authentication and authorization are highly related concerns, as they together decide who is entitled to assume a role.

However, specific topics, such as delegation, fall under authorization. Granularity is a concept related to authorization. The services an object provides might be modulated based on the number of credentials presented, i.e. authority projected.

Separation of identity and locator is an innovative trend, although the architectural problem of supporting the real people behind the physical device while protecting information about the user and its context has no solution yet [130]. As per [131] various architectures have been proposed in relation to IdM in the IoT, including those concerned with naming, addressing, routing and security issues such as Mobility and Multihoming supporting Identifier Locator Split Architecture (MILSA) and Enhanced MILSA [132, 133]. These architectures are based on identities rather than addresses to organise networks using distributed hash tables [134, 135]. Some of the architectures are concerned with separating the ID and the locator [136]. According to [84], the issue of bringing identity management to the network was first addressed by the EU project Daidalos [137], and further contributions in this direction were made under the EU ICT FP7 project SWIFT [138]. These projects address a vertical approach to identity management, as well as how to leverage identity technologies as an enabling technology for convergence. The concept of Virtual Identity [139] is of relevance to this context. Other prominent IdM schemes are: Microsoft Passport [140], Microsoft CardSpace [141], OpenID [142]. Though these schemes present general Web 2.0 types of approaches, they do not explicitly consider the large population of devices that the IdM would have to manage in an IoT environment [84].

[143] states that the majority of the proposed solutions implement ID frameworks which are applicable within well-defined administrative boundaries, hence creating "identity management islands with interoperability issues". Such solutions shift the problem from the isolation of domains to the isolation of federations and certainly away from network convergence, which is a key aspect of the IoT.

4.1.4 Trust Management

Trust should be deemed to be a vital component of the IoT. Trust in the context of the IoT encompasses the following two concepts:

- Reduction of uncertainty and improvement of trustworthiness of the consti-

tuting elements of the IoT.

- User experience: How comfortable, secure and capable the users feel while interacting with the IoT.

Various trust models have been proposed which define trust in a dynamic, collaborative environment between interacting IoT elements. For example, [144, 145] are examples of distributed trust managements systems for the IoT. While [146, 147] are examples of IoT trust management models based on Fuzzy Reputation. Such models enable the IoT objects to dynamically choose an adequate partner for interaction to accomplish certain function, improving overall reliability of the IoT system.

User trust on the IoT can be instilled by protecting user privacy, providing users adequate control over their services and interactions with the system and providing them clear knowledge of their virtual surroundings. Feelings of helplessness and being under some unknown external control can greatly undermine the IoT's trustworthiness [52]. Governance plays a vital role in strengthening trust in the IoT. [52] recognizes the importance of a common framework for formulation and enforcement of security policies in supporting interoperability and ensuring consistent and continuous security. The Social Governance Framework proposed in this thesis (Chapter 5) shares a similar vision. Such frameworks would also bring accountability in the IoT and strengthen the trust in the IoT.

4.1.5 Fault Tolerance

Fault tolerance is critical for ensuring service reliability. The IoT is especially prone to attacks which would test its fault tolerance due to two reasons:

- Large population of devices producing and consuming services.
- Presence of highly resource-constrained members in the IoT.

The IoT requires specialized, lightweight solutions for fault tolerance issues. [52] recognizes three cooperative measures required to achieve fault tolerance in the IoT:

- *Build security and fault tolerance into all objects.* Along with designing secure protocols and mechanisms, hardware and firmware/software quality of the devices should also be improved. This would reduce physical vulnerability of the devices. Moreover, it is infeasible to provide software patches for billions of devices.

- *Enable all the IoT objects to learn the state of the network and its services.* This would require consistent communication between interacting objects, each giving feedback to many other elements. An important task in this effort is to build an accountability system that will help monitor state.

- *Build resistance against network failures and attacks, and self-recovery in objects.* The protocols should incorporate mechanisms for detecting anomalous situations and allowing objects to gracefully degrade their service. Objects should be able to use intrusion-detection systems and other defensive mechanisms to avoid and defend against attacks. Fast recovery of affected network elements is also desired. [52] suggests that such elements can use feedback from other mechanisms and entities to map the location of unsafe zones, where an attack has caused service outages, and trusted zones with no service outages, and implement recovery services using this information. Mechanisms could also inform human operators of the damaged zone and then perform maintenance operations. This infrastructure self-management is a key the IoT tenet.

4.2 Standardization

Standardization is a huge concern in the development of the IoT. Standardization is required mainly in the following aspects of the IoT:

- Commnunication Protocols and Mechanisms Standardization

- Development Standardization

Communication protocols and mechanisms standardization is necessitated due to the scale of operation, heterogeneity, interoperability requirements, and dispar-

ity in device complexity in the IoT. [56] reflects that although current standardization efforts are making progress in pursuing the secure IP-based IoT, security remains to date, at least partially, unsolved. Section 3.1 discusses the security issues raised by the heterogeneity and interoperability in the IoT which requires standardization of communication and security protocols. [148, 149] addresses the needs of producing specific standards. [26] states that standards are needed for interoperability both within and between domains. Here a domain can even be an organization/enterprise realizing an IoT. Intra-domain standards can provide cost efficient realizations of solutions. Inter-domain interoperability standards would ensure cooperation between the engaged domains, and is more oriented towards IoT applications. There is a requirement of end-to-end standard security protocols and architectures. Standardization is required to be incorporated as a vital activity in the life-cycle process of the IoT. Along with efforts for the "pre-selection" of standards through collaborative research, attention should also be paid to regulation, legislation, interoperability and certification as other activities in the life-cycle.

Comprehensive security also entails standardization of the development of IoT equipments and services. *Development Standardization* would require cooperation of all the stakeholders and following of same design, manufacture and testing standards to ensure consistent and predictable behavior of every network element, and in turn every network domain. Efforts are being made to develop standards for the future the IoT. A workshop,"Internet of Things: Trends and challenges in standardization", was held at ITU headquarters in Geneva on 18 February, 2014, where a multi-disciplinary selection of experts gathered to take stock of progress in the IoT arena with a view of highlighting priorities for its future development [150].

4.3 Governance

Governance, at any level of social organization, refers to conducting the public's business to the constellation of authoritative rules, institutions and practices by means of which any collectivity manages its affairs [151]. Governance would be critical for structured implementation of the IoT and enforcing its reliability. According to [151], a sound governance for the IoT would encompass both legal and social efforts. Legal efforts would mean formulation of comprehensive and highly

relevant (yet not unnecessarily innovation-stifling) policies. Social efforts would focus on enforcing development standards for IoT services as well as ensuring secure implementation and usage of IoT services. However, governance is a double-edge sword. While it offers system, stability, support for political decisions, and a fair enforcement mechanism, it can easily become excessive, resulting an environment which continuously monitors and controls people. If we learn from the Internet's partially solved governance problem, it will take the combined efforts of several research communities to address the challenges of a governance framework when countless stakeholders and objects are involved. The concept of "multi-stakeholder in governance" should be perceived as the new way forward in favor of including the entire society [11]. Though the IoT's future development is hardly predictable, a preliminary assessment of the current environment regarding the Internet's structure, institutional issues and governance principles is desirable. As the IoT uses the Internet, it is important that proposals for governance are considered in cooperation with relevant bodies involved in parallel developments of the Internet. The European Future Internet Assembly [152] is such an organization. Furthermore, [11] suggests that given the difference in stakeholders of the two frameworks (global society vs. mainly businesses), and the difference in purpose, separate (but closely cooperating) governing bodies for the Internet and IoT is a suitable proposition, considering the specific needs of each framework.

We realize the close relation between legal and social governance. For the formulation of policies which are updated and comprehensive, yet not excessively severe on the users or the innovators, the law makers need to have a clear picture of the societal needs and technological trends. This would require adequate information exchange between the law making bodies and the other stakeholders (the innovators, enterprises, and users). Moreover, the formulation of foolproof legislatures and policies is not enough. Efficient policy enforcement mechanisms are required. [52] states, "Future research must also carefully consider the balance of governance and legal frameworks with innovation. Governance can sometimes hinder innovation, but innovation in turn can inadvertently ignore human rights. The right balance will ensure stable progress toward realizing and securing the IoT as envisioned, and the benefits to humanity will be well worth the effort". Figure 4.2 presents the model for IoT Governance.

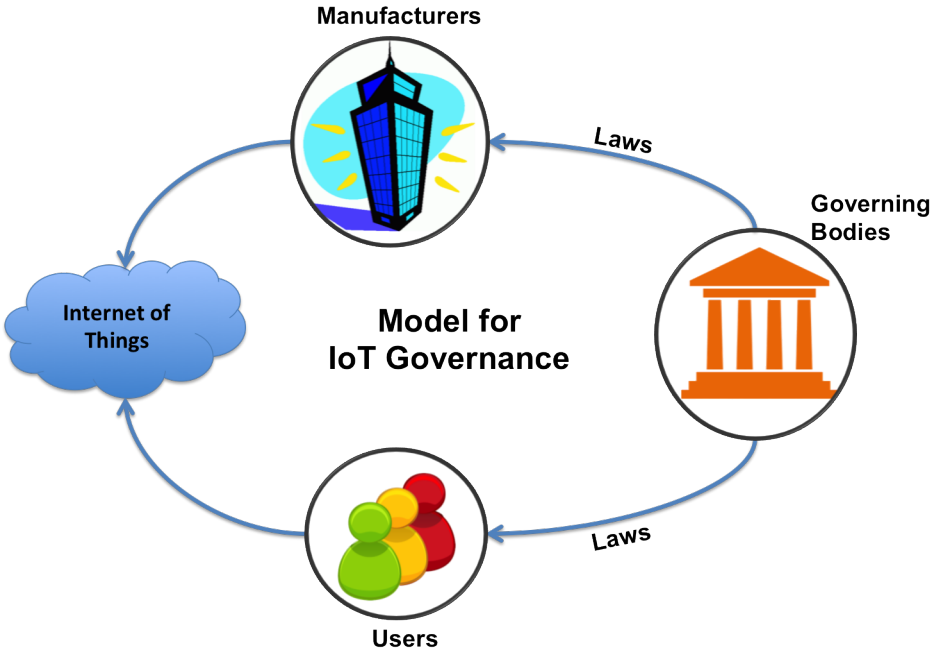

Fig. 4.2 The Model for IoT Governance

The proposed Social Governance Framework (Chapter 5) envisions facilitating adequate information flow between the key drivers of the networked society, to aid sound manufacturing/legal/usage decision making. The framework would also ensure efficient law formulation and enforcement. Such a framework can also provide augmented services to improve data management and accountability of the IoT.

4.4 Social Awareness

At the Final Conference of the CASAGRAS1, in London, October 2009, the project leaders recognized that the governments, industry and business lacked awareness of the IoT and its benefits, and awareness programmes are key requirements in creating a better understanding of the potential and benefits. It is vital to spread IoT related awareness among the enterprises, the government, and the users.

The manufacturers, service providers and enterprises need to consider societal needs and legal obligations while developing IoT services. They also need to

be updated about the development standards set by an established consortium. IoT device and application developers should be aware of secure development practices. Application developers should ensure stable, resilient and trustworthy coding through observing better code development standards, developer trainings, threat analysis and rigorous software testing. Vendors should update device software/-firmware to fix vulnerabilities, but should avoid untrusted third parties to apply the upgrades. Moreover, device manufacturers should build-in maximum possible security in the devices. Devices must be resilient at least to the common attacks. Such resilience can be achieved through application of existing systems engineering tools to security threats, incorporation of security into products by using modular hardware and software designs, using existing open security standards where possible, and through rigorous product testing and review.

The governing bodies need to be aware of the societal preferences, and latest developments in technologies to be able to revise their vision for information security, IT security, operational technology security and physical security, and formulate effective (yet not harsh) policies.

Finally, the users should be aware of secure usage practices, the technologies and policies related to the services, and their social and legal obligations. Enterprises and service providers should maintain transparency by providing complete information of the services and device features to the users. Tools like Privacy Coach [153] and Trusted Tiny Things [97] can empower user awareness. Vendors should list the known vulnerabilities that exist in their devices as part of the purchase process. Moreover, awareness about secure practices like changing default passwords and setting strong passwords, and about the available tools and features which facilitate users' control over the services and their data can help in avoiding the security incidents raised due to the human factor involved in the IoT.

Social Governance can provide an ideal medium for the information exchange required for the awareness of the every stakeholder of the IoT system. It would also reduce the required user awareness by removing the users from the governance loop. Above discussed models of governance and social awareness involve the users as a significant factor in establishing the governance. Users are expected to comply with the laws which dictate what can/cannot be done. With Social Governance users have to comply with the laws, unless the device is compromised.

Figure 4.3 summarizes the above discussions on the solutions for ensuring security, privacy, system and stability in the IoT.

Fig. 4.3 Solutions for security, privacy, system and stability in the IoT

Chapter 5

Social Governance

It is highly desirable to improve the data management, trust, and accountability in the IoT ecosystem, and to align the key players of a networked society to collaborate in the creation, refinement and effective enforcement of the security and privacy policies. This would not only strengthen the defense of IoT systems against threats like undesired/unlawful surveillance, user profiling, active intrusion, and misuse or misrepresentation of services/products, but would also facilitate better awareness and discipline among the key players.

5.1 The Concept

Social Governance is a philosophy of establishing a symbiotic framework to facilitate free flow of information between the three pivotal drivers of the networked society, namely, the *Service and Device Manufacturers*, the *Policy Making Bodies*, and the *Users* of the devices and services, to foster an expeditious, organized, and secure development of the IoT in the society.

Each of the three drivers have different interests for adopting the IoT. If a structured provision is made for ceaseless exchange of information between these three drivers, the development of the IoT would be much more well directed, stable, and secure.

5.2 Evolution of Network Management and Social Governance

The management of the IoT infrastructure is a major concern. IoT management deals with the concerns like how a network resource should be managed and who would manage it. For example, if an organization like McGill University has set up a network infrastructure, there is no question that McGill University is the one who should be managing it and dictate how its resources should be utilized. This is fine in a small, contained network system as the sphere of impact is limited. At most the users are going to worry about things like their emails and web access. It is not really a show-stopper if the management of the network is done in a way which is unsuitable for few/many users.

With the advent of the IoT and the fusion of cyber-physical space, not only has the sphere of impact expanded, the threats have become much more physical than merely virtual. If the way the smart-doors are locked, or smart-lights work are not acceptable by the users, not only would it make their lives inconvenient, an accidental/malicious dysfunction of the system can even bear severe physical consequences.

Network systems management has existed for decades. *Simple Network Management Protocol* (SNMP) was established way back in the 70's [154]. Once widely accepted, over the years SNMP was realized to be inadequate for management of modern inter-networks, and hence *Policy Based Networking* was brought in.

A lot of work has been done on the idea of developing frameworks for policy management in distributed computing systems [155, 156, 157, 158]. In existing frameworks the objective is to enable an enterprise to create programmatic specifications of their operational security policies. These programmatic policies can run and create instances of the policies suitable for any deployment scenario. For example, firewall rules, and access control policies at database servers are created from such policy specifications. Although started mostly as logic-based frameworks, policy frameworks have evolved into risk minimization frameworks, which are closer to the approach of Social Governance.

However, the particular focus of the policy management frameworks remain different. They are geared to allow an enterprise dictate how its resources should be

managed. Whereas, Social Governance is about a larger society, and collaboration of the key players of IoT system, users, manufacturers, and policy makers in the formulation and evolution of the policies.

A policy based network management works fine in the virtual world. But in a physical world, things may not work differently. For example, in a household, a family might have a son who is a gamer. Rest of the family might ask the son to set up his gaming console in his room and not in the living room to avoid disturbing others. The son has the autonomy on his behaviour within his room, but in places of the house outside his room, he is required not to create inconvenience for the rest of the family. Hence, the bigger the space of influence is, there has to be a wider consensus that has to emerge for the governance. The local policies would emerge as part of the consensus. Social Governance strives to provide a framework to facilitate a solution for this tension.

Social Governance would also help in optimizing the actions of each of the IoT stakeholders. For example, if an enterprise is trying to introduce something like Google Glass in a particular region, it would be crucial for the eterprise to be aware of the market status. If the product is only permitted to operate in a very small portion of the region, it may not be a viable decision to market the product in the region. Such information is also critical for the consumers. Currently, no such infrastructure exist which may facilitate such realization.

The Social Governance framework,

- evolves policies in a collaborative manner.
- has to work with incomplete policy formulations.
- formulates some policy rules as a reaction to user actions.

5.3 The Framework

Figure 5.1 illustrates the framework for *Social Governance*. The purpose of the framework is to provide sufficient information to each of the three drivers, to equip them to make the best innovative/production (from innovators' or manufacturers' perspective), political (from policy makers' perspective), and usage (from users' perspective) decisions.

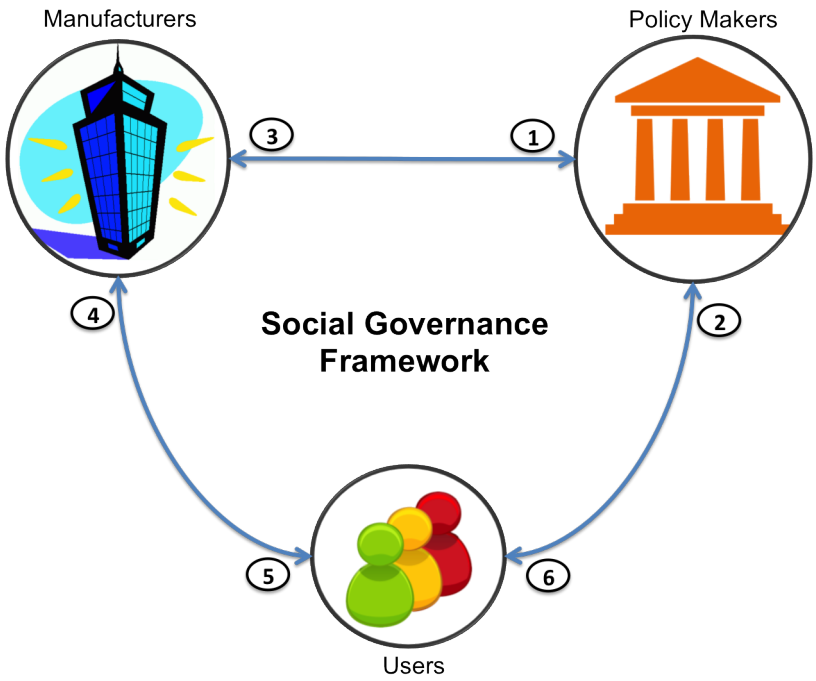

Fig. 5.1 The Social Governance Framework

Before discussing the nature of communications between each pair of the driver entities, let us discuss two critical elements of the Social Governance Framework: the *Hierarchical Distributed Policy Management System* and the *Policy Compliant Smart Devices*.

5.3.1 The Hierarchical Distributed Policy Management System

A *Hierarchical Distributed Policy Management System (HDPMS)*, is a *"DNS-like"* [159] hierarchical and distributed system designed to facilitate enforcement of security and privacy policies formulated by policy making bodies with different scopes of authority, synergistically. The use of hierarchical and distributed systems has been prevalent in computer networks [160, 161, 162, 163].

HDPMS would ensure high availability of location and context specific policies. A hierarchical policy management system would be useful in contexts where the authority to formulate policies is decentralized and delegated to multiple bodies. In real life scenarios, security and privacy policies of an area may be the outcome of

decisions made by multiple bodies with different degrees of authority. For example, the government of a nation may allow the use of a certain technology/product, say Google Glass, but the administration of an office might forbid it's use within the office premises. Or the office administration may have no specific regulations for Google Glass, but the law of the land might have banned it. Hence, the policy for a specific location must be a logical compilation of the policies enforced by all the relevant authorities. Figure 5.2 indicates the scope of relevance of the security and privacy policies enforced by different authorities.

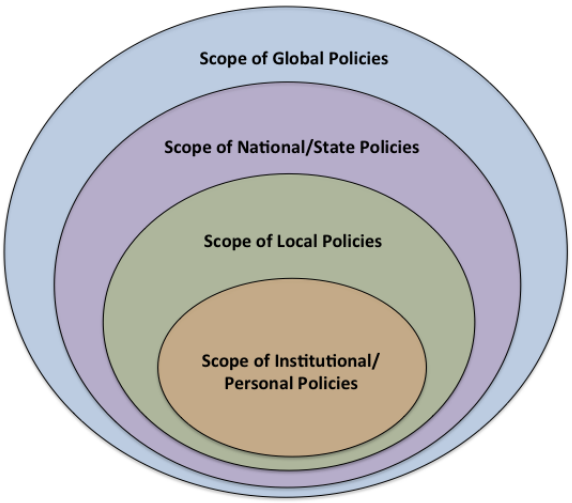

Fig. 5.2 Scope of Policies Enforced by Different Authorities

A hierarchical policy management system would provision for each of the concerned policy making bodies to implement the formulated policies at respective levels in the hierarchy and then composing decisions based on the relative importance of the policies at each level of the hierarchy [164]. The domain of authority descends from top to bottom in the hierarchy. Figure 5.3 illustrates a typical HDPMS. The compilation of the policies for a location and context, based on the existing policies in each level of the hierarchy is discussed in details in Section 5.3.5.

During the functioning of the HDPMS, the policy servers receive policy information from the higher level servers in the form of policy response messages (refer Section 5.3.5). To reduce the latency of response to policy requests, the

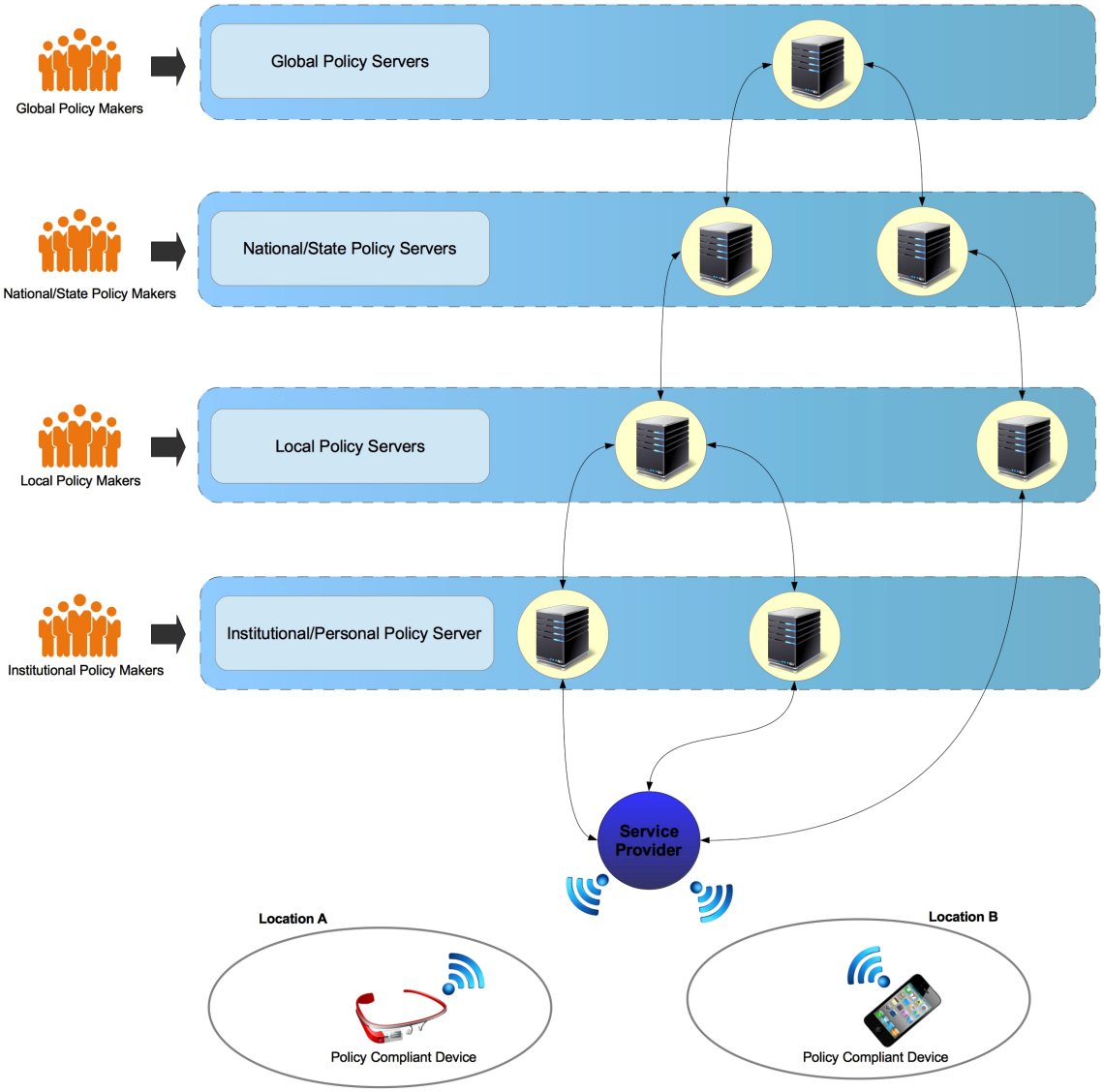

Fig. 5.3 The Hierarchical Distributed Policy Management System

servers cache the policy information received from the higher level servers for a fixed amount of time, after which the cached data becomes stale. If a policy request is received at a server and the relevant policies of the higher domains are either unavailable locally, or the cached data has expired, the server sends an inquiry message for the requested policy to its parent. The HDPMS can have some augmented features which can aid in making the policy-formulation and enforcement procedure much more dynamic and efficient (refer Sections 5.3.8 and 5.4). Figure 5.4 depicts the work-flow of a typical HDPMS server.

5.3.2 Policy Compliant Smart Devices

With more and more things (devices, objects, or even living beings) becoming *"smarter"*, mobile and less visible, a challenge bigger than formulating reliable security and privacy policies is ensuring high policy adherence. The commercial usage of IoT enabled devices would require fine-grained security enforcement as opposed to the current "perimeter-based" enforcement [165]. Security needs to be an inherent feature and integral part of the architecture. The bootstrapping of smart things in security domains [17, 166] is an effective solution for smart things which are joining a particular security domain. For example, if a device present in the premise of an organization is trying to access the organization's communication infrastructure, a secure bootstrapping would ensure policy adherence by allowing/denying access to the device, and monitoring and controlling its activities. But what happens when a smart thing which is physically present at a protected premise, has its own network connectivity (e.g. 3G/4G network link)? How could the adherence to the local *"device etiquette"* be ensured? A failure in controlling such devices' activities within protected premises might lead to severe security/privacy breaches.

[167] presented *"Policy-Aware Smart Objects"*, which are activity-aware objects with added embedded policy model. These systems operate according to the *"static"* embeded policies. The *Policy Compliant Smart Devices (PCSDs)* could be an augmented version of Policy-Aware Smart Objects, operating on policies which are not embeded, but dynamic and location-specific. PCSDs would find its applicability in a much more extensive domains of the IoT. PCSDs would be de-

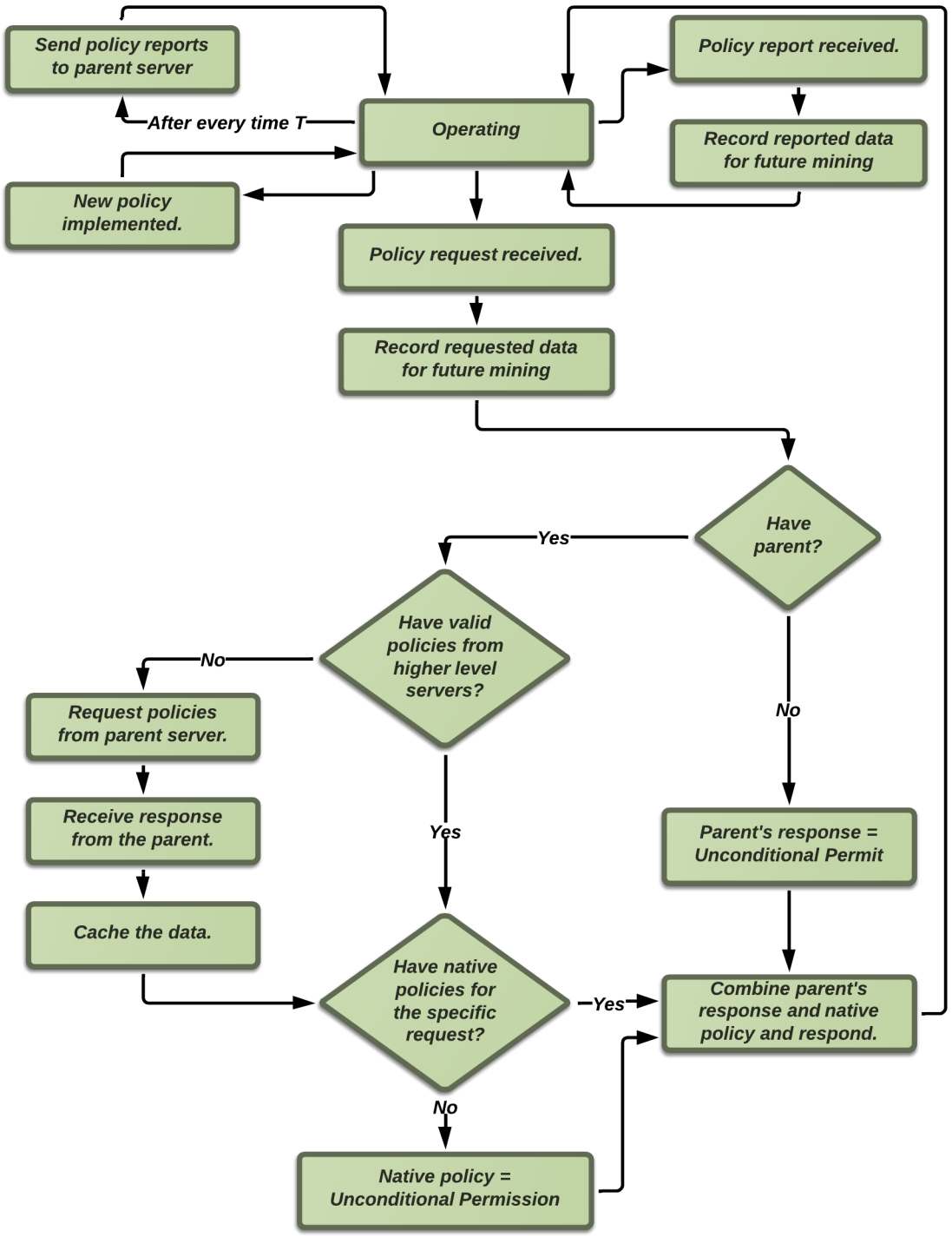

Fig. 5.4 The Work-flow of a Typical HDPMS Server

signed to determine the security and privacy policies of its locality and inherently adhere to them, irrespective of the activities of the device owner. With PCSDs, the users would have no control over the degree to which the rules are followed. Policy adherence mechanisms would be built into a PCSD, helping in avoiding malicious or unintentional infringement of privacy and security in the locality.

The idea of a PCSD is also mildly inspired by the concepts of Privacy Coach [153] and LoPSiL [168]. Privacy Coach explicitly fetches the product policies of any IoT application or device that the user wishes to use, and makes the user aware of the usage policies and implications. *Location-Based Policy-Specification Language (LoPSiL)* is used to specify the security and privacy policies by the user, and then compile the untrusted application to be used with the *"policy program"* to obtain a secure policy compliant application. PCSDs borrow the concept of *"policy conscious decision-making"* from [153], and the idea of *"making security and privacy default in applications"* from [168].

Some of the benefits of the Policy Compliant Smart Devices are:

- Guaranty of security and privacy policy adherence by IoT devices.
- Effective policy enforcement requires minimal user and administrator participation.
- Few security and privacy incidents boost manufacturers' reputation and product reliability.

5.3.3 HDPMS and PCSDs in Action

Figures 5.5 and 5.4 depict the work-flows of a PCSD and a HDPMS, respectively, in a typical IoT environment. Figure 5.6 shows the major communications in the HDPMS-PCSDs setup. The functioning of the HDPMS-PCSD based IoT environment is described below.

- Every PCSD would be considered as an aggregation of multiple *functionalities*. For example, a smartphone can be considered to be composed of functionalities like voice calling, text messaging, video recording, audio recording,

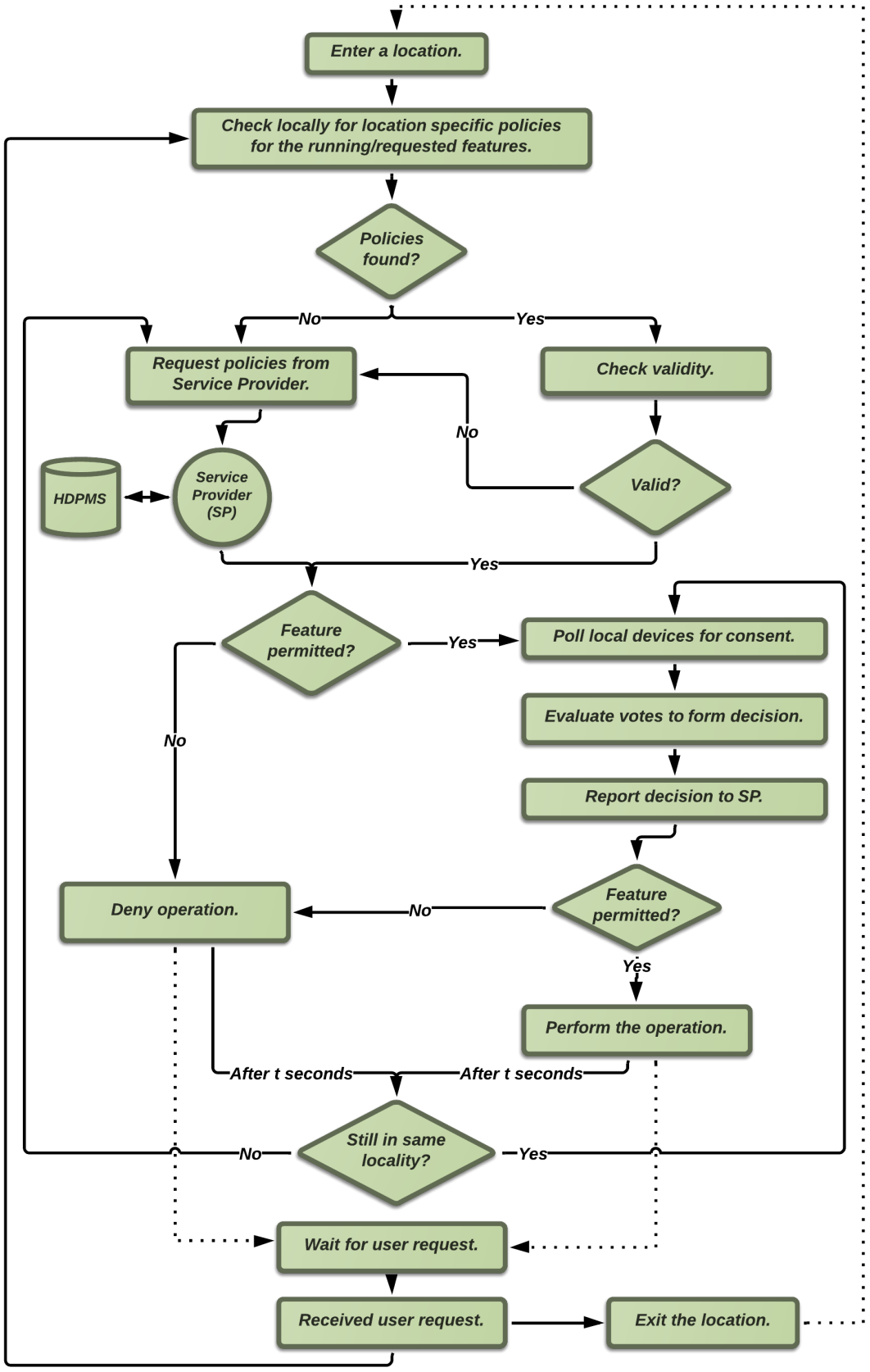

Fig. 5.5 The Work-flow of a Policy Compliant Smart Device

media playing, and direction finding. Each functionality would have a standardized description. The manufacturers who wants to include any functionality in their devices, would have to assign that unique description to the functionality. For example, if the *Functionality ID* for media playing is, say PLAY_MEDIA, then every device incorporating this functionality would recognize the functionality by the same Functionality ID (PLAY_MEDIA).

- Each functionality is associated with a set of one or more *actions (denoted by 'a')*. Actions are those elements of a functionality for which the functionality is deemed to require permission to operate at any particular location and context. For example, the media playing functionality (Functionality ID: PLAY_MEDIA) of any device can be considered to have actions like volume, genre of music played, etc, as a locality might have specific policies for the loudness and the type of music that can be played in the locality.

$$\textit{Actions for functionality, } f_1 = \{a_{1,1},\ a_{1,2},\ a_{1,3},\ a_{1,4}\}$$

- The PCSDs would request policies for the actions of all running (or requested to run) functionalities after every $\boldsymbol{t}$ seconds. The policy request format has been explained in Sections 5.3.4. The value of $\boldsymbol{t}$ can be determined based on the characteristics of the device, like mobility. A device that changes its location/context very frequently would require frequent refreshment of policies, and hence a smaller value of $\boldsymbol{t}$. The value of $\boldsymbol{t}$ can be designed to be changed by the OS of a device as per the rate at which the device changes its location.

  Moreover, the rate policy refreshment should consider the local policy as well. In scenarios where a specific location might want to ensure that the changes in a local policy are immediately observed, as and when they are implemented, it is required that the PCSDs in the area to detect and adhere to that policy within a certain time limit. This can be achieved by provisioning for the local policy to specify the desired rate of policy refreshment. The device should follow the rate specified by the local policy, or the one calculated by the device itself, whichever is higher.

- A PCSD first queries the service provider for the policies (*Label 1* in Figure 5.6). The service provider in turn queries the HDPMS for the local policies (*Label 2* in Figure 5.6), and relays back the response received from the HDPMS, to the requesting device (*Labels 3 and 4* in Figure 5.6).
- When queried for policies, if the HDPMS has valid policies for the functionality, it responds back to the service provider with the policies. Else, it responds with an unconditional grant for the particular functionality to operate in the locality. The policy resolution in HDPMS is explained in Section 5.3.5.
- If the response received from the service provider prohibits operation of the particular functionality with the requested action in the locality, the functionality is disabled for $\boldsymbol{t}$ seconds before a fresh policy is requested from the service provider.
- Whereas, if the response received allows the functionality to run with the requested action in the locality, then the device undertakes the following procedure.
  - The PCSD would seek local consent on the operation of the functionality through a polling protocol based localized broadcast communication similar to ARP [169] or NDP [170]. The device would broadcast a policy request message within its physical locality, to which only the local *policy compliant devices* can reply (*Label 5* in Figure 5.6). The local consent polling mechanism is discussed in Section 5.3.6.
  - If the requesting device does not receive any response from the locality, the OS of the device assumes to have unconditional permission for operation of the functionality with the requested actions in the locality and context. Else, the OS of the device enables or disables the functionality based on the majority formed by the peer votes.
  - If enabled, the functionality operates for $\boldsymbol{t}$ seconds before requesting fresh permission. Whereas, if the functionality is disabled, it would be disabled for $\boldsymbol{t}$ seconds, before a fresh permission is requested. If at the

end of the t seconds, the device's physical location is still within the area which it had polled for the previous vote, it can directly poll for the local consent once again. Else, it would request the service provider for a fresh policy.

- Whenever a decision on the operation of a functionality is formed based on local votes, the PCSD reports the details of the decision, i.e. the Functionality ID, the decision (approval/denial) and the conditions of approval/denial (e.g. the time of the decision, the actions and the values permitted and/or prohibited), to the HDPMS through the service provider (*Labels 7 and 8* in Figure 5.6). Section 5.3.4 discusses the report message format.
- Reported data of the decision made by the local votes is received by and stored into the lowest level policy server in the HDPMS. The information is not used by the HDPMS immediately for formulating/modifying any policies. Collection of such data over a considerable period of time, can be mined for critical information and patterns, aiding in amending existing policies or formulation of new policies. Every policy server in the hierarchy would periodically report all its policies to its parent server. If any information mined from the data collected through the decision reports sent by the PCSDs is found to be significant enough to culminate in policies, the policies would first be enforced in local domain. Through the periodic policy reporting by the policy servers to their parents, if a consistent pattern is found for a particular functionality in the policies reported by all the children servers of a policy server, it might itself amend/create policies accordingly.

5.3.4 Communications in HDPMS-PCSDs Setup

Figure 5.6 depicts the communications between the PCSDs, the service providers and the HDPMS, in a typical HDPMS-PCSDs setup. Note that the figure is not a comprehensive depiction of all the types of messages exchanged in the setup. There are intra-HDPMS message transmissions between the policy servers as well,

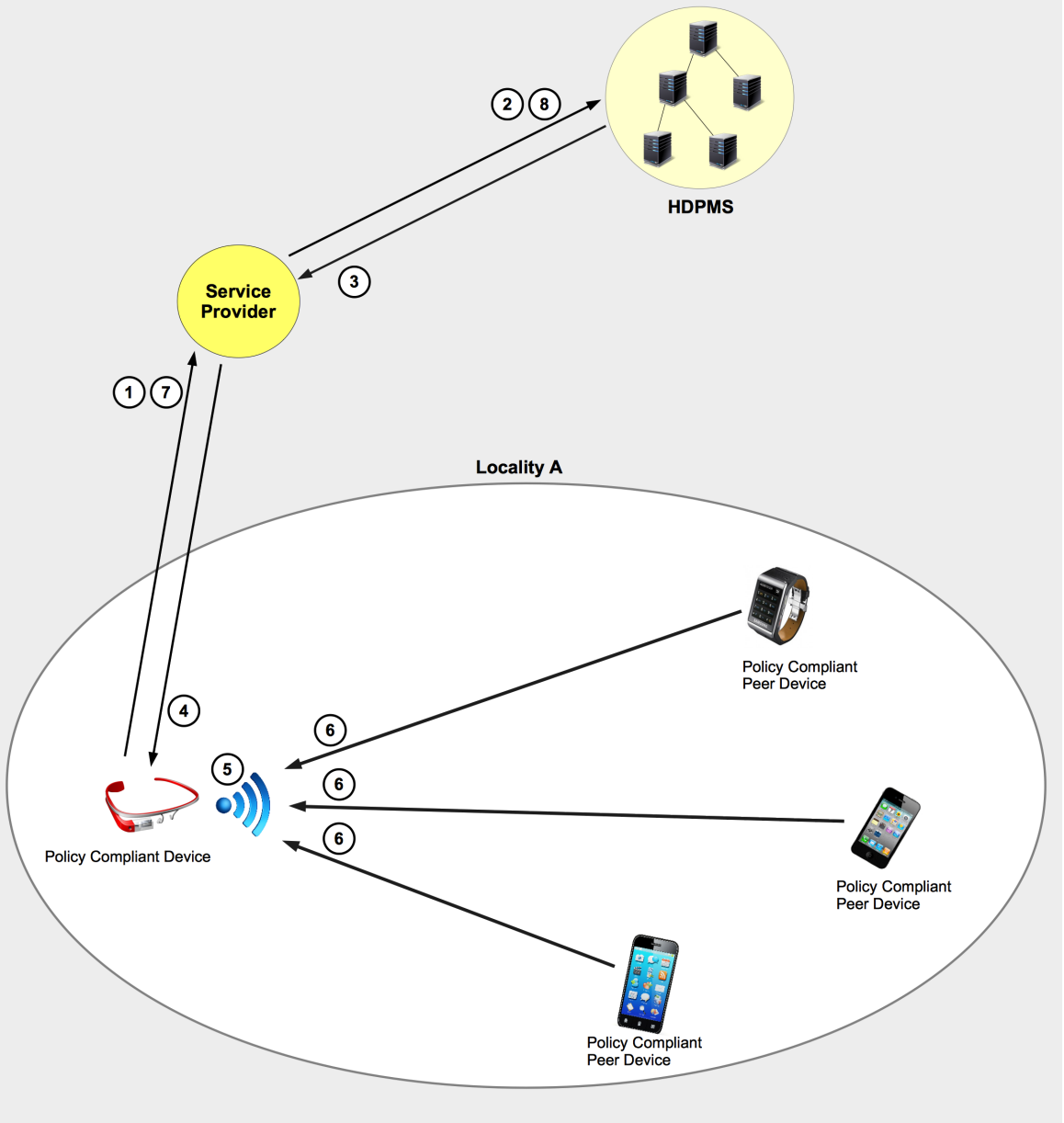

Fig. 5.6 The Communications in HDPMS-PCSDs Setup

which are not shown in the figure, but are explained in Section 5.3.5. Three major types of messages that circulate in the HDPMS-PCSDs setup are *policy request*, *decision report* and *policy response*.

- ***Policy Requests:*** These messages are primarily initiated by PCSDs inquiring the location-based security policies for the functionalities running in them. They are used to request policies from the service provider (*Label 1* in Figure 5.6), as well as from the local peer devices, in case of local consent based decision-making (*Label 5* in Figure 5.6). The same messages are relayed by the service provider to the HDPMS (*Label 2* in Figure 5.6), and also used by the policy servers in HDPMS to request policies from their parent servers, if required. For a node $\boldsymbol{n_1}$, a composite statement,

  n_1 **REQUESTS** y $\{(f_1,\ a_{1,1}),\ (f_2,\ a_{2,1},\ a_{2,2}),\ (f_3,\ a_{3,1},\ a_{3,2},\ a_{3,3}),\ (f_4,\ a_{4,1})\}$

  denotes $\boldsymbol{n_1}$, which may be a request initiating device, a service provider, or a policy server in the HDPMS, requesting policies for each functionality-action pair from $\boldsymbol{y}$. The composite statement comprises multiple individual requests denoted by,

  $$n_1 \textbf{ REQUESTS } y \{f_1,\ a_{1,1}\}$$

  $$n_1 \textbf{ REQUESTS } y \{f_2,\ a_{2,1}\}$$

  $$n_1 \textbf{ REQUESTS } y \{f_2,\ a_{2,2}\}$$

  $$\vdots$$

  $$n_1 \textbf{ REQUESTS } y \{f_4,\ a_{4,1}\}$$

  The format of the *policy request* messages has been depicted in Listing 5.1 under the tag <policy_request>. The field *message_type* denotes the type of information contained in the message (*request* in this case). The message also contains the identity of the source of the policy request message (*source_id*),

the identity of the device initiating the policy request (*device_id*), and a pair of a *functionality_id* and an *action*, for which the device is seeking the local policy. For a particular policy request, the Source ID (*source_id*) keeps changing as the request message is transmitted between different nodes of the HDPMS-PCSDs setup, but the Device ID (*device_id*) remains constant throughout the request-response cycle. For example, if a device $\boldsymbol{d_1}$ requests a policy to the service provider or to its local peers, the Device ID of the message would be $\boldsymbol{d_1}$ throughout. In this case the Source ID would be $\boldsymbol{d_1}$ as well. When the request is transmitted from the service provider to the HDPMS, the Source ID would be the identity of the service provider. And finally, if the request is transmitted by a policy server to its parent in the hierarchy, the Source ID would be the identity of the requesting policy server.

Listing 5.1 Message Transmitted in HDPMS-PCSDs Setup

```
<message_formats>

   <policy_request>
      <message_type> request </message_type>
      <source_id>...</source_id>
      <device_id>...</device_id>
      <feature_id>...</feature_id>
      <action>...</action>
   </policy_request>

   <policy_response>
      <message_type> response </message_type>
      <source_id>...</source_id>
      <device_id>...</device_id>
      <feature_id>...</feature_id>
      <permission>...</permission> <!- allow/deny -->
      <condition_for_denial>...</condition_for_denial>
      <!- condition_for_denial considered only when
          permission == deny -->
   </policy_response>

   <policy_report>
      <message_type> report </message_type>
```

```
23        <source_id>...</source_id>
24        <device_id>...</device_id>
25        <feature_id>...</feature_id>
26        <permission>...</permission> <!- allow/deny -->
27        <permission_condition>...</permission_condition>
28    </policy_report>
29
30 </message_formats>
```

- ***Policy Responses:*** These messages are initiated by the policy servers in the HDPMS (*Label 3* in Figure 5.6) or the local peers of a PCSD in response to the policy request messages which are initiated by the PCSD (*Label 6* in Figure 5.6). It is also used by the service provider to relay HDPMS's response to the requesting device (*Label 4* in Figure 5.6). The possible forms of policy response messages are: **GRANTS** and **DENIES**. The composite statement,

$$y \textbf{ GRANTS } d_1 \{f_1, f_3\}$$

denotes node $\boldsymbol{y}$, which can be a policy server in HDPMS, the service provider, or a local peer device, allowing the functionalities $\boldsymbol{f_1}$ and $\boldsymbol{f_3}$ to operate with the actions requested by device $\boldsymbol{d_1}$. This statement comprises multiple individual responses denoted by,

$$y \textbf{ GRANTS } d_1 \{f_1\}$$

$$y \textbf{ GRANTS } d_1 \{f_3\}$$

Similarly, the composite statement,

$$y \textbf{ DENIES } d_1 \{(f_2, <conditions>_2), (f_4, <conditions>_4)\}$$

denotes node $\boldsymbol{y}$, denying the functionalities $\boldsymbol{f_2}$ and $\boldsymbol{f_4}$ the permission to operate with the actions requested by device $\boldsymbol{d_1}$ in the locality. The response message also contains the conditions based on which the permission was denied. Once again, this statement comprises multiple individual responses denoted by,

$$y \textbf{ DENIES } d_1 \{f_2, <conditions>_2\}$$

$$y \textbf{ DENIES } d_1 \{f_4, <conditions>_4\}$$

The conditions for denial are supplied in the response message to aid in the device's awareness about the reason for denial of permission to run the particular functionality in the location. This can help the device to adjust the values of the requested actions of the functionality, to make it suitable to operate in the locality, if required and if possible. For example, if a policy compliant smart car enters a locality which has a permissible speeding range of 20 to 45 MPH, and is speeding at 55 MPH, the car would request for the local policy for its different operational functionalities including running. One of the actions of 'running' would be speed. When the HDPMS receives the request from the car for running at the speed of 55 MPH, it responds with a denial of permission. In this condition, if the OS of the car is not supplied with the condition for denial, it would not know any other way to obey the policy but to instantly stop! This of course is not a practical solution. If the OS of the car receives the conditions for the denial in the response, i.e. if in this case the car receives a denial of running at 55 MPH, and the condition "Speed Limit = 20 MPH-45 MPH", the OS can either warn the driver, or automatically slow down into the permissible speed limit.

The format of the *policy response* messages has been depicted in Listing 5.1 under the tag <policy_response>. The field *message_type* denotes the type of information contained in the message (*response* in this case). The message also contains identity of the source of the message (*source_id*), identity of the device which initiated the policy request (*device_id*), description of the functionality on which the decision has been made (*functionality_id*), the permission (*permission*), and the conditions for denial (*condition_for_denial*). As discussed earlier, the condition_for_denial is needed to be considered only when the permission has the value 'deny'. Like the policy request messages, for a particular response, the source_id keeps changing as the response message is transmitted between different nodes, but the device_id remains constant throughout. Section 5.3.5 explains the policy resolution in the HDPMS while forming the response for the policy requests.

- ***Decision Reports:*** These messages are sent by a PCSD to the HDPMS, through the service provider (*Labels 7 and 8* in Figure 5.6), whenever the device makes a operation decision for any of its functionalities based on the local vote. Such reports can help in effective representation of the local activities and opinions on various technologies to the policy servers, which in turn can culminate in formulation of highly location and context relevant and robust policies. For a node $\boldsymbol{n_1}$ (a PCSD or a service provider), the following composite statement,

$$n_1 \textbf{ REPORTS } y \{(f_1,\ decision_1,\ <decision\_conds>_1),\ (f_2,\ decision_2,\ <decision\_conds>_2)\}$$

denotes $\boldsymbol{n_1}$ reporting of decisions made on operation of functionalities $\boldsymbol{f_1}$ and $\boldsymbol{f_2}$ based on the local vote, and the conditions based on which the decision (permission/denial) was formed. This composite statement of decision reporting comprises multiple individual reports of the forms,

$$n_1 \textbf{ REPORTS } y \{f_1,\ decision_1,\ <decision\_conds>_1\}$$

$$n_1 \textbf{ REPORTS } y \{f_2,\ decision_2,\ <decision\_conds>_2\}$$

The format of a decision report message has been depicted in Listing 5.1 under the tag <policy_report>. The field *message_type* denotes the type of information contained in the message (*report* in this case). The message also contains the identity of the source of the decision report message (*source_id*), the identity of the device initiating the report (*device_id*), the identity of the functionality on which the decision has been made (*functionality_id*), the decision (*permission*), and the conditions based on which the decision has been made (*permission_condition*). The conditions are basically a compilation of the all the conditions under which each of the actions of the functionality were allowed/denied to operate in the locality. Similar to policy request and response messages, for a particular report message, the Source ID keeps changing as the request message is transmitted between different nodes of the HDPMS-PCSDs setup, but the Device ID remains constant throughout.

5.3.5 Policy Resolution in the HDPMS

The HDPMS is a hierarchical and distributed system in which policies are simultaneously implemented at multiple levels of the hierarchy. The domain of authority broadens as we go from the bottom to the top in the hierarchy. Hence, the resultant policies for a location are obtained by compiling all the relevant policies across the height of the hierarchy. As explained in Section 5.3.1 and illustrated in Figure 5.3, the incoming policy request messages that are initiated by the PCSDs and forwarded by the service providers, are first received at the lowest level policy server of the HDPMS. As shown in Figure 5.4, the policy server tries to respond back to the request by using its local policies (if any) and the cached copies of relevant policies that have been received from policy servers higher in the hierarchy. If a server does not have any relevant policies from the higher servers cached locally, or the validity of the cached data has expired, then it sends a *policy request message* to its parent server, and this procedure is continued recursively.

The upward traversal of the policy request message in the hierarchy terminates when either the top of the hierarchy has been reached, or the request reaches a policy server which has a valid cached copy of the relevant policies received from its parent. At this point the *policy response* message originates (check Listing 5.1, under the tag <policy_response> for the message format). Based on the policies for the requested functionality, each server decides if the requested action value of the functionality is permissible or not. If it is permissible, the local permission of the server is to *'allow'* operation of the functionality-action pair. Else, the local permission is to *'deny'* operation of the functionality-action pair. The policy server combines this local permission with the permission contained in the policy response message received from its parent. The rule for permission combination is as follows,

$$\textit{Resultant Policy} := \textit{Parent Policy}\ \textbf{AND}\ \textit{Local Policy}$$

If the local permission is to *'allow'* the operation of the requested functionality-action pair, only the permission of the incoming policy response from the parent is modified, to generate the resultant policy response message which the server forwards to its child. If the local permission is to *'deny'* the operation of the requested functionality-action pair, along with the modification of the permission,

the local *'condition_for_denial'* is merged with the conditions that are descending from the higher levels. In special cases like the local server being the top level policy server, or the local server having valid cached copy of the relevant policies, solely the local permission (and if required, the conditions for denial) are released as the output response message to its child.

5.3.6 Local Consent Polling Mechanism

As discussed in Section 5.3.3, while requesting the policy for a particular functionality-action pair from the service provider, the PCSD receives permission to operate in two scenarios: 1) the requested functionality with the action value is permissible as per the relevant policies contained in the HDPMS, and 2) the HDPMS does not have any relevant policy for the functionality-action pair. In both the cases, the PCSD polls for the consent of the local *PCSDs* to learn the *"local etiquette"*, i.e. whether the local PCSDs are willing for the particular functionality-action pair to be operational in the locality. The capability of casting its rules on the operation of a functionality in its physical proximity can be built into a PCSD.

The concept of using peers' opinion in decision-making through polling is common in distributed network protocols [171, 172] and peer-to-peer communications [173]. In the first scenario mentioned in the previous paragraph, local vote polling could be useful as the opinion of local people might differ from the enforced policies in specific contexts. For example, an university might allow the calling and text messaging functionalities of cell phones in its premise, but at the same time an examiner might want to prohibit their use in an examination hall. In such cases local consent polling can prove effective in imposing the preferences of the local authority even when relevant polices are not in place. A mechanism can be set up allow some local voting devices' votes to weigh more in the decision making. Moreover, as discussed in Section 5.3.3, the decision made through local voting is reported to the HDPMS. This aids in registering the opinion of the users of a locality on particular functionalities, which can culminate in more relevant and effective policy formulation.

Labels 5 and 6 in Figure 5.6 represent the local consent polling mechanism. The policy request message is broadcasted in the physical locality (*Label 5* in

Figure 5.6). The communication for consent polling can be setup using the Bluetooth technology with automatic connection initiation (no requirement of pairing) enabled in the devices [174].

The peer PCSDs would have the capability to let their users set their preferences for the behavior of different functionalities of PCSDs in their physical proximity. For example, an owner of a policy compliant smart watch might not want to be photographed or videographed at his/her workplace. He/she can set the smart watch's preference likewise. When the device receives a policy request from a local peer for the camera functionality, the device would respond with a vote against the request. A vote against a request is accompanied by the condition for denial. In case the device does not have any relevant rule, it votes in favor of the request. This communication (*Label 6* in Figure 5.6) uses the policy response message.

Based on the response votes received, the polling PCSD decides on the operation of the functionality-action pair in the locality. The decision is aligned with the majority of the votes. To base the decision on the votes received, the polling device needs to trust the votes [173]. The reliability of the messages exchanged and of the behavior of the devices in general can be ensured by: 1) securing the communications and communications channel, and 2) by developing a trusted computing base (TCB) in the policy compliant smart devices.

5.3.7 Trusted Computing Base in the IoT

One of the motivations of Social Governance is to endorse active participation of the users of devices and technologies in policy formulation and enforcement. Accomplishing this goal would imply a greater role of user actions on the formulation of policies, and ultimately on the security and privacy of the society. The users would virtually be represented by the PCSDs they own. Hence, the obvious first step towards ensuring integrity of the framework is by safeguarding the integrity of the PCSDs. The integrity of the PCSDs need to be enforced in two different ways:

- Prevent the PCSDs from ignoring the policy directives.
- Prevent the PCSDs from registering fake/incorrect votes.

The PCSDs can be developed with a trusted computing base. [81] defines the trusted computing base (TCB) as everything in the trusted operating system on which we depend for correct enforcement of policy. The TCB protects the integrity of the system by separating all the parts of the trusted operating system that handle the security related operations, from the rest of the elements. The trust in the security of the entire system would completely depend on the TCB. [81] recognizes the following as the elements of an operating system on which the security enforcement could depend:

- *hardware*, including processors, memory, registers, and I/O devices
- *security-critical processes*
- *primitive files*, like the security access control database and identification/authentication data
- *protected memory*, to protect the reference monitor against tampering
- *interprocess communication* used to pass data within different parts of the TCB.

The TCB is generally required to contain a small part of the entire trusted OS. Figure 5.7 represents the composition of a trusted OS. The TCB should monitor the following four basic activities.

- *Process activation:* Context switching in multiprocessing systems requires change of security-sensitive resources and information like registers, relocation maps, file access lists, and process status information.
- *Execution domain switching:* Processes running in one domain might invoke processes in other domain to obtain sensitive data or services.
- *Memory protection:* As each domain has access to some part of the memory, the TCB must monitor memory references to ensure confidentiality and integrity of all the domains.
- *I/O operations:* Software involved in I/O operations can connect domains outside the trusted computing base to trusted domains.

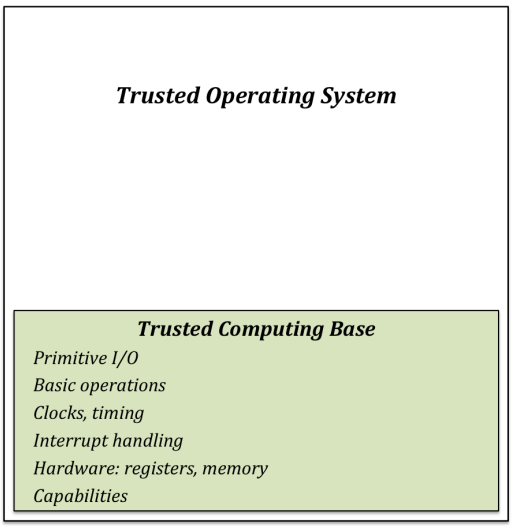

Fig. 5.7 The Trust Computing Base in PCSDs

Moreover, modern computing devices contain autonomous processing elements that all have field-upgradable firmwares and are integral part of a computer system's trust model [175]. Hence, during the secure booting of a trusted device, the firmwares of the field-upgradable devices should also be verified. [175] propose augmentation of the secure booting of computing devices with mechanisms to protect against compromises to the field-upgradable devices.

5.3.8 Social Governance for Policy Makers

The Social Governance Framework will facilitate more effective security and privacy policy formulation and enforcement.

- ***Communication with Manufacturers/Innovator:*** Refer to *Label 1* in Figure 5.1. Systematic communications with the manufacturers/innovators can confer the policy makers a clear understanding of their visions and motives, and the capabilities and implications of the technologies. Such communications can take many possible forms. The innovators/manufacturers may be required to acquire *innovational licenses* [176] or *manufacturing licenses*, respectively, for their technologies/products. The process of acquiring the license would require the innovators/manufacturers to present their idea and

intentions to the policy making body. This would help in avoiding formation and imposition of unreasonable, weak or extremely strict security/privacy policies.

- ***Communication with Users:*** Refer to *Label 2* in Figure 5.1. The proposed framework can enable the policy makers to consider user preferences while formulating policies.

  The HDPMS-PCSDs setup can be used as a learning mechanism by the policy makers to learn about the activities of different types of devices in their region over a period of time. Whenever a device requests for a policy for any of its functionalities, the HDPMS can procure the data, which can aid in future decision making. When a technology/device is introduced in the market, the policy makers of a region may not enforce any specific policies for it due to reasons like lack of popularity of the product in the region, or even ignorance of the administration. When policy requests are received from such devices, the policy servers of the region would be unable to respond with any specific policy, and would relay more generic policies from the higher level servers. The server can keep track of such queries. If the frequency of such queries exceeds a set threshold for a considerable amount of time, the policy makers may roll out specific regulations for the functionality.

  Furthermore, mining of data like for which functionalities of a particular type of devices are policies being most frequently requested for, can help make the policies more granular. For instance, an institution may prohibit the usage of GPS services within its premise. So enforcing a policy requiring all GPS enabled devices to suspend all the signal transmitting functionalities would unnecessarily disable a smartphone's capability of calling or text messaging. Data procured over time indicating high amount of requests for using the calling or messaging functionalities by smartphones, can advice the policy makers to revise the policy and explicitly prohibit just the GPS functionality.

  Some of the benefits of such a learning mechanism for the policy makers are,

  - Makes the policies highly location-specific and robust over time.
  - Helps in avoiding redundant policies.

  - Data collected from the users, along with the information acquired through communication with the manufacturers, give the policy makers a practical premise to base their decisions upon, in turn increasing their accountability.
  - By refining the granularity of the policies, the usability of devices/technologies may be improved.

- ***Policy Enforcement:*** With the proposed framework, policy enforcement would be much more efficient. The HDPMS would enable policy makers with different scopes of authority to form highly location and context specific policies. HDPMS would make the enforcement and administration of the policies effective and systematic.

5.3.9 Social Governance for Innovators/Manufacturers

The innovators and the manufacturers of IoT technologies and devices would possibly be the biggest beneficiary of the Social Governance Framework.

- ***Communication with Policy Makers:*** Refer to *Label 3* in Figure 5.1. The communication with the policy makers would enable the manufacturers/innovators to have a better knowledge of the policies of any region. This knowledge may be derived from the policies that have been explicitly defined for the genre to which the technology/product under consideration belongs. If no explicit policies are enforced for the genre, it might be possible to still gain some important knowledge from policies enforced on technologies/products which include some of the functionalities of the product under consideration. For example, an office might not have yet implemented any explicit policies for the use of Google Glass within its premise, but a policy which prohibits usage of cameras within the premise would indicate that the camera functionality of a Google Glass might not be permitted to operate as well. A sound understanding of the legal limitations would save the innovators/manufacturers the efforts of conceptualizing, developing and marketing a product which might ultimately get axed by legal prohibitions. Moreover,

such knowledge would also help in refinement of their ideas/products to better fit the societal requirements. Also, an organized communication between the manufacturers/innovators and the policy makers (for example, acquisition of license) increases accountability of both the parties, as the policy makers would have to allow or reject a product sensibly, and the innovators/manufacturers would have to cohere to the commitment of intentions and implications of their product as declared in the license.

- ***Communication with Users:*** Refer to *Label 4* in Figure 5.1. The communication between the producers and the consumers of the IoT technologies and devices, would lead to a well directed and rapid growth of the IoT in the society. The proposed framework would make updated information about user preferences available to the innovators/manufacturers, equipping them to make better design and deployment decisions.

  Moreover, a structured communication would enable the innovators/manufacturers to create a quality user base. They can spread awareness about the features and implication of the products, as well as about secure usage practices. A quality user base would mean less security and privacy incidents, and better reputation of the products and manufacturers.

- ***Policy Compliance:*** The remarkable concept of the PCSDs would make the policy enforcement effective by ensuring high policy adherence on part of the smart devices. PCSDs would enable the manufacturers to produce more secure devices, which in turn would benefit their reputation.

5.3.10 Social Governance for Users

Social Governance Framework would make the adoption of new technologies and products by the users, much easier, well informed and secure.

- ***Communication with Manufacturers/Innovator:*** This corresponds to the label 5 in Figure 5.1. The provision of systematic communication with the manufacturers and innovators would enable the users to have a better understanding of the technologies and products, and the implications

of using them. It would also empower the users to demand more transparency in manufacturer's/innovator's policies.

- ***Communication with Policy Makers:*** This corresponds to the label 6 in Figure 5.1. The augmented utility of HDPMS discussed earlier enables the policy makers to mine vital information from the policy requests received over a period of time. This information helps the policy makers to formulate relevant and reasonable policies. In ways, this enables the users' participation in policy making. Moreover, PCSDs and HDPMS makes policy adherence simpler for the user and the IoT ecosystem less prone to malicious or unintentional privacy and security infringements.

- ***User Security and Privacy:*** The PCSDs along with the HDPMS (refer Sections 5.3.1 and 5.3.2) would shift the onus of adherence to the security and privacy policies of a region, from the users onto the devices. It would also ensure prompt enforcement of highly relevant policies. These factors would result in less incidents of users being victims of security/privacy intrusion, or (intentionally or unintentionally) causing security/privacy intrusions. Moreover, with devices smart enough to act according to the contextual policies, the required level of awareness and participation of users in security/privacy protection would be reduced, resulting in more popular and carefree (yet secure) usage of technologies.

5.4 Example of Utility

The Social Governance would find relevance in every aspect of the modern, connected society. We have already discussed about effective adherence to privacy and security policies in case for devices like the Google Glass and smartphones. Let us try to understand the utility of the proposed framework through another example.

With the increasing popularity of smart cars in recent years and the advent of connected cars, making the automobiles policy compliant would mean avoidance of a lot of unwanted incidents on the roads. Let us think of a residential locality which also has a school. For the welfare of the residents, the locality wants to

have a low speed limit on the vehicles which pass through the neighborhood street during the school hours (8 A.M. to 4 P.M.), and restrict the vehicles driving through the street between 12 A.M. and 6 A.M. from making too much noise. They appeal to the local concerned authority, and the office enforces the policies. When a policy compliant smart car enters the locality, the OS of the car probes for local policies on its running functionalities (running, head lights, horn, music player, etc). The functionality 'running' has an action 'speed limit'. Suppose the time is between 8 A.M. and 4 P.M., and the car is speeding (or trying to speed) over the set limit. When the car requests the policy for this functionality-action pair, the HDPMS will deny permission based on the local policy. Based on the condition for denial received by the OS of the car, it may either slows down the car within the speed limit, or notify the driver. If the driver does not slow down within a stipulated amount of time, then the OS of the car may automatically report the policy infringement to the traffic control department. Similarly, if a smart car passes by the locality in between 12 A.M. and 6 A.M., and is playing music, or honking the horn louder than the set decibel limits, either the volumes are automatically reduced within the the permissible range or the driver is notified.

When the frequency of such policy queries in other localities which do not have location/context specific policies for passing automobiles, exceed a limit set by the local authority, the HDPMS system can suggest the local policy makers about which devices/situation should specific policies be formulated for.

If provisions are made for the lower level policy servers to send their native policies to their parents, many useful information may be deduced. If a region's policy management server learns that considerable number of localities under it are implementing similar vehicular policies, the server can implement algorithms to infer the similarities in the geographic, demographic, and contextual features of the localities enforcing similar policies, and formulate similar policies for all the localities with similar features. Or it may suggest suitable policies to the servers lower in the hierarchy based on the policies imposed in other regions (horizontal servers) with similar geographic, demographic, or contextual features.

Some of the ways in which establishment of the Social Governance Framework would benefit the society are,

- Better administration and less involvement of IoT technologies in law violation.
- Effective formulation and enforcement of IoT related policies.
- Building an intelligent, self-learning system, which adapts itself with the changing activities of the users and with changing technologies.
- Less security, privacy and awareness concerns for the users of smart technologies.

In conclusion, existing policy frameworks are pushing for the efficiency, and secure and safe operation of a very large scale installation that an enterprise is responsible for rolling out. Social Governance considers an even larger installation. But, more importantly, it does not intend in seeking a "best" way to run for the sake of a single entity. It is about seeking a collaborative consensus among all parties so that the system can function.

Chapter 6

Conclusion And Future Work

6.1 Conclusion

The IoT is growing so fast that it would not be foolish to assume that the notion of a "Super-connected World" is not very far from reality now. As the IoT is necessarily an extension of the Internet, most of the security and privacy issues of the Internet would be inherited by the IoT. Moreover, the unique features of the IoT may introduce novel vulnerabilities which would further expand the attack surface [50] of the IoT system. While the solutions and mechanisms for the Internet can definitely be extended to the IoT to solve the known problems, it is crucial to strategically design and deploy the IoT architecture with security and privacy built into it, so as to minimize the scope of introduction of new vulnerabilities. Moreover, through systematic analysis of vulnerabilities of the IoT and through formulation of a detailed threat taxonomy, specialized threat spaces can be created. This would refine threat recognition and safeguarding during the device, application and service design and deployment phases, and detection, isolation and containment of attacks during the operational phase.

Social Governance envisions establishment of a standardized symbiotic framework which would facilitate free flow of information between the key drivers of the networked society. The framework would promote active participation of all the drivers in the activities throughout the IoT services' life-cycle, thus fostering an expeditious, organized, robust and secure development of the IoT system. The framework could be the solution to many of the privacy, trust and reputation re-

lated threats. Moreover, the framework, by virtue of the HDPMS and PCSDs would be able to optimize the security and privacy policy formulation and enforcement, in turn making the future connected society not only technologically secure, but also *socially safe*. Social safety is an issue which is rarely discussed, and is generally considered an implication of technical security. But in fact, a secure IoT system may not be safe for the society. Social Governance would also focus on social safety. Open problems remain in areas like cryptographic mechanisms, network protocols, data and identity management, user privacy, self-management, and trusted architectures [52].

6.2 Future Work

Future works can realize the concept of Social Governance. This thesis does not present the details of the procedures and protocols for the information exchange between the drivers of the networked society. Hence, a detailed design and formalization of these procedures and protocols is a promising direction of work. Moreover, future researches could actually develop a prototype of the HDPMS-PCSDs setup to demonstrate the practical feasibility of the concept of Social Governance.

References

[1] B. Zhang, Z. Zou, and M. Liu, "Evaluation on security system of Internet of Things based on Fuzzy-AHP method," in *International Conference on E-Business and E-Government (ICEE), 2011*, pp. 1–5, IEEE, 2011.

[2] J. Pescatore, "Securing the "Internet of Things" Survey," tech. rep., SANS, Jan. 2014.

[3] D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," tech. rep., Cisco Systems, Inc. (White Paper), Apr. 2011.

[4] "Dealing with the risks and rewards of the Internet of Everything, part 1." http://blog.trendmicro.com/dealing-risks-rewards-internet-everything-part-1/#.U9mAH4BdU3A, July 2014.

[5] C. Clearfield, "Why The FTC Can't Regulate The Internet Of Things." http://www.forbes.com/sites/chrisclearfield/2013/09/18/why-the-ftc-cant-regulate-the-internet-of-things/, Aug. 2014.

[6] C. Clearfield, "Rethinking Security for the Internet of Things." http://blogs.hbr.org/2013/06/rethinking-security-for-the-in/, Aug. 2014.

[7] J. Steinberg, "These Devices May Be Spying On You (Even In Your Own Home)." http://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you-even-in-your-own-home/, Aug. 2014.

[8] "Hackers Reveal Nasty New Car Attacks–With Me Behind The Wheel." http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/, Apr. 2014.

[9] R. Boyle, "Proof-of-Concept CarShark Software Hacks Car Computers, Shutting Down Brakes, Engines, and More." http://www.popsci.com/cars/article/2010-05/researchers-hack-car-computers-shutting-down-brakes-engine-and-more, Aug. 2014.

[10] National Intelligence Council, *Disruptive Civil Technologies: Six Technologies With Potential Impacts on US Interests Out to 2025*. Official US Government Document, Accession Number ADA519715, 2008.

[11] R. H. Weber and R. Weber, "Governance of the Internet of Things," in *Internet of Things*, pp. 69–100, Springer, 2010.

[12] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, *Vision and challenges for realising the Internet of Things*. EUR-OP, 2010.

[13] S. Sarma, D. L. Brock, and K. Ashton, "The networked physical world," *Auto-ID Center White Paper MIT-AUTOID-WH-001*, 2000.

[14] L. Tan and N. Wang, "Future Internet: The Internet of Things," in *3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010*, vol. 5, pp. V5–376, IEEE, 2010.

[15] A. Bassi and G. Horn, "Internet of Things in 2020: A Roadmap for the Future," *European Commission: Information Society and Media*, 2008.

[16] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, *et al.*, "Internet of Things Strategic Research Roadmap," *Internet of Things-Global Technological and Societal Trends*, pp. 9–52, 2011.

[17] O. Garcia-Morchon, S. Kumar, S. Keoh, R. Hummen, and R. Struik, "Security Considerations in the IP-based Internet of Things," *draft-garcia-core-security-06*, 2014.

[18] J. van den Hoven, "Fact sheet- Ethics Subgroup IoT - Version 4.0," tech. rep., Delft University of Technology, Chair Ethics Subgroup IoT Expert Group, 2012.

[19] "ETICA: Ethical Issues of Emerging ICT Applications." http://www.etica-project.eu/, May 2014.

[20] N. Olifer and V. Olifer, *Computer Networks: Principles, Technologies and Protocols for Network Design*. John Wiley & Sons, 2005.

[21] "Google-Blogger." https://www.blogger.com/, Aug. 2014.

[22] "WordPress." https://wordpress.com/, Aug. 2014.

[23] D. Le-Phuoc, A. Polleres, M. Hauswirth, G. Tummarello, and C. Morbidoni, "Rapid prototyping of semantic mash-ups through semantic web pipes," in *Proceedings of the 18th international conference on World wide web*, pp. 581–590, ACM, 2009.

[24] B. Zhang, Z. Zou, and M. Liu, "Evaluation on security system of internet of things based on Fuzzy-AHP method," in *International Conference on E-Business and E-Government (ICEE), 2011*, pp. 1–5, May 2011.

[25] S. Haller, "The Things in the Internet of Things," in *Internet of Things Conference*, 2010.

[26] O. Vermesan and P. Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. River Publishers, 2013.

[27] B. N. Schilit and M. M. Theimer, "Disseminating active map information to mobile hosts," *IEEE Network*, vol. 8, no. 5, pp. 22–32, 1994.

[28] B. Schilit, N. Adams, and R. Want, "Context-aware computing applications," in *First Workshop on Mobile Computing Systems and Applications, 1994. WMCSA 1994.*, pp. 85–90, IEEE, 1994.

[29] A. K. Dey, "Understanding and using context," *Personal and ubiquitous computing*, vol. 5, no. 1, pp. 4–7, 2001.

[30] D. Preuveneers and Y. Berbers, "Internet of things: A context-awareness perspective," *The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems*, pp. 287–307, 2008.

[31] C. Associati, "The Evolution of Internet of Things," tech. rep., Focus, Feb. 2011.

[32] "IoT-I: Internet of Things Initiative." http://www.iot-i.eu/, May 2014.

[33] "50 Sensor Applications for a Smarter World." http://www.libelium.com/50_sensor_applications/, May 2014.

[34] O. Vermesan, P. Friess, G. Woysch, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, M. Eisenhauer, and K. Moessner, "Europes IoT Strategic Research Agenda 2012," *Chapter 2 in The Internet of Things 2012 New Horizons*, 2012.

[35] A. B. Zaslavsky, C. Perera, and D. Georgakopoulos, "Sensing as a Service and Big Data," *CoRR*, vol. abs/1301.0159, 2013.

[36] A. Zaslavsky, "Internet of Things and Ubiquitous Sensing." https://www.computer.org/portal/web/computingnow/archive/september2013, May 2014.

[37] "China Telecom Internet of Things Report," tech. rep., China Telecom, 2011.

[38] M. Covington and R. Carskadden, "Threat implications of the Internet of Things," in *2013 5th International Conference on Cyber Conflict (CyCon)*, pp. 1–12, June 2013.

[39] "Internet of Things." http://www.w3.org/WAI/RD/wiki/Internet_of_Things, Mar. 2014.

[40] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards Survivable Cyber-Physical Systems," *System*, vol. 1, no. a2, p. a3, 2008.

[41] M. Conti, S. K. Das, C. Bisdikian, M. Kumar, L. M. Ni, A. Passarella, G. Roussos, G. Trster, G. Tsudik, and F. Zambonelli, "Looking ahead in pervasive computing: Challenges and opportunities in the era of cyberphysical convergence," *Pervasive and Mobile Computing*, vol. 8, no. 1, pp. 2 – 21, 2012.

[42] Q. He and R. S. Blum, "New hypothesis testing-based rapid change detection for power grid system monitoring," *International Journal of Parallel, Emergent and Distributed Systems*, no. ahead-of-print, pp. 1–25, 2013.

[43] B. K. Samanthula, H. Chun, W. Jiang, and B. M. McMillin, "Secure and threshold-based power usage control in smart grid environments," *International Journal of Parallel, Emergent and Distributed Systems*, no. ahead-of-print, pp. 1–26, 2013.

[44] D. Li, Z. Aung, J. R. Williams, and A. Sanchez, "No peeking: privacy-preserving demand response system in smart grids," *International Journal of Parallel, Emergent and Distributed Systems*, no. ahead-of-print, pp. 1–26, 2013.

[45] A. Greenberg, "Americas Hackable Backbone. Forbes," 2007.

[46] R. Bush and D. Meyer, "Some internet architectural guidelines and philosophy," 2002.

[47] "Making Markets: Smarter Planet." https://www.ibm.com/investor/events/investor0512/presentation/05_Smarter_Planet.pdf, Apr. 2014.

[48] "An Internet of Cows (and Sheeps!)." http://designculturelab.org/2011/07/20/an-internet-of-cows-and-sheeps/, Mar. 2014.

[49] C. M. Medaglia and A. Serbanati, "An Overview of Privacy and Security Issues in the Internet of Things," in *The Internet of Things*, pp. 389–395, Springer, 2010.

[50] P. K. Manadhata and J. M. Wing, "An Attack Surface Metric," *IEEE Transactions on Software Engineering*, vol. 37, no. 3, pp. 371–386, 2011.

[51] "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020." http://www.gartner.com/newsroom/id/2636073, Mar. 2014.

[52] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, pp. 51–58, Sept 2011.

[53] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A Survey on Facilities for Experimental Internet of Things Research," *IEEE Communications Magazine*, vol. 49, pp. 58–67, November 2011.

[54] T. Teixeira, S. Hachem, V. Issarny, and N. Georgantas, "Service Oriented Middleware for the Internet of Things: A Perspective," in *Proceedings of the 4th European Conference on Towards a Service-based Internet*, ServiceWave'11, (Berlin, Heidelberg), pp. 220–229, Springer-Verlag, 2011.

[55] E. De Poorter, I. Moerman, and P. Demeester, "Enabling Direct Connectivity Between Heterogeneous Objects in the Internet of Things Through a Network-Service-Oriented Architecture," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 1, p. 61, 2011.

[56] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security Challenges in the IP-based Internet of Things," *Wirel. Pers. Commun.*, vol. 61, pp. 527–542, Dec. 2011.

[57] M. Brachmann, O. Morchon, S. Keoh, and S. Kumar, "Security Considerations around End-to-End Security in the IP-Based Internet of Things," in *Proceedings of the Workshop on Smart Object Security, in Conjunction with IETF83, Paris, France*, pp. 25–30, 2012.

[58] N. Kushalnagar, G. Montenegro, C. Schumacher, *et al.*, "IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals," *RFC4919, August*, vol. 10, 2007.

[59] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained Application Protocol (CoAP), draft-ietf-core-coap-13," *Orlando: The Internet Engineering Task Force–IETF, Dec*, 2012.

[60] "Oxford Dictionaries Online." http://www.oxforddictionaries.com/, Apr. 2014.

[61] S. Applegate, "The Principle of Maneuver in Cyber Operations," in *2012 4th International Conference on Cyber Conflict (CYCON)*, pp. 1–13, June 2012.

[62] J. Claessens, J. Gessner, H.-J. Hof, and C. Kloukinas, "IoT@Work, WP3 SECURITY: D3.1 THREAT ANALYSIS," tech. rep., IoT@Work, Nov. 2010.

[63] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti, "Secure pebblenets," in *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pp. 156–163, ACM, 2001.

[64] J. E. Boritz, "IS practitioners' views on core concepts of information integrity," *International Journal of Accounting Information Systems*, vol. 6, no. 4, pp. 260 – 279, 2005.

[65] "Information Security: A Closer Look." http://quickbase.intuit.com/articles/information-security-a-closer-look, Apr. 2014.

[66] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Course Technology; 4 edition, 2011.

[67] R. H. Weber, "Accountability in the Internet of Things," *Computer Law & Security Review*, vol. 27, no. 2, pp. 133 – 138, 2011.

[68] D. Morgan, "Web application security SQL injection attacks," *Network Security*, vol. 2006, no. 4, pp. 4 – 5, 2006.

[69] M. J. Handley and E. Rescorla, "Internet denial-of-service considerations," 2006.

[70] T. Bhattasali, R. Chaki, and S. Sanyal, "Article: Sleep Deprivation Attack Detection in Wireless Sensor Network," *International Journal of Computer Applications*, vol. 40, pp. 19–25, February 2012.

[71] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "IPv6 Routing Protocol for Low-Power and Lossy Networks," tech. rep., Internet Engineering Task Force (IETF), Mar. 2012.

[72] S. D. Warren and L. D. Brandeis, "The Right to Privacy," *Harvard Law Review*, vol. 4, pp. 193–220, December 1890.

[73] J. Eloff, M. Eloff, M. Dlamini, and M. Zielinski, "Internet of People, Things and Services - The Convergence of Security, Trust and Privacy," in *3rd CompanionAble Workshop IoPTS, Novotel Brussels - Brussels*, December 2009.

[74] D. E. O'Leary, "Big Data, the 'Internet of Things' and the 'Internet of Signs'," *Intelligent Systems in Accounting, Finance and Management*, vol. 20, no. 1, pp. 53–65, 2013.

[75] "The 'Internet of things' will mean really, really big data." http://www.infoworld.com/d/big-data/the-internet-of-things-will-mean-really-really-big-data-223314, June 2013.

[76] C. Lampe, N. B. Ellison, and C. Steinfield, "Changes in Use and Perception of Facebook," in *Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work*, CSCW '08, (New York, NY, USA), pp. 721–730, ACM, 2008.

[77] J. Wortham, "More Employers Use Social Networks to Check Out Applicants," *The New York Times*, Aug. 2009.

[78] "Privacy and Security." http://msdn.microsoft.com/en-us/library/ms976532.aspx, Apr. 2014.

[79] T. Thornburgh, "Social Engineering: The "Dark Art"," in *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, InfoSecCD '04, (New York, NY, USA), pp. 133–135, ACM, 2004.

[80] "Privacy." http://plato.stanford.edu/entries/privacy/, May 2014.

[81] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing (4th Edition)*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2006.

[82] M. Elkhodr, S. Shahrestani, and H. Cheung in *10th International Conference on ICT and Knowledge Engineering (ICT Knowledge Engineering), 2012.*

[83] L. Zhou, Q. Wen, and H. Zhang, "Preserving Sensor Location Privacy in Internet of Things," in *Fourth International Conference on Computational and Information Sciences (ICCIS), 2012*, pp. 856–859, Aug 2012.

[84] A. C. Sarma and J. Girão, "Identities in the future internet of things," *Wireless Personal Communications*, vol. 49, no. 3, pp. 353–363, 2009.

[85] T. Denning, T. Kohno, and H. M. Levy, "Computer Security and the Modern Home," *Commun. ACM*, vol. 56, pp. 94–103, Jan. 2013.

[86] T. Oluwafemi, T. Kohno, S. Gupta, and S. Patel, "Experimental Security Analyses of Non-Networked Compact Fluorescent Lamps: A Case Study of Home Automation Security," in *Proceedings of the LASER 2013*, (Berkeley, CA), pp. 13–24, USENIX, 2013.

[87] "In the Matter of TRENDnet, Inc.." http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter, Apr. 2014.

[88] "Internet of Things." https://www.youtube.com/watch?v=QaTIt1C5R-M, 2014.

[89] "Cyber criminals hack smart fridge to send out spam," *The Economic Times*, Jan. 2014.

[90] S. Garfinkel, A. Juels, and R. Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions," *IEEE Security Privacy*, vol. 3, pp. 34–43, May 2005.

[91] M. J. Brian Cashell, William D. Jackson and B. Webel, "The Economic Impact of Cyber-Attacks," tech. rep., Government and Finance Division, Apr. 2004.

[92] Z. Ramzan, "Phishing Attacks and Countermeasures," in *Handbook of Information and Communication Security* (P. Stavroulakis and M. Stamp, eds.), pp. 433–448, Springer Berlin Heidelberg, 2010.

[93] A. Council, "Excellence in Travel Information & Marketing," *Scottish Transport Awards 2013*, 2013.

[94] L. Hyvonen, A. Pinto, and J. Troelsen, "Near Field Communication," July 3 2012. US Patent 8,212,735.

[95] P. Agrawal and S. Bhuraria, "Near field communication," *IT Matters*, vol. 67, 2012.

[96] "Public Transport." http://www.aberdeencity.gov.uk/transport_streets/public_transport/put_public_transport_unit.asp, Apr. 2014.

[97] E. Pignotti and P. Edwards, "Trusted Tiny Things: Making the Internet of Things More Transparent to Users," in *Proceedings of the International Workshop on Adaptive Security*, ASPI '13, (New York, NY, USA), pp. 2:1–2:4, ACM, 2013.

[98] "Google Glass May Be Banned In Australia Under New Proposed Privacy Laws." http://au.ibtimes.com/articles/546007/20140401/google-glass-privacy-law-australian-reform-commission.htm#.U1RwDuZdUl8, Apr. 2014.

[99] A. L. R. Commission, "Serious Invasions of Privacy in the Digital Era," tech. rep., Australian Government, Mar. 2014.

[100] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, "IEEE 802.15. 4: a developing standard for low-power low-cost wireless personal area networks," *IEEE Network*, vol. 15, no. 5, pp. 12–19, 2001.

[101] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 522–533, 2007.

[102] P. H. Cole and D. C. Ranasinghe, "Networked RFID systems and lightweight cryptography," *London, UK: Springer. doi*, vol. 10, pp. 978–3, 2008.

[103] B. A. Forouzan, *Cryptography &Amp; Network Security*. New York, NY, USA: McGraw-Hill, Inc., 1 ed., 2008.

[104] J. A. Kraemer, R. H. Levesque, and A. P. Nadkarni, "Key Management for Network Communication," Oct. 20 1998. US Patent 5,825,891.

[105] V. Gupta, M. Millard, S. Fung, Y. Zhu, N. Gura, H. Eberle, and S. Shantz, "Sizzle: A Standards-based End-to-End Security Architecture for the Embedded Internet," in *Third IEEE International Conference on Pervasive Computing and Communications, 2005. PerCom 2005.*, pp. 247–256, March 2005.

[106] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15. 4 networks," *Internet proposed standard RFC*, vol. 4944, 2007.

[107] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol", RFC 4306," 2005.

[108] T. Dierks, "The transport layer security (TLS) protocol version 1.2," 2008.

[109] T. Phelan, "Datagram transport layer security (DTLS) over the datagram congestion control protocol (DCCP)," 2008.

[110] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host Identity Protocol," *RFC5201, April*, 2008.

[111] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin, "Protocol for carrying authentication for network access (PANA)," *http://www.ietf.org/rfc/rfc5191.txt*, 2008.

[112] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, *et al.*, "Extensible Authentication Protocol (EAP)," tech. rep., RFC 3748, June, 2004.

[113] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Symposium on Security and Privacy, 2003. Proceedings. 2003*, pp. 197–213, IEEE, 2003.

[114] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wireless networks*, vol. 8, no. 5, pp. 521–534, 2002.

[115] "ZigBee Alliance." http://www.zigbee.org/, Apr. 2014.

[116] I. Gudymenko, K. Borcea-Pfitzmann, and K. Tietze, "Privacy Implications of the Internet of Things," in *Constructing Ambient Intelligence*, pp. 280–286, Springer, 2012.

[117] P. Schaar, "Privacy by Design," *Identity in the Information Society*, vol. 3, no. 2, pp. 267–274, 2010.

[118] M. Langheinrich, "Privacy by Design Principles of Privacy-Aware Ubiquitous Systems," in *Ubicomp 2001: Ubiquitous Computing* (G. Abowd, B. Brumitt, and S. Shafer, eds.), vol. 2201 of *Lecture Notes in Computer Science*, pp. 273–291, Springer Berlin Heidelberg, 2001.

[119] A. Cavoukian, "Privacy by design," *Report of the Information & Privacy Commissioner Ontario, Canada*, 2012.

[120] M. Langheinrich, "Privacy in ubiquitous computing," *Ubiqutious Computing Fundamentals*, pp. 96–156, 2009.

[121] G. Broenink, J.-H. Hoepman, C. v. Hof, R. Van Kranenburg, D. Smits, and T. Wisman, "The Privacy Coach: Supporting customer privacy in the Internet of Things," *arXiv preprint arXiv:1001.4459*, 2010.

[122] C. Bizer, T. Heath, and T. Berners-Lee, "Linked data-the story so far," *International journal on semantic web and information systems*, vol. 5, no. 3, pp. 1–22, 2009.

[123] Y. L. Simmhan, B. Plale, and D. Gannon, "A survey of data provenance in e-science," *SIGMOD Rec.*, vol. 34, pp. 31–36, Sept. 2005.

[124] K. E. Johnson, A. Kamineni, S. Fuller, D. Olmstead, and K. J. Wernli, "How the provenance of electronic health record data matters for research: A case example using system mapping," *eGEMs (Generating Evidence & Methods to improve patient outcomes)*, vol. 2, no. 1, p. 4, 2014.

[125] O. Hartig, "Provenance information in the web of data.," in *LDOW*, 2009.

[126] L. Moreau, "The Foundations for Provenance on the Web," *Found. Trends Web Sci.*, vol. 2, pp. 99–241, Feb. 2010.

[127] T. El Maliki and J. M. Seigneur, "A Survey of User-centric Identity Management Technologies," in *The International Conference on Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007.*, pp. 12–17, Oct 2007.

[128] I. Friese, "Concepts of Identity within the Internet of Things." https://kantarainitiative.org/confluence/display/IDoT/Concepts+of+Identity+within+the+Internet+of+Things, Aug. 2014.

[129] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010*, pp. 238–243, Oct 2010.

[130] A. F. Gomez-Skarmeta, P. Martinez-Julia, J. Girao, and A. Sarma, "Identity Based Architecture for Secure Communication in Future Internet," in *Proceedings of the 6th ACM Workshop on Digital Identity Management*, DIM '10, (New York, NY, USA), pp. 45–48, ACM, 2010.

[131] C. Chibelushi, A. Eardley, and A. Arabo, "Identity Management in the Internet of Things: the Role of MANETs for Healthcare Applications," *Computer Science and Information Technology*, vol. 1, no. 2, pp. 73–81, 2013.

[132] J. Pan, S. Paul, R. Jain, and M. Bowman, "MILSA: A mobility and multihoming supporting identifier locator split architecture for naming in the next generation Internet," in *IEEE Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008.*, pp. 1–6, IEEE, 2008.

[133] J. Pan, R. Jain, S. Paul, M. Bowman, X. Xu, and S. Chen, "Enhanced MILSA architecture for naming, addressing, routing and security issues in the next generation Internet," in *IEEE International Conference on Communications, 2009. ICC'09.*, pp. 1–6, IEEE, 2009.

[134] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications," in *ACM SIGCOMM Computer Communication Review*, vol. 31, pp. 149–160, ACM, 2001.

[135] L. Cheng, A. Galis, B. Mathieu, K. Jean, R. Ocampo, L. Mamatas, J. Rubio-Loyola, J. Serrat, A. Berl, H. de Meer, *et al.*, "Self-organising Management Overlays for Future Internet Services," in *Modelling Autonomic Communications Environments*, pp. 74–89, Springer, 2008.

[136] T. Li, "Design goals for scalable Internet routing," 2011.

[137] "Designing Advanced Network Interfaces for the Delivery and Administration of Location Independent, Optimised Personal Services (DAIDALOS)." http://www.ist-daidalos.org/, Apr. 2014.

[138] "Secure Widespread Identities for Federated Telecommunications (SWIFT)." http://www.ist-swift.org/, Apr. 2014.

[139] A. Sarma, A. Matos, J. Girão, and R. L. Aguiar, "Virtual identity framework for telecom infrastructures," *Wireless Personal Communications*, vol. 45, no. 4, pp. 521–543, 2008.

[140] "Microsoft Passport: Streamlining Commerce and Communication on the Web." http://www.microsoft.com/en-us/news/features/1999/10-11passport.aspx, Apr. 2014.

[141] "Introducing Windows CardSpace." http://msdn.microsoft.com/en-us/library/aa480189.aspx, Apr. 2014.

[142] "OpenID Specifications." http://msdn.microsoft.com/en-us/library/aa480189.aspx, Apr. 2014.

[143] K. Lampropoulos, D. Diaz-Sanchez, F. Almenares, P. Weik, and S. Denazis, "Introducing a cross federation identity solution for converged network environments," in *Principles, Systems and Applications of IP Telecommunications*, pp. 1–11, ACM, 2010.

[144] J. P. Wang, S. Bin, Y. Yu, and X. X. Niu, "Distributed Trust Management Mechanism for the Internet of Things," *Applied Mechanics and Materials*, vol. 347, pp. 2463–2467, 2013.

[145] H. Li and M. Singhal, "Trust management in distributed systems," *IEEE Computer*, vol. 40, no. 2, pp. 45–53, 2007.

[146] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things," *Computer Science and Information Systems*, vol. 8, no. 4, pp. 1207–1228, 2011.

[147] J. Carbo, J. M. Molina, and J. Davila, "Trust management through fuzzy reputation," *International Journal of Cooperative Information Systems*, vol. 12, no. 01, pp. 135–155, 2003.

[148] P. Barnaghi, W. Wang, C. Henson, and K. Taylor, "Semantics for the Internet of Things: early progress and back to the future," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 8, no. 1, pp. 1–21, 2012.

[149] D. consortium (Eds.), "DiYSE Report on Service Ontologies," *DiYSE deliverable D3.1*, p. 8, 2010.

[150] "Internet of Things - Trends and Challenges in Standardization." http://www.itu.int/en/ITU-T/Workshops-and-Seminars/iot/201402/Pages/default.aspx, May 2014.

[151] J. G. Ruggie, "Reconstituting the global public domainissues, actors, and practices," *European journal of international relations*, vol. 10, no. 4, pp. 499–531, 2004.

[152] "Europian Future Internet Portal." http://www.future-internet.eu/, May 2014.

[153] G. Broenink, J.-H. Hoepman, C. van 't Hof, R. V. Kranenburg, D. Smits, and T. Wisman, "The privacy coach: Supporting customer privacy in the internet of things," *CoRR*, vol. abs/1001.4459, 2010.

[154] J. Case, M. Fedor, M. Schoffstall, and C. Davin, "A simple network management protocol (SNMP)," 1989.

[155] L. Kagal, T. Finin, and A. Joshi, "A policy based approach to security for the semantic web," in *The Semantic Web-ISWC 2003*, pp. 402–418, Springer, 2003.

[156] N. C. Damianou, *A policy framework for management of distributed systems*. PhD thesis, Imperial College, 2002.

[157] E. C. Lupu and M. Sloman, "Towards a role-based framework for distributed systems management," *Journal of Network and Systems Management*, vol. 5, no. 1, pp. 5–30, 1997.

[158] M. Sloman, "Policy driven management for distributed systems," *Journal of network and Systems Management*, vol. 2, no. 4, pp. 333–360, 1994.

[159] P. Mockapetris and K. J. Dunlap, "Development of the Domain Name System," *SIGCOMM Comput. Commun. Rev.*, vol. 18, pp. 123–133, Aug. 1988.

[160] N. Karonis, B. De Supinski, I. Foster, W. Gropp, E. Lusk, and J. Bresnahan, "Exploiting hierarchy in parallel computer networks to optimize collective operation performance," in *14th International Parallel and Distributed Processing Symposium, 2000. IPDPS 2000. Proceedings.*, pp. 377–384, 2000.

[161] L. Jakab, A. Cabellos-Aparicio, F. Coras, D. Saucez, and O. Bonaventure, "LISP-TREE: A DNS Hierarchy to Support the LISP Mapping System," *IEEE Journal on Selected Areas in Communications*, vol. 28, pp. 1332–1343, October 2010.

[162] P. Rodriguez, C. Spanner, and E. Biersack, "Analysis of Web caching architectures: hierarchical and distributed caching," *IEEE/ACM Transactions on Networking*, vol. 9, pp. 404–418, Aug 2001.

[163] F. Maturana and D. Norrie, "Distributed decision-making using the contract net within a mediator architecture," *Decision Support Systems*, vol. 20, no. 1, pp. 53 – 64, 1997. Intelligent Agents as a Basis for Decision Support Systems.

[164] T. L. Saaty, *Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World*. Pittsburgh, Pennsylvania: RWS Publications, 1999.

[165] J. Pan, S. Paul, and R. Jain, "A Survey of the Research on Future Internet Architectures," *IEEE Communications Magazine*, vol. 49, pp. 26–36, July 2011.

[166] B. Sarikaya, Y. Ohba, R. Moskowitz, Z. Cao, and R. Cragie, "Security Bootstrapping Solution for Resource-Constrained Devices," tech. rep., CoRE Internet draft, Jan. 2013.

[167] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the Internet of things," *IEEE Internet Computing*, vol. 14, pp. 44–51, Jan 2010.

[168] J. Ligatti, B. Rickey, and N. Saigal, "LoPSiL: A location-based policy-specification language," in *Security and Privacy in Mobile Information and Communication Systems*, pp. 265–277, Springer, 2009.

[169] D. Plummer, "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48. bit Ethernet address for transmission on Ethernet hardware," 1982.

[170] T. Narten, W. A. Simpson, E. Nordmark, and H. Soliman, "Neighbor discovery for IP version 6 (IPv6)," 2007.

[171] Y. Hassin and D. Peleg, "Distributed Probabilistic Polling and Applications to Proportionate Agreement," in *Automata, Languages and Programming* (J. Wiedermann, P. Emde Boas, and M. Nielsen, eds.), vol. 1644 of *Lecture Notes in Computer Science*, pp. 402–411, Springer Berlin Heidelberg, 1999.

[172] S. Gambs, R. Guerraoui, H. Harkous, F. Huc, and A.-M. Kermarrec, "Scalable and secure polling in dynamic distributed networks," in *IEEE 31st Symposium on Reliable Distributed Systems (SRDS), 2012*, pp. 181–190, IEEE, 2012.

[173] E. Damiani, D. C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante, "A Reputation-based Approach for Choosing Reliable Resources in Peer-to-peer Networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, CCS '02, (New York, NY, USA), pp. 207–216, ACM, 2002.

[174] J. Bray and C. F. Sturman, *Bluetooth 1.1: Connect Without Cables*. pearson Education, 2001.

[175] J. Hendricks and L. van Doorn, "Secure Bootstrap is Not Enough: Shoring Up the Trusted Computing Base," in *Proceedings of the 11th Workshop on ACM SIGOPS European Workshop*, EW 11, (New York, NY, USA), ACM, 2004.

[176] M. L. Katz and C. Shapiro, "On the Licensing of Innovations," *RAND Journal of Economics*, vol. 16, pp. 504–520, Winter 1985.