

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 [212], 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 [200]. Several technologies drive the IoT’s vision. [212] 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 [213]: “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 [47]: “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 [47]: “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) [105].

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 [125]. The underlying infrastructure of virtually represented “things” in an Internet-like structure includes existing and evolving Internet and network developments [10]. Emerging services and applications will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability [10].

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* [172]. 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 [13] or WordPress [31], 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 [47]. 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 feeding of information into the virtual world, and/or associated actions carried out in the physical world based on the information in the virtual world [147]. 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.

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* [231, 232]. The *Application Layer* represents the intelligence for processing the data for achieving desired functionality. The *Network and*

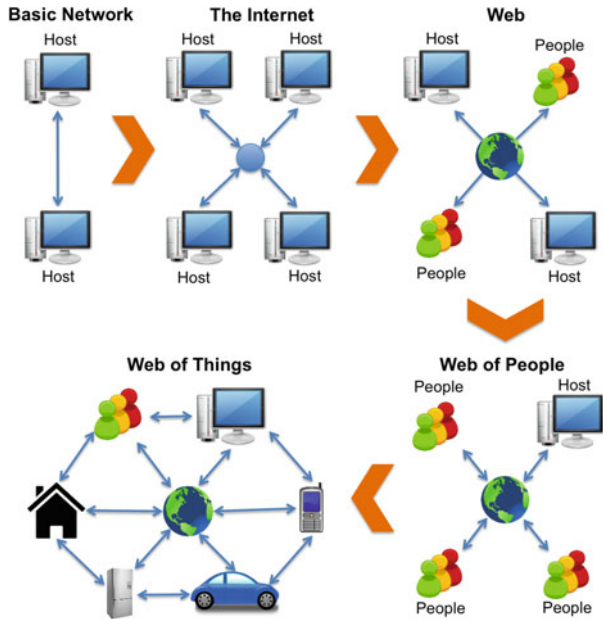


Fig. 2.1 Evolution of the Internet

Evolution of Networks ➡		Internet	Web	Web of People	Web of Things (IoT)
Involved Components ⬇					
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

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 into 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. 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.

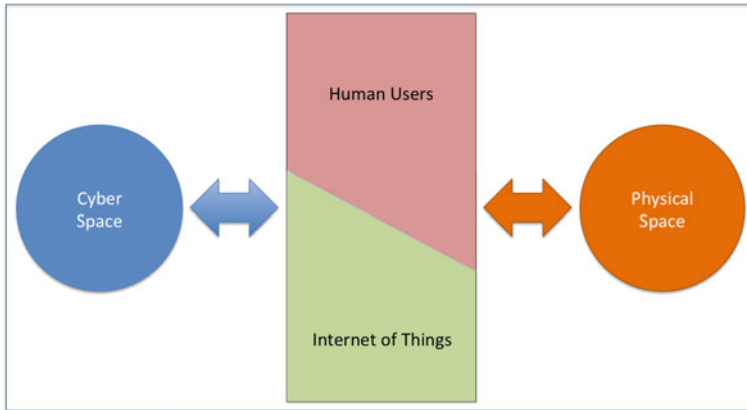


Fig. 2.3 Interaction of cyber-physical spaces through the IoT

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 aspects:

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 realms are converging to create smart environments that makes energy, transport,

cities and many other areas more intelligent [118]. 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 [216]. 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 devices, RFID tags will create highly decentralized common pool of resources interconnected by 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 [216], 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 [202, 203], 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, entertainment and business applications, which are more supportive and suited to the user, would require acquiring, analyzing, and interpreting relevant context information [90] regarding the user [185].

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, [44] 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 any-time 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 network 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) [217] 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*” [216].

Based on inputs from experts, surveys [22] and reports [4], the European Research Cluster on the Internet of Things identified the IoT application domains [217, 218]. [216] 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 people's home.
 - *Ultraviolet Radiation*: Measuring UV sun rays to warn people not to be exposed in certain hours.

Furthermore, [216] 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 towards 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 [299] a Boeing jet generates 10 TB of data per engine every 30 min. A single six-hour flight would

thus generate some 240 TB of data, and there are about 28,537 commercial flights in the USA 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 [228].

- *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 Chap. 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,

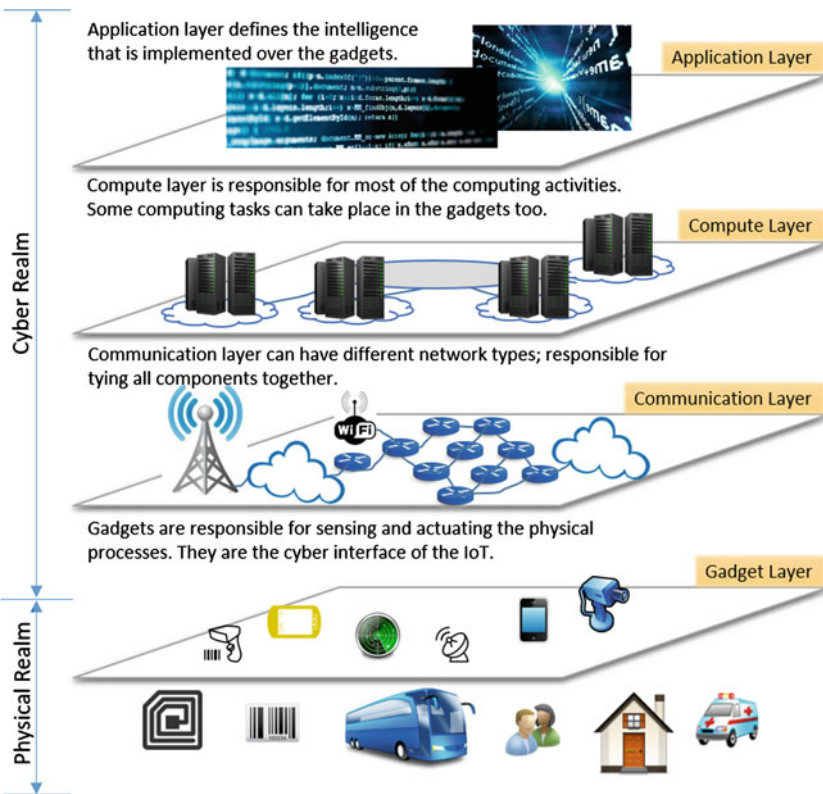


Fig. 2.4 Security problems of IoT s all layers are facing [232]

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 [2] 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.
- *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 reusing the security technology for the Internet. The distinctive characteristics of the IoT needs to be taken into consideration. Appropriately modifying the Internet security architectures or designing a new architecture is

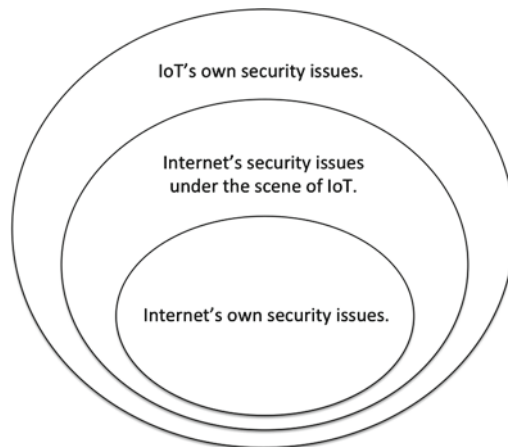


Fig. 2.5 Categories of IoT security issues

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.

Security Challenges and Approaches in Internet of Things

Misra, S.; Maheswaran, M.; Hashmi, S.

2017, VI, 107 p. 27 illus., 23 illus. in color., Softcover

ISBN: 978-3-319-44229-7