Chapter 8
Internet of Things (IOT) and Big Data Analytics

8.1 Introduction

Having surveyed in the last chapter how Big Data Analytics is applied in Social Semantic Web, in this chapter we shall delve into another very important application domain, IOT. We shall examine the interaction between IOT and Big Data Analytics.

In the evolutionary phase of Big Data on the Internet, we have IOT or Internet of Things [1] or Internet of Everything (IOE) as the recent and one of the latest trends and big time thrust of development. IOT may be described as interaction and interoperability domain of divergent areas of activity such as the telecommunications industry, software industry and hardware industry, including device manufacturing industries with a promise of great opportunities for various sectors of industry and commerce.

To provide a formal definition, 'IOT is a seamless connected network of embedded objects/devices, with identifiers, in which M2M (machine to machine) communication without any human intervention is possible using standard and interoperable communication protocols (phones, tablets and PCs are included as part of IOT)'.

Internet of Things (IOT) [2] made a beginning driven by inputs from sensor networks with trillions of sensor devices which are interfaced with smart and intelligent subsystems and in millions of information systems. The Internet of Things (IOT) shall drive unforeseen new vistas of business and customer interests which will require more and more smart and intelligent systems which automatically drive an increasingly large number of opportunities for business in IT/IOT industry and their supply chain companies.

The number of Internet-connected devices exceeding 12 billion had far surpassed the number of human beings of 7 billion and by 2020, the number of Internet-connected devices is expected to reach 30–50 billion globally [3].

C. S. R. Prabhu et al., *Big Data Analytics: Systems, Algorithms, Applications*,
https://doi.org/10.1007/978-981-15-0094-7_8

8.2 Smart Cities and IOT

To provide the better quality of living to the people living in both urban and rural areas, IOT devices, such as sensors, are being deployed in smart cities and smart villages. Globally, smart cities have been proposed, designed and are being implemented in large numbers in all countries.

The applications of IOT in smart city implementation are the following subjects:

1. Smart parking
2. Smart urban lighting
3. Intelligent transport system [4]
4. Smart waste management
5. Tele care
6. Women safety
7. Smart grids
8. Smart city maintenance
9. Digital signage
10. Water management.

Smart home [5] IOT services contribute to enhancing the personal lifestyle by making it easier and more convenient to monitor and operate home appliances such as air conditioners and refrigerators.

While interacting with each other, the IOT devices produce large amounts of data. Processing this data and integrating the IOT devices lead to establishment of a system. The development of smart city system and smart village system is based on IOT and Big Data. Such system development and implementation include data generation and collecting, aggregating, filtration, classification, preprocessing, computing and are finished at decision making.

Sectoral Applications

In addition to smart cities, smart and remotely controlled devices can help solve various problems being faced by the industry in divergent sectors such as agriculture, health, energy, security and disaster management.

This is an opportunity to telecommunication industry on the one hand and system integrators on the other, to enhance their revenues by implementing IOT applications that offer a variety of services that can be offered by this technology. In addition, the IT industry can offer direct services and also analytics-related services or other services independent of IOT.

8.3 Stages of IOT and Stakeholders

8.3.1 Stages of IOT

Four stages of IOT implementation can be identified:

Stage 1: Identify the sensors appropriate for the application.
Stage 2: Develop the application.
Stage 3: Server should receive the sensor data from the application.
Stage 4: Data Analytics software to be used for decision making process.

All the major countries have taken initiative in implementing IOT applications.

8.3.2 Stakeholders

The key stakeholders in IOT implementation are:

1. The citizens
2. The government and
3. The industry.

Each stakeholder has to show commitment to collaborate to produce the results. The participation of stakeholders at each stage or step is essential. Promotional policies are essential for developing answers on the questions: 'What data will give service to the Citizens?' IOT should clearly strategize with a single goal of 'Value Up' and 'Cost Down' models.

8.3.3 Practical Downscaling

In terms of practical realities, the downscaling of IOT from a vision of billions to a reality of thousands of IOT devices in vicinity, loosely connected with each other is to be realized. Also, many of such devices are connected or embedded with mobile devices with P2P, 2G/3G/4G and Wi-Fi connectivity.

Cloud-centric connectivity providing for data collection and the appropriate Big Data Analytics which may be personalized may also be provided. Open ecosystem without vendor lock-in is essential.

8.4 Analytics

Analytics can be performed on either 'Little' data coming from sensor devices or on 'Big' Data from the cloud. Both need to be combined as per the needs.

8.4.1 Analytics from the Edge to Cloud [6]

We cannot push all data to cloud for analytics purposes. In the context of smartphones and potentially intermittent communication, we need to decide if/when to push a subset of 'Big' Data to the phone, if/when to push a subset of the 'Little' data to the cloud and how to make collaborative decisions automatically. Communication and compute capability, data privacy and availability and end-use application inform these choices.

8.4.2 Security and Privacy Issues and Challenges in Internet of Things (IOT)

The primary issues of security and privacy that pose challenges in IOT scenario are the standard issues of (a) privacy of data, (b) confidentiality of data, (c) trust, (d) authentication, (e) integrity, (f) access control, (g) identity protection and (h) privacy of user.

These issues can be addressed in middleware level and also at the other layers of IOT ecosystem such as: (a) at sensor or hardware level, (b) sensor data communication level, (c) content annotation, content discovery level, (d) content modeling, content modeling and content distribution level. The security issues are required to be examined in a wide variety of dimensions such as the types of threats in IOT, protocols and network security, data privacy, management of identity, governance, static trust, dynamic trust, fault tolerance, management of security and privacy. Let us focus on some of the key issues identified above:

(1) To achieve privacy of sensitive details of financial, technical, personal data transmission or exchange (in the IOT ecosystem comprising of radio links, etc.), the data control techniques such as anonymization, encryption, aggregation, integration and synchronization may be deployed to hide the critical information.
(2) Authentication of identity and access control: This comprises steps to prevent intrusion and permit only authentic access to legitimate and authenticated persons into restricted areas. This may be applicable to identification of individuals, vehicles, measurement of humidity and temperature tracking of products, surveillance in sensitive areas.

(3) Trust: Trust comprises transparency and reliable guarantee of security between any two intelligent beings—persons or technological objects. Trust will be leading to a global system of reliable system of information exchange and communication between specific source and specific destination. Trust will depend upon (a) the ability of self-protection despite hostile environment and (b) the verifiability of trustworthiness of an object or node by interrogating it.
(4) Reliability: In any process, the reliability comprises of reliable information collected and the results reported being reliable. This implies that all the steps involved in the process such as sensing, sensing devices, metrology, calibration, processing of signal or data, diagnosing and diagnostics finding out exceptions anomalies, support and maintenance, etc. To insure reliability, automatic, feedback control systems are also required to be established.
(5) How to insure privacy in IOT systems? In IOT application systems existing pervasively, sensitive or confidential data may be stored in a distributed way. Hence, we have to set up adequate controls in managing and disclosing data to third parties according to the respective levels sensitivity. Data usage at processing is done at various levels such as collection transmission and storage of data. In each stage, the appropriate technologies have to be adopted and mechanisms are required to be set up to insure and guarantee data confidentiality, data integrity and data security. Possible methodologies and techniques that can be adopted for these purposes can include: anonymization, ciphers (block and stream), hashing functions, random number generator functions and public key (lightweight) infrastructure.
Privacy in access concerns itself with the manner in which people can access the private and personal information. We need to implement effective policies to insure access privacy.

8.5 Access

We need to insure that we bring the network close to the sensors. The extensive proliferation of tens and hundreds of thousands of sensors will lead to constraints in power and communication bandwidth. Instead of relying on possible large-scale deployment of custom sensor networks, it may be of greater value to piggyback on the existing standards. Peer-to-Peer data may be utilized for last-mile connectivity purposes. We can also integrate highly functional gateways and clouds. Asymmetric architecture may be preferable. The penetration of technology has not been uniform across different countries or even across different regions in the same country, reflecting the inequalities and disparities in infrastructure, access, cost, telecom networks, services, policies, etc. Therefore, affordable sensor devices, affordable networking cost and affordable analytics solutions are to be offered accordingly.

8.6 Cost Reduction

Reuse of deployed infrastructure shall be the inevitable requirement for the successful implementation of IOT. Reusable devices and sensors to be deployed for novel usage ways are preferable in developing or poor countries as the model adopted in advanced nations with advanced infrastructure will not give relevant or cost-effective solutions for the developing or poor countries.

8.7 Opportunities and Business Model

The data that flows in IOT devices and networks shall open up endless and immense opportunities for analytics. The effective interplay between the technology of sensor devices, telecommunication infrastructure and the data flowing through them results in new business models.

Technology model will fail or succeed based on the business models that generate revenues. For Google on Internet, the boom of revenues comes from advertisements using personal data of Google users in return for free information search and retrieval services to end user. With Internet of Things, the information captured will be large, minutely microscopic and fast. Its use, reuse sharing and payment for all these activities are important. Data brokering services can be offered where open data can be utilized for sharing with businesses. This may produce rewards such as greater common good, in addition to revenue that encourages open data sharing by users with businesses in return for clear rewards, be they monitory, peer recognition or the greater good of open data policies.

8.8 Content and Semantics

Being human-centric, content and semantics form the core of data for decision making. Content-based mining and analytics become more meaningful and relevant to the content. Therefore, there has to be a mechanism to capture semantics which can describe system behavior and social behavior.

Sometimes, it is possible that intelligent agents or software agents may replace human users and therefore may become aware of personal information. For example, we have Siri and Cortana which are software agents. They will interact with other agents of service provider, utility companies, and vendor companies.

8.9 Data-Based Business Models Coming Out of IOT

Semantic content can extend the data content in M2M data interchange. Business models based on data will be evolving out. The new vistas of technology and applications that spring out of Internet of Things are characterized by low power, cheaper devices, more computation based on robust connectivity. This technology provides an opportunity of a window to look at our life and environment at microscopic level of detail, as almost everything can be monitored.

IOT business models can be either horizontal or vertical which can be integrated with the supply chain which can become a value proposition for the end user. Such value proposition span is divergent and large in number with multitude of user requirements or aspirations to be fulfilled.

The first step is to develop cost-effective sensors and actuators which make low cost and microlevel observations. The next step is to build a business model which can perform collection, storage, brokering and curation of data coming out. The third business model will be targeting at the analytics portfolio on the data. End-to-end system integration is the fourth business model.

To summarize, the development of IOT-based business models will require concerted efforts to support the modularization of the architecture, to provide access to capabilities through service-based models for solving real customer problems.

8.10 Future of IOT

8.10.1 Technology Drivers

The future of technology drivers includes low cost and accurate sensor and actuator development along with their networking technology along with computer and memory capabilities. Therefore, we can state that understanding this technology of IOT comes out of understanding of devices, their networking and their computing profiles. The devices and sensors are getting miniaturized continuously and their costs are going down too. The ‘Smart Dust’ technology pushed by the defense in the 90s was based on devices using MEMS and electronic textiles and fabrics or wearable computers which are all drivers for IOT-based devices and sensors.

Smart fabrics and their commercial applications in sports or medicine have become conference topics.

8.10.2 Future Possibilities

By 2020, it is expected that most hitherto manual processes could be replaced with automated processes and products and supply chains could have been embedded

with sensor and active devices. Wearable devices or clothes integrated with devices could help in sports and art (dance) training, as also for patient monitoring in medical settings.

8.10.3 Challenges and Concerns

What about privacy concerns in IOT-based sensor networks? While it may be a good idea to have the sunglasses to recognize a man in a room, will it be correct to monitor the self through a cloud-based monitoring application? Numerous commercial opportunities spring up for many new initiatives and application ideas but the questions of ethics and security and privacy concerns also come to the fore. IOT has innumerable and endless industrial and commercial applications: transportations and truck fleet tracking, courier and mail tracking, environmental sensing and monitoring that engage special devices and sensors integrated into smartphones.

In sports, balls and players can be attached with sensors to obtain better accuracy of goal making. Tracking and locating goods and packages in airports, in warehouses and during transport. Wandering robots with sensors can reduce the stocking quantities in warehouses. Tracking temperatures in data center, monitoring insects, bees, migratory birds, gesture recognition, video games, virtual reality (VR), etc. are possible applications. Urban and rural consumer applications such as smart home, smart farms and smart dairy, where parameters such as temperature, moisture, etc. will be monitored online to enhance feedback-based efficient power or water usage are possible. In Europe, South Korea and USA such applications including smart grids, smart cities and smart villages, all use IOT devices and sensors for monitoring and feedback-based action steps. Oil and gas industry had already deployed such devices for long time.

Applications which do not get affected by privacy concerns can be: monitoring traffic, load on bridges, smart aeroplane wings that adjust according to airflow currents and temperatures, etc.

IOT can improve quality of life of citizens and tourists when compared with manual city guidance centers, indicating best routes, guided tours, car-sharing automation, automated self-driving car, wildlife applications as animal monitoring, fish monitoring, bird monitoring are all possible.

The global scope of IOT with sensors in all kinds of different settings provides opportunities to facilitate our daily lives, saving environment, better monitoring and implement law and order (police applications). The list is endless.

Critical factors are the ability to embed sensors and devices in important and relevant locations to monitor all kinds of phenomena and connect them to networks to monitor the data being collected. What determines investments in IOT? 'Microservices' for citizens, tourists, sportspersons, industrial houses, transportation systems, police and security requirements, etc. all provide revenues. Legal and government hurdles, if any, are required to be cleared before implementation and roll out.

8.11 Big Data Analytics and IOT

The significant and substantial increase in the connected devices that are going to happen in Internet of Things (IOT) will lead to an exponential surge in the size of data that an enterprise is expected to manage, analyze and act upon. Therefore, IOT becomes a natural partner match for Big Data simply because it provides the requisite data volumes for Big Data Analytics.

As Howard Baldwin says 'we will have data spewing from all directions – from appliances, from machinery, from train tracks, from shipping containers, from power stations etc.'. All this real-time data needs to be handled, analyzed to sense actionable signals.

IOT is still in its infancy. Soon, the data will start flowing from the sensors and devices. The actionable insights can be identifying purchasing habits of customers or efficiency of machine performance. For example, LexisNexis has open-source HPCC Big Data platform, a solution for data integration, processing and delivery of the results by integrating, machine learning and BI integration.

8.11.1 Infrastructure for Integration of Big Data with IOT

The integration of Big Data with IOT is dependent on the infrastructure environment. This includes storage and cloud infrastructure. Many organizations are attempting to move to PaaS (platform as a service) cloud for hosting and analyzing the huge IOT data since maintaining own storage for this purpose will be very expensive. PaaS cloud will be expected to provide scalability, flexibility compliance and effective sophisticated architecture to store cloud data arriving from IOT devices. If the data is sensitive, then private cloud architecture can be deployed. Otherwise, public cloud services such as AWS (Amazon) or Azure (Microsoft) can be deployed. Many cloud services provide and offer their own IOT platform for implementing IOT Applications.

8.12 Fog Computing

Data is continuously generated by IOT devices. Such data has characteristics of Big Data such as volume, variety, velocity and veracity. Latency becomes a critical requirement in IOT applications which are real time in nature, as they expect real-time response. Cloud computing cannot deliver real-time response, as latency will be very large and significant. Hence, a new concept called 'Fog Computing' has come up of late. Fog server is located near the edge (as a kind of extension of the cloud to the edge). Analyzing IOT data close to the collection point minimizes latency. It

offloads network traffic from the core network and also keeps sensitive data inside the network with at most security.

Fog applications include locking a door, changing equipment settings, applying the brakes on a train, zooming a video camera, opening a valve in response to a pressure reading, creating a bar chart or sending an alert to a technician to make a preventive repair.

Fog computing is mainly useful when the IOT devices are placed globally, data is collected from extreme edges like vehicles, ships, factory floors, roadways, railways, etc. and requirement of data analysis at the same time as data collected.

8.12.1 Fog Data Analytics

I. **Introduction**

Analytics near the edge itself will be possible if we deploy Fog server near the edge and perform analytics in the Fog server itself. This will prevent the transmission of data from the edge to the cloud and therefore avoid the network latency delays in the application execution at the edge.

II. **Fog Computing Environment and Data Analytics**

Fog computing is a new technology paradigm to reduce the complexity, scale and size of the data actually going up to the cloud. Preprocessing of raw data coming out of the sensors and IOT devices is essential and it is an efficient way to reduce the load of the big data on the cloud.

The Fog server, located very near to the edge devices, offers the possibility of preprocessing and even completing local analytics, to take fast decisions for the real-time local edge requirements. Only, the aggregate or summary data, small in size, needs to be sent to the cloud. This will lead to the benefits that accrue from Fog computing that include local, fast processing, storage for geo deductible and latency-sensitive applications, drastically reduced communication overheads over the network and the Internet, thereby having a substantially reduced volume and velocity of data that will be required to be sent to the cloud.

Applications such as augmented reality, interactive gaming and event monitoring require data stream processing, a processing scenario in contrast with a ready data bank, assumed to exist in conventional Big Data application ecosystems.

III. **Stream Data Processing**

Stream data is abundant, in RFID applications, weblogs, telecom call records, security monitoring, network monitoring, stock exchange data, traffic and credit card transactions and so on. It is characterized by high speed, transient and continuous nature of the data.

IV. Stream Data Analytics and Fog Computing

Stream data analytics in Fog servers can be achieved by deploying products like tensor flow and even in mobile edge devices ('Mobile Tensor flow'). In spite of such implementations, the open unsolved challenges do exist—how to perform load balancing among multiple Fog servers and edge devices, without affecting the performance? While we have APIs for Fog streaming in IoT and stream processing platforms like Kafka, APIs for differential equations and control error estimations for Fog-based real-time applications are yet to come up.

V. Different Approaches in Fog Analytics

In the following sections, we present a survey of the different approaches for Fog Analytics.

A. 'Smart Data'

As a complete capsule of structured IoT data, its metadata and its VM, 'Smart Data' is a product available for Fog Analytics.

B. Fog Engine

Fog Engine, a product, provides data analytics on premise. It enables processing of data in cloud as well as IoT devices in a distributed manner. One unit of Fog Engine can collaborate with another. Data can be offloaded into the cloud periodically. Several scenarios can be identified for Fog Engine deployment, depending on multiple receivers, multiple or single analyzers, multiple or single transmitters. The Fog Engine deployment can partially undertake the burden of network backbone and data analytics at utilities side and reduce the dependence on the cloud. While computations are done locally, only a fraction of the data that is cleaned and analyzed by the Fog Engine is transferred to the cloud, thus drastically reducing the volume of data transferred over the network, resulting in substantially reduced network congestion and delay due to latency.

C. Other Products

Other products in Fog Analytics include Microsoft Azure Stack and also CardioLog Analytics by Intlock which offers on-premise data analytics. Oracle delivers Oracle Infrastructure-as-a-Service (IaaS) on-premise with capacity on demand that enables customers to deploy systems based on Oracle in their own data centers. IBM's Digital Analytics on-premise is the core Web Analytics software component of its Digital Analytics Accelerator solution.

D. Parstream

CISCO's Parstream is capable of offering continuous real-time data analytics functionality. It can be deployed on standard CPUs and GPUs. Parstream is well integrated

with many platforms such as R Language. It can analyze large streams of data with time series analysis for historical analysis purposes. Alerts and actions are used and raised to monitor data streams, create user-friendly procedures that generate alerts, send notifications and execute actions; derives models and hypotheses from huge amounts of data by applying statistical function and analytical models, using advanced analytics.

VI. **Comparison**

All the above products have their own respective strengths and weaknesses. Although all of them offer on-premise data analytics services, they lack in providing a holistic approach based on the Fog concept which is the intermediate layer between the edge and the cloud.

VII. **Cloud Solutions for The Edge Analytics**

Solutions by cloud services providers (CSPs) such as Amazon are also available—Amazon's AWA IOT offers implementing data collection through HTTP, Web sockets, MQTT and integrates with REST APIs with device gateway in cloud. Amazon QuickSight is available for machine learning purposes.

Microsoft offers Azure IOT Hub using HTTP, AMQP, MQTT and also custom protocols for data collection; offers REST APIs integration; offers stream analytics and machine learning uses Azure IOT gateway (in-premise gateway).

IBM offers IBM Watson IOT using HTTP and MQTT for data collection, integration with REST and real-time APIs. Data analytics is offered through IBM's Bluemix Data Analytics platform.

Google offers Google IOT uses HTTP only for data collection, integrates with REST APIs and RPC. Analytics is offered through cloud data flow, Big Query Datalab and Dataproc and uses general gateway (on-premise) to cloud.

Alibaba offers Alicloud IOT, uses HTTP, integrates with REST APIs, uses own analytics solution, Max Compute and uses cloud gateway to the cloud.

In this section, a survey of the approach, techniques and products for Fog analytics is presented.

8.12.2 Fog Security and Privacy

Provisioning security and privacy in Fog computing is quite different from provisioning the same in the cloud. Wireless carriers who have control of home gateway or cellular base stations may build Fog with their existing infrastructure. Cloud service providers who want to expand the cloud up to the edge also may build the Fog infrastructure.

Authentication
The main security issue is authentication at various levels of fog nodes. Traditional PKI-based authentication is not scalable. Near-Field Coins (NFC) can be used effectively in Fog computing to simplify authentication procedures. Biometrics-based authentication (such as the Aadhar card in India) can also be effectively used in Fog computing ecosystem. Authentication becomes important at various levels of gateways or at the level of device itself. Each device such as a meter in smart grids or such as an i-pad in any Fog environment should have any authentication-biometric-based authentication or otherwise, to prevent misuse, manipulation or impersonation. For example, smart meters can encrypt the data and send to the Fog devices such as home area network (HAN) where the data can be decrypted, the results are aggregated and then pass them forward to the cloud, for example.

Privacy Issues
Privacy issues pertaining to the devices which device was used, when, for what purpose, etc. are required to be analyzed. Encryption can be used to provide encrypted result which cannot be decrypted, by the individual devices.

Man in the Middle Attack
The Fog is vulnerable and the man in the middle is an example of this vulnerability. In this situation, the gateway serving as the Fog device may be compromised and replaced with fake or malicious access paths which provide deceptive SSIDs as public, legitimate ones. Thereby, the attacker can take control of the gateways and thus the private communication will be hijacked. Man in the middle attack in Fog computing can be very stealthy. It is very difficult to protect the Fog devices from it.

8.13 Research Trends

The current Big Data tools such as Hadoop are not suitable for IOT, as they do not offer online or real-time analytics for IOT purposes and applications [6]. Also, the amount of IOT data is too huge to be processed by such tools, in real time. One alternative possibility is to keep track of only the interesting data coming out of IOT devices. For this purpose, approaches such as principle component analysis (PCA), pattern reduction, dimensionality reduction, feature selection and distributed computing methods are identified [6].

Another important direction is to provide a common platform of analytics as a cloud service, instead of providing application-specific analytics software. It is proposed [7] to offer time series analytics as service or TSaaS, using time series data analytics to perform pattern mining on large sensor data.

8.14 Conclusion

IOT is here to stay, driven by device and sensor technology advances, the opportunities created by billions of smartphones which can be supplemented by IOT devices and sensors, Internet connectivity through mobile networks, resulting in millions of applications in cost reduction through automation, reduced loses or wastages and shorter duration in supply chain processes in all aspects of human life and industrial sectors. In this chapter, we have also seen how the techniques of Big Data Analytics become essential analyzing the data originating from IOT devices. We have also seen how Fog computing becomes essential; in addition to the cloud services being available, we have examined various products of Fog analytics. We have also probed into the security and privacy issues in Fog computing. Finally, we attempted to see how future IOT will shape with new developments such as wearable devices and 'Smart Dust' are coming up.

8.15 Review Questions

1. How the IOT phenomenon is going to impact the Society?
2. How IOT is essential for smart cities?
3. What are the stages in IOT implementation?
4. Explain Analytics from the edge to the cloud.
5. What is the data-based business model coming out of IOT?
6. What is the future of IOT? What are its technology drivers?
7. What are the challenges and concerns for the future of IOT?
8. What are the dynamics of linkage between IOT and Big Data Analytics?
9. What is the infrastructure requirement for integrating IOT with Big Data?
10. Explain Fog computing, its role and its importance for future.
11. What are the research trends in integrating IOT and Big Data?
12. What is Fog computing? Explain its characteristics and benefits.
13. Explain Fog analytics and its products with comparison.
14. Explain Fog security and challenges.
15. Explain Fog privacy and challenges.

References

1. J.R. Frederich, F.W. Samuel, D. Maithaias, Introduction to internet of things and big data analytics, in Mini Track, 2015 48th Hawaii International Conference on System Science
2. A. Al Faquha, M. Guizani, M. Mohammedi, M. Aledhari, M. Ayyash, Internet of things: a survey on enabling technologies, protocols and applications. IEEE Commun. Surv. Tutor. **17**(4) (2015)
3. J. Gantz, D. Revisel, The digital universe in 2020: big data, bigger digital shadows and biggest growth in the far east, in *IDC, iView: IDC Analyze the Future*, vol. 2007, pp. 1–16, Dec 2012

4. http://www.intel.in/contain/lan/www/program/embedded/internet-of-things/blueprints/IOT-building-intelligent-transportsystem
5. N. Komninos, E. Phillipon, A. Pilsillides, Survey in smart grids and home security: issues, challenges and counter measures. IEEE Commun. Surv. **16**(4), 1933–1954 (2014)
6. C. Tsai, C. Lai, M. Chiang, L.T. Yong, Data mining for IOT: a survey, 1st part. IEEE Commun. Surv. **16**(1), 77–97 (2014)
7. X. Xu, S. Huang, Y. Chen, K. Browny, I. Halilovicy, W. Lu, TSAaaS: time services analytics as a service on IOT, in *Proceedings of IEEE ICWS*, pp. 249–256 (2014)