United Nations ECE/TRADE/C/CEFACT/2022/11

Economic and Social Council

Distr.: General
21 July 2022

Original: English

Economic Commission for Europe

Executive Committee

Centre for Trade Facilitation and Electronic Business

Twenty-eighth session
Geneva, 10-11 (am) October 2022
Item 5 (d) of the provisional agenda
Recommendations and standards:
Implementation support material

Report of the eDATA Management Domain on the Internet of Things in Trade Facilitation: the Internet of Things in Supply Chains and Government Services

Submitted by the Bureau

Summary

The internet of things (IoT), and the data it provides, is becoming an integral part of business and supply chain management, and thus an essential tool in trade. To help trade participants better understand both how IoT systems work and how they can be used to support trade facilitation and government infrastructure management, UN/CEFACT has developed this paper on *IoT in Trade Facilitation: IoT in Supply Chains and Government Services,* which looks at how IoT can be specifically used to support trade and some of the legal challenges faced by IoT system implementors.

Document ECE/TRADE/C/CEFACT/2022/11 is submitted to the twenty-eighth session by the Bureau for noting.

I. Introduction

1. The internet of things (IoT) is no longer a term used exclusively by technical experts. The IoT is becoming an integral part of business and supply chain management, providing data that supports inventory management, equipment maintenance, building management, insurance claims, and the tracking and tracing of a wide variety of assets. Therefore, it has also become an essential tool in trade.

2. The IoT helps people and businesses to be and act smarter. The increasing use and utility of IoT ecosystems is reflected in worldwide annual spending on IoT, which reached over $742 billion in 2020 and is expected to reach over 1 trillion dollars by 2023[1]. The vast majority of that expenditure is by businesses looking to improve operational efficiency and find new revenue opportunities.

3. Trade facilitation is “the simplification, standardization and harmonization of procedures and associated information flows required to move goods from seller to buyer and to make payments”[2]. IoT ecosystems can support trade facilitation by providing data that can be used for simplified procedures. For example, status and location data can be used to reduce the need for inspections and manual verification; it can also be used to support certificates of origin (or might even replace them some day). IoT location and environmental data can be used to simplify insurance claims for everything ranging from late delivery to goods damaged by the environment (temperature, humidity, excess motion, etc.) and they can also be used to support reconciliation in goods accounting (e.g. reconciliation between purchase orders and deliveries), including for letter-of-credit payments.

4. To help trade participants better understand both how IoT systems work and how they can be used to support trade facilitation and government infrastructure management, the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) has developed the following papers:

- *IoT in Trade Facilitation: IoT in Supply Chains and Government Services,* which looks at how IoT can be specifically used to support trade. It also looks at some of the legal challenges faced by IoT system implementors in the trade sector (this publication, part one)
- *IoT in Trade Facilitation: Guide to IoT Technology, Communications and Connectivity*[3], which provides an overview of the technologies used in IoT for trade-related applications—the objective being to provide explanations that are accessible to those who are familiar, as managers, with information technology but who may have little or no experience with IoT (part two of this publication)
- *White Paper on IoT Standards in Trade Facilitation*[4], which looks at the need for new standards to support IoT use in trade

[1] Statista, “Prognosis of worldwide spending on the Internet of Things (IoT) from 2018 to 2023”, 28 June 2022. Available at https://www.statista.com/statistics/668996/worldwide-expenditures-for-the-internet-of-things/ (accessed on 26-01-2021).

[2] The Trade Facilitation Implementation Guide is available at https://tfig.unece.org/details.html.

[3] UN/CEFACT, "Report of the eDATA Management Domain on the Internet of Things in Trade Facilitation: Guide to Internet of Things Technology, Communications and Connectivity" (ECE/TRADE/C/CEFACT/2022/12), 2022.

[4] UN/CEFACT, " Report of eDATA Management Domain on Internet of Things Standards for Trade Facilitation " (ECE/TRADE/C/CEFACT/2022/13), 2022.

- *Trade Facilitation White paper on Smart Containers*[5] which looks in depth at the implementation of IoT in the transport sector

5. Trade facilitation requires the exchange of data between different parties and the usefulness of IoT data for facilitation is dramatically reduced when different definitions and formats are used for data, since this results in a burdensome network of data translation needs. Therefore, in order to realize the potential of IoT to support trade facilitation, the standardization of IoT data is needed.

6. UN/CEFACT can provide solutions to this problem through its Core Components Library (CCL), which provides data definitions and code lists. The challenge remains, however, to make the existence of the CCL known to IoT system developers, with easy-to-access information about its use, and to ensure that the data which is needed can be found in the CCL. The UN/CEFACT smart container project has made important steps toward ensuring that the required data is available, but more work is needed to ensure that IoT data used in other areas, such as inventory management, accounting, and finance, are fully reflected.

7. For a more in-depth discussion of standards and the potential need for new standards to support the use of IoT in trade facilitation please refer to the UN/CEFACT Report of the eDATA Management Domain on Internet of Things Standards for Trade Facilitation referenced above.

II. Internet of things in trade: supply chains and governments services

A. Internet of things and supply chains

8. Today, supply chains play a vital role in sustainable economic growth in every industry and region. At the same time, rapid globalization and the expanding geographic reach of supply chains has resulted in ever-increasing complexity, and modern supply chains face numerous challenges such as the following:

- Coordinating across various geographically disbursed and often disconnected supply chain actors (producers, brokers, transporters, processors, retailers, wholesalers and consumers);
- Reacting to unexpected changes in demand and supply chain configurations such as those created by the COVID-19 pandemic;
- Responding to demands for fast, last mile delivery, accurate delivery times and direct-to-consumer fulfilment (with its direct impact on customer relationships);
- Handling manual and difficult data reconciliation procedures;
- Dealing with a lack of end-to-end supply chain transparency, product traceability and record maintenance, coupled with a need for in-depth, end-to-end supply chain inventory visibility (with instant data access and data security);
- Handling stock-management issues (back orders, recording stolen, damaged or lost stock, maintaining minimum stock levels, etc); and

[5] UN/CEFACT, "Trade Facilitation White Paper on Smart Containers: Real-time Smart Container Data for Supply Chain Excellence" (ECE/TRADE/446), 2020. Available at https://unece.org/fileadmin/DAM/trade/Publications/ECE_TRADE_446E_SmartContainers.pdf

- Dealing with the unexpected costs of unplanned logistic movements and the unpredictability of freight transportation.

9. When combined with other technologies, IoT can address many of these challenges. Indeed, the majority of IoT expenditures are undertaken by businesses to improve operational efficiency and to find new revenue opportunities.

10. In the above-mentioned UN/CEFACT White paper on Smart Containers[6], the use cases for IoT in multimodal transport have been described in great detail; so that information, while important for supply chains, will not be repeated here.

1. How could supply chains benefit from adopting IoT?

11. The internet of things is changing the way we look at tracking products and how we monitor the environments in which they are produced along the supply chain. Some of these new approaches, and how they can help address the above challenges, are described below.

Location management systems

12. In the logistics sector, IoT can be integrated into smart location management systems. These systems call for the incorporation of IoT devices into vehicles and, when appropriate, logistics packages and containers, in order to support systems that track driver activities, vehicle location and delivery status. Once goods are delivered or arrive at a specified location, a manager can be automatically notified. The resulting real-time data is an invaluable asset in delivery planning and in the compilation and viewing of schedules used to improve location management and streamline business processes. This type of application will become significantly more useful with the widespread adoption of the electronic version of consignment notes, which are at the heart of all transport contracts.

Improved inventory management

13. Inventory management and warehousing are among the most important parts of supply chain ecosystems. Inventory systems are designed to help supervisors and business owners keep track of the products they have on hand, but there's only so much these systems can do when they rely on manual input and manual hand counts to update inventory numbers.

14. The use of small, inexpensive sensors can allow companies to easily track inventory items, monitor their status and position and create smart warehouse systems. Such systems can prevent losses and ensure the safe storage of goods, as well as efficiently locate needed items.

Improved supply chain transparency and management

15. Consumers are making more environmentally friendly choices and want to know where their products are coming from. One Nielsen poll of 30,000 consumers found that 66 per cent of shoppers were willing to pay more for a product if the company was committed to environmental change and maintained a transparent supply chain[7].

16. In addition, supply chain transparency has more benefits than just attracting eco-conscious customers; it can also help prevent disastrous supply chain disruptions by highlighting small problems before they become big. Therefore, both companies and their

[6] ECE/TRADE/446

[7] Curtain, Melanie, "73 Percent of Millennials Are Willing to Spend More Money on this 1 type of Product", Inc.com, 30 March 2018. Available at https://www.inc.com/melanie-curtin/73-percent-of-millennials-are-willing-to-spend-more-money-on-this-1-type-of-product.html (accessed 17 July 2022).

customers want the ability to trace a product’s life cycle—from the origin of the goods all the way to their delivery into the customer’s hands.

17. Transparency requires extensive data collection which can be supported through the use of IoT ecosystems. Blockchain and IoT technologies, when used together, can help fulfil the need for supply chain traceability, transparency and data security. The use of radio frequency identification (RFID) tags and IoT readers and sensors can allow for the monitoring of things such as product temperature and humidity, vehicle location and stages in the transportation process. Using a blockchain-based system, every product can be given a digital ID, and information collected about that ID by IoT devices can be securely recorded. The result is information which is secure and available for access by authorized users throughout the product’s life cycle.

Real-time tracking of transport conditions (i.e. cold-chain transport)

18. Cold-chain transport is an integral part of the supply chain for food, beverages, pharmaceuticals and chemicals. Globally, between 14 and 30 per cent of perishable cargo is destroyed during transit and storage, mainly due to unregulated temperatures and poor storage conditions[8]. With extremely sensitive products, like some pharmaceuticals, a temperature variation of fewer than two degrees could ruin an entire shipment. IoT devices can be used to constantly monitor real-time temperatures during transport and storage and to send alerts if there are any unacceptable variations in a shipment’s environment, including the interior temperature of trucks or warehouses. Depending upon the product, IoT sensors can also be used to measure other potentially damaging environmental factors such as physical shocks, humidity, air pressure, etc.

Advanced and predictive analytics

19. The unprecedented volume of data that IoT systems can generate provides companies with the opportunity to gain insights into operations using advanced analytics. Real-time performance monitoring creates opportunities for predictive analytics. Predictive analytics is helping companies and corporations create more effective operational strategies and improve decision-making, risk management and much more. One important example of advanced analytics is predictive maintenance.

20. Most warehouses and supply chains have established maintenance schedules, taking equipment offline on a strict schedule to inspect and repair it in order to minimize damage and downtime from unexpected equipment failures. However, a study by the ARC Advisory Group found that only 18 per cent of equipment failures were due to age. The rest happened randomly, so supply chain owners need new strategies to reduce this remaining, 82 per cent of equipment failures[9].

21. Combined with predictive analytics, IoT can address this issue by monitoring the health of each piece of equipment, feeding that data back into management software, and then alerting supervisors and maintenance teams when something needs to be taken offline and repaired, thus preventing costly schedule disruptions, downtime and equipment failures.

[8] Thompson, Andrew, "Here's How the Internet of Things Advances Supply Chain Management", SupplyChainBrain, 31 July 2019, available at https://www.supplychainbrain.com/blogs/1-think-tank/post/29983-how-iot-improves-supply-chain-management; and Reiner Jedermann et al., “Reducing food losses by intelligent food logistics”, Royal Society Publishing, 13 June 2014, available at https://royalsocietypublishing.org/doi/10.1098/rsta.2013.0302 (both accessed 17 July 2022).

[9] Rio, Ralph, “Proactive Asset Management with IIoT and Analytics”, Arc Advisory Group, 15 January 2015. Available at https://www.arcweb.com/blog/proactive-asset-management-iiot-analytics (accessed 17 July 2022).

Better contract enforcement and new opportunities for service-level contract clauses

22. By allowing constant monitoring, IoT can support contract enforcement and the inclusion of more service-level clauses in contracts. This will allow shippers to better control the implementation of requirements for product storage and establish clear procedures in case of a breach—for example in the form of immediate penalties and/or inspection requirements when storage/transport conditions exceed tolerances.

23. This additional layer of transparency brings greater value by ensuring that claims are based on data rather than speculation, by clearly identifying responsibilities and by allowing shippers to provide more reliable, and thus valuable, product warranties to the final customer. In addition, the collection of this data results in a better understanding (and management) of vendor and service provider performance.

Fleet management

24. When a business manages a fleet of vehicles—from trucks and vans for deliveries to forklifts and cranes within a warehouse—IoT can help improve the quality of fleet management. As discussed above, under advanced and predictive analytics, IoT sensors can reduce costs and improve efficiency by supporting preventative vehicle maintenance. In addition, IoT sensors can support safe and efficient vehicle use by tracking vehicle fuel efficiency and even driver behaviour.

Smoother last mile deliveries

25. E-commerce has driven an exponential increase in last mile deliveries which are among the most challenging because they are time-consuming and costly. IoT can be part of the solution to this problem. GPS, together with IoT (for package and vehicle tracking) and real-time traffic analytics (which often uses traffic data collected by IoT devices), can create optimized routes to reduce fuel waste and time spent stuck in traffic. The same asset-tracking technology used in warehouses can be used to improve consumer package tracking. E-commerce is here to stay, which means last mile deliveries and the use of IoT-supported delivery logistics will also continue to grow.

IoT and financial services

26. Digital insurance services based on IoT technology can support supply chain activities. By collecting and sharing data through IoT devices, underwriters could achieve better insights into customer behaviours, thus allowing them to better evaluate risk on a real-time basis. For example, and as described earlier, IoT devices can be used to monitor the environment in which goods are transported and stored to ensure the maintenance of their quality.

27. In addition, data from IoT devices, when combined with advanced analysis programmes like AI and machine learning, can forecast possible losses that may occur during transport, if extraordinary events take place.

IoT and financial operations in supply chains

28. Based upon the above-mentioned advantages, improvements and innovations in supply chain processes, this table shows the main supply chain actors and describes how each one could leverage IoT to support financial functions.

Table 1
Examples of IoT use by supply chain actors to support trade finance functions

Sellers (receivables, treasury)	*Carrier(s)*	*Buyers (delivery point and supply monitoring)*
Data collection at each production phase Communication of delivery status or its updating (e.g. acceptance/rejection/other)	Providing updates on the status of consignment lots at each stage of the transport process (and, if applicable, execution of blockchain smart contracts) Communication of delivery status (e.g. acceptance/rejection/other) including, if applicable, execution of a blockchain smart contract	Communication of IoT monitoring results during transport (temperature, humidity, etc.) that impact the quality of the goods Activation of lot reception and storage processes at delivery point
Sellers (dispatch point and supply monitoring)		*Buyers (payables, treasury)*
Order reception and/or dispatching with identification of the delivery lot, recording of data, and updating on a blockchain (if applicable)		Communication of quantity of goods and delivery completion status (e.g. acceptance/rejection/other) including, if applicable, execution of a blockchain smart contract Communication of any IoT monitoring during transport (for temperature, humidity, etc.) that impacts the quality of the goods

29. The above uses of IoT technology, when coupled with blockchain and other technologies, could help fulfil the following financial business requirements:

- Ensure that the quality of goods and logistics services are aligned with contractual agreements;
- Reduce errors and time in information exchange, ensuring data security, operation tracking, and proper information access for each player;
- Ensure the legal validity and feasibility of activities in all phases, also in case of disputes and/or in cross-border/jurisdiction environments; and
- Fully integrate financial players and services in order to create an end-to-end trade finance process.

30. The final impact of these applications is resulting in better performance in financial activities and related operations, with increased efficiency in treasury and working capital management.

2. The future of IoT in supply chains

31. The use of IoT in supply chains is growing exponentially. The internet of things, with its sophisticated sensors and communication capabilities, makes the invisible visible, transforming supply chains to be more efficient and increasingly transparent. When combined with other technologies, IoT can integrate pallets, parts, products, packages, equipment (etc) into one ecosystem where they can be continuously monitored, automatically tracked and controlled across networks. The real-time data IoT makes available is paving the way for smarter and more efficient supply chains.

32. This will lead us toward a future supply chain based on a “don’t touch” philosophy. This means designing all aspects of a supply chain with the intent of reducing, if not eliminating entirely, the manual handling and touching of materials, goods, paper and data. In the next decade, IoT will become an invaluable tool to keep products moving, regardless of the industry. As we have seen, optimizing asset utilization to drive greater operational efficiency is at the heart of the IoT value proposition for supply chains. Supply chains and logistics aren't the only industries that could benefit from adopting IoT technology, but this is one industry where it might not be optional for much longer.

B. IoT and government services

33. There are many opportunities for IoT use in government, particularly at the municipal level, but also at the regional and national levels. IoT applications can help governments provide better and new services to their citizens, in large part by making smarter use of their infrastructure and improving asset management.

34. For governments, the use of standards in IoT solutions is important to reduce costs and increase efficiency. Research has shown that, just at the city level, municipal governments and their technology partners could squander up to 341 billion USD by 2025 if they do not use standards in their implementations[10]. UN/CEFACT can contribute to a solid standards foundation through the internationally agreed data definitions in its Core Components Library (CCL) [11].

35. IoT applications have the potential to benefit both governments and the people they serve. The data collected and processed by IoT systems can provide insights which support solutions for improving public sector services and reducing public risks through enriched planning, better facilities management and enhanced security.

36. IoT, when combined with technologies such as blockchain, can provide additional support in addressing the challenges faced by governments as they provide public services. For example, sensors embedded in infrastructure such as buses, trains, and bridges can automatically register the need for maintenance and repair work on a blockchain. Once the data is recorded, it can automatically trigger a request for repair work through smart contracts. Once a problem is recorded through IoT sensors, those same devices can also identify whether the issue has been fixed or not. Such IoT-based applications can reduce costs, improve services and provide greater public safety.

37. Government-supported trade infrastructure varies across countries and can include ports as well as roads and facilities used for customs and inspection activities. Most of these

[10] IoT Alliance Australia, “Inquiry into the Australian Government's Role in the Development of Cities”, July 2017.

[11] For more information, see the UN/CEFACT Executive Guide on Core Components, 2017, available at https://unece.org/fileadmin/DAM/cefact/GuidanceMaterials/ExecutiveGuides/CCL-CCTS-ExecGuide_Eng.pdf.

can benefit from the use of IoT in activities ranging from the management of parking and container storage to increasing energy efficiency and improving maintenance.

38. Recent research provides an example of the growing use of IoT by governments. It predicts that the global market for IoT in smart cities will grow at a compound annual growth rate (CAGR) of 18.8 per cent reaching $347,6 billion by 2027[12]. This market growth is mainly driven by government smart-city initiatives and public-private partnership (PPP) models for providing government services.

39. IoT devices can be used to monitor traffic lights, sound levels, air quality, water security, parking spaces and when public garbage bins are full. A wide range of additional applications also exist, including the tracking of assets, infrastructure management, support in the fight against crime, and the management of emergencies. For example, data from IoT devices can be used to control traffic lights so that they stay green on roads when it is beneficial to the flow of traffic and fuel economy; or, as previously mentioned, IoT devices can be used to monitor the physical status of critical infrastructure such as bridges, roads and buildings in order to notify managers when repair work is needed.

40. By deploying IoT systems, governments can provide better, more timely services through situational awareness, resulting in quicker response times and operational efficiencies. The cost of IoT systems has also decreased over time, providing more opportunities for governments to install IoT-supported systems.

41. Remote monitoring (e.g. traffic and parking), network management, real-time location systems, data management, security, reporting and analytics are a few of the areas driving demand for IoT-supported government systems. Some other of areas in which IoT-supported systems can improve government services are described below.

1. Energy

42. Governments have a responsibility to efficiently manage their own use of energy; in some countries they are also responsible for fulfilling the energy needs of their citizens. The environmental impact of inefficient energy use also makes it important for governments to promote and support smart and clean energy solutions as well as energy conservation.

43. Smart grids are an emerging IoT-based solution to this need. They can allocate energy through demand matching and by keeping track of energy pricing without any human intervention. By deploying IoT sensors and blockchain technology, these transactions can be tracked at a granular level and charged to customers accordingly. For example, using IoT devices and blockchain technology, a micro-grid with 15-20 houses with installed solar panels can allocate electricity across households and order more energy from the main grid when needed, while also tracking the money each household owes, based on their usage. In the future such systems could also include the establishment of carbon credits for each household, calculate related taxes and provide data to support government energy policy.

44. IoT devices can also help governments to be more energy efficient themselves, as described in section B.3, below.

2. Public safety and crises management

45. Information gaps and asymmetries in times of emergency often lead to an inefficient response by public authorities. There are often delays between the start of an emergency, the time when affected citizens are able to alert the authorities, and the moment when authorities have enough information to respond appropriately. This can create a difficult situation where

[12] https://www.globenewswire.com/news-release/2022/04/04/2415496/0/en/Global-IoT-in-Smart-Cities-Market-Size-Share-Industry-Trends-Analysis-Report-By-Component-By-Solution-Type-By-Services-type-By-Application-By-Regional-Outlook-and-Forecast-2021-202.html.

authorities are forced to choose between waiting for adequate information and risking the welfare of involved citizens, or committing resources which may not fit the situation, may be unnecessary and may risk endangering underinformed responders.

46. In defined contexts, particularly when risks are known in advance, IoT applications have the capability to quickly collect and analyse data about an event and rapidly identify and communicate the optimal action(s) to those involved in crisis management.

47. IoT devices can report on early indicators of emergency events and the situation on the ground as they happen by measuring environmental indicators such as smoke in forest areas, rising water levels, the strength of winds and structural stress on structures such as dams and bridges (which may be caused by age or extreme temperatures as well as high water).

48. Environmental sensors can also identify early indications of human-driven emergency events such as traffic jams caused by accidents. An interesting example of this is a device that can detect the sound of a gunshot, providing its location within 10 feet of the incident. By automatically sensing the sound, the system alerts the police, speeding up their reaction, and also makes them less dependent on witnesses to report a crime. Apart from detecting gunshots, several other data points can be collected from sensors, such as cameras and databases to identify any patterns in crime at a particular location. For example, once the police started deploying one such solution in Camden, New Jersey in the United States, it was found that 38 per cent of gunshots in a particular location were not even reported.

49. IoT-connected devices can also help responsible authorities perform better when handling incidents. For example, wearables connected to an IoT ecosystem could provide information about firefighters, first responders and police officers from sensors that monitor their immediate environment, their heart rate, voice volume and stress levels; based on that information, and when appropriate, the system could alert the person in question and/or other respondents for support. In addition, such data could be used for training and handling future situations, promoting better responses.

50. Some smart cities are embedding smart infrastructure in sidewalks, for example, Bluetooth and Wi-Fi-enabled paving material could send emergency messages or crime alerts to mobile phones within a certain distance. These systems could further be integrated with other connected devices such as cameras, or even social media, to allow responders to have a better picture of the scene before they arrive.

3. Infrastructure planning, management and monitoring

51. IoT can be used by governments for planning and infrastructure design and control. IoT devices can collect real-time data on factors such as transportation and traffic conditions, water delivery, food delivery and land use. To analyse complex environments, IoT-based systems take this real-time data from IoT devices and combine it with other information such as data from land registries and available social services in order to support intelligent decision-making and produce more accurate records.

52. IoT-based systems can provide dynamic road and highway management by providing smart, real-time data on road status, lane closures, travel times and toll rates.

53. In ports and airports IoT ecosystems can be used to track and analyse traffic patterns as the basis for infrastructure planning and they can support more efficient space allocation,

especially for containers and vehicles. In addition, equipment monitoring in ports can be used to increase safety and minimize downtime[13].

54. IoT data can also support smart energy solutions based on the monitoring of power usage by governments. For example, electricity and heating used by buildings is responsible for about 28 per cent of all greenhouse gas emissions (another 11 per cent assigned to buildings comes from construction)[14]. It is estimated that, “a smart building with integrated systems can realize 30-50 per cent savings in existing buildings that are otherwise inefficient”[15]. Thus, government implementation of smart buildings and use of IoT devices in existing government facilities can reduce costs, energy wastage and consumption, lower energy-related emissions and result in enhanced government sustainability and energy efficiency.

4. Water security

55. IoT devices can be usefully deployed to support water security and address the challenges surrounding water supply, governance and consumer needs. According to the 2030 Water Resources Group, if current water trends continue, “by 2030, global demand will exceed supply by 40%”[16].

56. IoT systems can help governments to better understand the challenges surrounding water security, equipping them with the data needed to set priorities, allocate resources and make governance decisions. Water management can be improved by highlighting the contributions from all parties in the ecosystem, some of whom may be directly responsible for water management without being aware of their roles in water conservation. By deploying IoT systems, agencies can better coordinate responses and better analyse the impact of each policy decision through real-time measurements that allow “lean start-up” style testing as well as predictive modelling.

57. In the past, the focus in better water management has been on increasing water supply when inventories drop. However, as new sources of water dry up, the focus is now on improving the yield from existing sources. One way IoT can improve the yield from these sources is to precisely determine the point when repair is needed to improve yield, and to provide a cost-benefit analysis looking at the cost of the repair versus the volume of water saved. Through sensors, water managers can obtain a better sense of water flows, prioritizing improvements even when the improvement needs to take place within individual households that are not directly involved in water infrastructure. In-home leaks result in a tremendous loss of potable water globally. Just in the United States, over 1 trillion gallons (3.79 trillion litres) of water are estimated to be wasted every year (an average of 10,000 gallons/37,850

[13] Smith, David, “How IoT Technology Can Enable Efficient Smart Port Operations”, SEARATES blog, 15 September 2020. Available at https://www.searates.com/blog/post/how-iot-technology-can-enable-efficient-smart-port-operations# (accessed 17 July 2022).

[14] International Energy Agency and UNEP, “2019 Global Status Report for Buildings and Construction”, available at: https://iea.blob.core.windows.net/assets/3da9daf9-ef75-4a37-b3da-a09224e299dc/2019_Global_Status_Report_for_Buildings_and_Construction.pdf (accessed 17 July 2022).

[15] Jennifer King and Christopher Perry, “Smart Buildings: Using Smart Technology to Save Energy in Existing Buildings”, published by the American Council for an Energy-Efficient Economy, February 2017, available at https://www.aceee.org/sites/default/files/publications/researchreports/a1701.pdf (accessed 17 July 2022).

[16] The 2030 Water Resources Group, “2020 Report: Valuing Water, Enabling Change”, page 2, available at https://www.2030wrg.org/wp-content/uploads/2020/12/WRG-Annual-Report_2020_Web.pdf (accessed 17 July 2022)

litres per household) [17]. Stopping or slowing these leaks can significantly increase yields of potable water.

58. Over 70 per cent of freshwater is used for agriculture[18], around 20 per cent for industry and the remaining 10 per cent is used for domestic purposes[19]. The greatest water conservation can be achieved through monitoring and automating water use.

59. Water conservation can be made easier if IoT applications are used to collect and distribute monitoring information that supports conservation processes. By providing information such as when and where consumers use water, and how much in comparison to others, IoT-based systems can provide insights, send reminders or apply rules on the use of showers, pools or appliances—thus helping to reduce the domestic use of water.

60. Agribusinesses often irrigate without considering the risk of potential overwatering. These problems can be eradicated through IoT sensors that provide measurements for use in calculating the water needs of plants, such as heat, soil moisture, humidity and land slope.

61. Thus, governments can improve water management by using IoT data to create better insights into both demand and supply. But information alone is not all that is needed, because an infrastructure needs to be in place to allow for actions to be taken based on that information. Some of this infrastructure consists of software, automated machinery and human intervention. Some consists of automated IoT control devices (i.e. devices which receive instructions via the Internet). For example, servo valves can be programmed to automatically shut off pipes upon receiving information that indicates a leakage or rupture.

62. Through improved operations and better insights, government officials can better use existing resources and improve operations, which could lead to cost-savings and lower environmental impacts and possibly free up capital for other government services.

5. Smart parking

63. One frequent IoT use case in government services is smart parking. In China, smart parking enabled by IoT technology allows drivers to easily locate free parking spots.[20] Pollution and congestion are created when drivers circle while looking for parking spaces. To help address this challenge, China Mobile created smart parking pilots using IoT technology in southeast Guizhou and Yunnan. The solution consists of sensors that detect several smart parking data parameters such as licence plates and parking bay places and combines these with parking guidance, intelligence parking management and mobile payments to the city. The benefits of using IoT include the maximized use of parking spaces, low power consumption (the IoT systems are designed to have a battery life of many years) and low costs due to reduced management and maintenance costs.

6. Government IoT deployment

64. One of the major challenges for governments in deploying IoT initiatives is that officials need to create a balance between handling urgent crises and making strategic improvements. Often a lack of support, budget limitations and poor infrastructure are a hindrance to deploying IoT solutions on a wider scale.

[17] United States Environmental Protection Agency, “Fix a Leak Week”, 13 July 2022, available at https://www.epa.gov/watersense/fix-leak-week (accessed 17 July 2022).

[18] World Bank, “Water in Agriculture”, 18 May 2020, available at https://www.worldbank.org/en/topic/water-in-agriculture (accessed 17 July 2022).

[19] McClelland, Jim, “Worldwide water crisis is looming”, Raconteur, 8 December 2016, available at https://www.raconteur.net/worldwide-water-crisis-is-looming/ (accessed 17 July 2022).

[20] IoT ONE, “China Mobile Smart Parking”, available at https://www.iotone.com/case-study/china-mobile-smart-parking/c1006.

65. The key to resolving these issues is creating a collaborative environment which keeps all stakeholders accountable for information sharing. Blockchain use when combined with IoT systems can help address these challenges and also provide security by protecting the large amounts of data collected by IoT devices using cryptography. The budgeting issues and infrastructure provision can be handled through the savings created and/or the use of public-private partnerships (PPPs).

C. Legal challenges for IoT in trade

66. While IoT makes many novel applications with huge potential possible, the implementation of IoT can also pose legal challenges. This chapter looks at the legal and data privacy concerns which are raised by the ability of IoT ecosystems to continuously collect, process and store data.

67. IoT ecosystems are a rapidly developing form of infrastructure that generates large amounts of data. Collecting this data and turning it into knowledge is a key feature of IoT ecosystems. In the context of international trade, this can require the ability to collect data in one country, aggregate it with data from other countries, and analyse it in a third country—all of which entails the ability to move data across borders. The exceptionally large amounts of data so collected can result in "big data" which lends itself to various types of analysis[21]. One example of such an application is the use of IoT for the tracking and tracing of shipping containers.

68. Considering the impact of IoT, it is important to understand the legal aspects that affect this infrastructure and the movement of data via various connected devices and objects in an ecosystem.

1. Data privacy and protection

69. The ever-expanding and ubiquitous character of IoT raises specific concerns about data privacy and data protection. IoT has a unique capacity for increasing the volume and variety of information collected about individuals and entities, as well as the speed of its collection.

70. Increasing digitization, often based on the use of IoT, of industrial sectors such as transportation, manufacturing, agricultural and utilities also means an exponential growth in data collection and processing. The often highly confidential information in data flows generated from the use of IoT in consumer and industrial settings may reveal critical business and personal information over time such as habits, preferences, locations, affiliations, payment patterns and other information. IoT-connected devices are often, by design, discreet and most often lack traditional screen interfaces, which can pose a challenge when obtaining informed consent from the "provider" of data is required. The integration of IoT with other emerging technologies such as artificial intelligence, augmented intelligence, mobile computing and, eventually, applications using quantum computation is leading to new applications for data, a redefinition of what is considered personal information, and a re-examination of how to address privacy concerns.

71. Data privacy and protection laws in the IoT context are increasingly being developed, particularly in the European Union (EU) jurisdiction. The European Commission (EC), which is the executive branch of the EU that proposes new legislation and monitors its implementation, has been working since 2009 to develop a clear IoT regulatory framework

[21] Meltzer, Joshua P. "Maximizing the Opportunities of the Internet for International Trade", E15 Expert Group on the Digital Economy – Policy Options Paper, E15Initiative, (Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, 2016). Available at http://www3.weforum.org/docs/E15/WEF_Digital_Trade_report_2015_1401.pdf.

which facilitates the use of the technology while keeping in mind the key issues affecting public trust in IoT, which are privacy, data protection, consumer protection, safety, security and liability[22].

72. The General Data Protection Regulation (GDPR) [23] is considered to be the first pillar of privacy reform in the EU as it strengthens privacy rights and harmonizes data privacy laws across the region and beyond. Some of the more significant provisions in the GDPR that affect IoT are as follows:

- Territorial scope (Art. 3);
- Conditions for consent (Art. 7);
- Right to erasure, often referred to as the 'right to be forgotten' (Art. 17), the right to rectification (Art. 16) and the right to restrict processing (Art. 18);
- Right to data portability (Art. 20);
- Data protection by design and by default (Art. 25); and
- Breach notification to national supervisory authority (Art. 33).

73. From a regional trade facilitation perspective, the GDPR has attempted to balance the relationship between the EU and foreign corporations. Specifically, foreign corporations need to apply the same rules as European corporations if they are offering goods and services or monitoring the behaviour or personal data of individuals in the EU. One way to transfer personal data abroad is on the basis of an EC 'adequacy decision' establishing that a non-EU country provides a level of data protection that is 'essentially equivalent' to that provided for in the EU[24]. The effect of such a decision is to enable the free flow of personal data to that third country without the need for the data exporter to provide further safeguards or obtain any authorization. In the absence of an 'adequacy decision', international transfers can take place on the basis of a number of alternative transfer tools that provide appropriate data protection safeguards. The GDPR formalizes and expands the possibilities for using existing instruments, like standard contractual clauses and binding corporate rules, to meet its requirements. For example, controllers and processors will be able to use, under certain conditions, approved codes of conduct or certification mechanisms (such as privacy seals or marks) to establish appropriate safeguards.

74. The second pillar of EU privacy reform is the proposed ePrivacy Regulation[25]. This regulation was proposed by the EC in 2017 and is still under consideration before the EU Council. The ePrivacy Regulation updates Directive 2002/58/EC (ePrivacy Directive) to provide a high level of privacy protection for users of electronic communication services and

[22] For more information see "Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions: Internet of Things – An Action Plan for Europe" (COM(2009) 278 final), 18 June 2009, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF.

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[24] Ibid., Article 45 'Transfers on the basis of an adequacy decision'.

[25] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

a level playing field for all market players across borders[26]. The regulation aims to safeguard the confidentiality of communications of personal information. It is a *lex specialis*[27] of the GDPR for electronic communications, which means that the regulation particularizes the GDPR to the case of electronic communications, adding specific provisions to protect electronic communications that include personal data and adapting the privacy regulations for electronic communications to take into account technological change. The ePrivacy Regulation proposal explicitly includes IoT under its scope. It considers the machine-to-machine (M2M) communication between IoT devices (i.e. transmissions of signals between machines over a network) to be an electronic communication service which falls within the scope of the ePrivacy Regulation proposal[28].

75. In the IoT context, data privacy and protection laws are also emerging in other jurisdictions. In the United Arab Emirates, the Dubai Government has introduced the Smart Dubai Plan 2021, which includes an IoT strategy, to encourage governmental authorities to transition to an entirely paperless government by 2021. The implementation of this strategy will happen in four phases over three years[29]. The Telecommunications Regulatory Authority, a governmental entity responsible for regulating telecommunications and facilitating smart transformation in the UAE, issued an IoT Regulatory Policy in 2018[30] and an IoT Regulatory Procedure in 2019[31]. The policy borrows some terminology from the GDPR, including the terms “consent”, “data controller”, “data processing”, “data processor”, “data subject” and “personal data”, but does not purport to incorporate the EU regulatory framework.

76. In Brazil, Decree No. 9.854 established a National Internet of Things Plan on 25 June 2019 to promote IoT in Brazil[32]. It focuses on smart cities, healthcare, agribusiness and manufacturing. To support these IoT plans, the General Law on the Protection of Personal Data 2018[33] is planned to come into effect in the coming years. It replaces and supplements a sectoral regulatory framework and creates a new transversal and multisectoral legal framework for the use of personal data in Brazil in the private and public sectors. Notably, it includes the right to access, rectify, cancel, exclude and oppose treatment of data, as well as the right to information and explanation about the use of data and data portability (see Art. 18).

77. In India a final, comprehensive version of its Draft Policy on the Internet of Things, first published in 2015[34], is expected. Its objectives include creating an IoT industry of USD 15 billion. Notably, the policy covers smart cities, smart water, smart environment, smart health, smart waste management, smart agriculture, smart safety, smart supply chain and logistics, smart manufacturing/industrial IoT, IoT enterprise incubation and capacity building. To support development of an IoT industry, the Indian Government also introduced

[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058.

[27] Lex specialis is a Latin phrase meaning specific statutory interpretation of laws.

[28] Aida Joaquin Acosta, ‘IoT International Regulatory Challenges’ Ch. 7 p. 203 in C. Cwik, C Suarez, L. Thomson (eds) *The Internet of Things: Legal Issues, Policy, and Practical Strategies* (ABA, 2019).

[29] ‘Mohammed bin Rashid launches Digital Wealth Initiative and IoT Strategy’, available at https://sheikhmohammed.ae/ar-ae/news/details?nid=25235&cid=.

[30] See UAE Regulatory Policy: Internet of Things (UAE Telecommunications Regulatory Authority, 22 March 2018)

[31] UAE Regulatory Procedure (Telecommunications Regulatory Authority, 6 March 2019)

[32] See Decree No. 9.854 (25 June 2019), available at http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm.

[33] See Law No. 13.709/2018 (14 August 2018), available at http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

[34] See Draft Policy on Internet of Things (Ministry of Electronics and Information Technology, 2015), available at https://meity.gov.in/writereaddata/files/Revised-Draft-IoT-Policy%20%281%29_0.pdf.

a comprehensive new data protection law in the Personal Data Protection Bill of 2018. Its objective is to protect the rights of individuals to control their personal data, to identify the rights of individuals whose personal data is processed, to create a framework for the implementation of organizational and technical measures in processing personal data, to and establish norms for the cross-border transfer of personal data[35]. The bill emulates the EU GDPR in some ways. For example, in Art. 24, the right to confirmation and access is similar to the 'subject access' right in the GDPR. It also makes several departures from the EU framework. For instance, unlike the GDPR where the right to data portability can be invoked only for personal data provided by the individual, under this bill it can also be exercised for personal data that is generated in the course of the provision of services or use of goods by the data fiduciary. In addition, unlike the GDPR, the right to be forgotten is not a right to erasure; it is only a right to restrict or prevent disclosure of personal data in particular circumstances.

2. Liability issues

78. In an IoT system, the interaction between devices and data involves numerous users and entities. These depend upon the implementation in question and can include the device manufacturers, IoT service providers, mobile application developers, retailers and consumers/end-users. Typically, for any one application/function there are multiple entry and exit points for data. A single vulnerability within the IoT systems supporting supply chains can compromise the security of the entire network and allow unauthorized access at multiple levels. Therefore, risk can be high, and it is critical to ascertain liability for the security of IoT devices and to determine who in the chain of supply is liable to the user. The hyper connectivity of devices leads to hyper complexity in assessing liability allocation.

79. Liabilities can be both civil and criminal in nature and can include strict liability. Strict liability is a liability that can be imposed regardless of whether the defendant intended to cause harm or acted with reasonable care. It is primarily used in reference to product liability.

80. In the EU, product liability rules are defined in the Product Liability Directive (PLD)[36]. The PLD has existed for some time, covering all types of products and including emerging digital technology products, including IoT devices. The PLD assigns liability to producers when defective products cause damages to victims or their property. It defines a strict liability regime, where the victim has to prove the damage, the defect of the product, and that the damage was caused by that defect. The EC has evaluated[37] the PLD and has set up an expert group on liability and technologies[38]. It intends to issue a guidance document to provide clearer definitions of product, producer, defect and damage and make it more relevant to IoT devices. For example, the concept of producer in the case of IoT devices could be revised to account for the possibility of devices being refurbished or their features changed outside of the producers' control. The scope of damages may be widened to cover privacy and cybersecurity damages in addition to physical and material damages.

[35] The "Personal Data Protection Bill, 2018" is available at https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf (accessed 17 July 2022).

[36] "Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (1985) is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374.

[37] See Commission Staff Working Document 'Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products' (2018), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018SC0157.

[38] See "Liability of Defective Products" available at https://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products_en.

81. The 2017 EC communication on "Building a European Data Economy"[39] states a commitment "to assess whether the current EU legal rules for product liability are fit for purpose when damages occur in the context of the use of IoT and autonomous systems". The European Parliament also published a report, asking for liability rules for autonomous systems that would consider safety aspects[40]. In 2018, the EC published a communication on 'Liability for Emerging Digital Technologies'[41] which accompanied a document on AI for Europe. This communication provided a list of liability challenges related to emerging technologies, and also considered a liability framework for cybersecurity attacks.

82. Since technology is developing faster than law, it is important for companies and businesses to protect themselves in cross-border trade where there can be an element of legal uncertainly. To mitigate risk, it is essential for companies and businesses to develop clear contractual expectations, warranties, limitations, and indemnities as well as to obtain insurance to cover potential liability. The integration of best practices into products, software, and operational infrastructures should be considered by companies in order to systematically reduce liability and for quality management.

83. Software developers may have traditionally been able to avoid liability for vulnerabilities in their products, but a confluence of new realities suggests that this protection may not be sustainable[42]. IoT devices are not software, they are devices with software. However, whether it is the owners of the IoT device performing the function that are legally required to comply with rules for the allocation of liability or exemption, or whether liability can be imposed on the device manufacturers, will be subject to the assertion of the claim, the nature of the vulnerability and the extent of injury and real harm.

3. Data ownership

84. The method, structure and analysis of the large data sets that form big data raise interesting issues on data ownership when such data sets are moved to, transmitted to, or interact with other large data systems in an industrial IoT environment. Data ownership and data rights are generally associated with intellectual property rights (IPRs) where a flow of customer data is being collected, processed, anonymized and sent to the data controller for the purposes of optimization. The ownership and usage of data is usually managed by data-use agreements (DUAs).

85. Agreements about data ownership and control affecting consumers may be under some form of government supervision or oversight, therefore certain industries (like the healthcare industry) may need to comply with a range of statutes and agency rules.

86. It is important to note that the term 'data' should be defined as clearly as possible in contractual agreements between parties. A related term is 'derived data' which is the new data generated though analysis of the original data. A data-use agreement should specify the ownership of the derived data and expressly allocate the ownership interest between the

[39] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Building A European Data Economy' (COM/2017/09 final), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A9%3AFIN.

[40] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL), available at http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html/.

[41] Commission Staff Working Document "Liability for emerging digital technologies Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial intelligence for Europe" (2018) (SWD/2018/137 final), available at https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137.

[42] Richard M. Martinez, 'Liability and Connected Products' Ch. 14 p. 411 in C. Cwik, C Suarez, L. Thomson (eds) *The Internet of Things: Legal Issues, Policy, and Practical Strategies* (ABA, 2019).

parties so that the ownership rights are clear and distinctive, regardless of any background IPRs. The agreement should also have anonymity requirements which obligate the analyst to analyse only anonymized data sets provided by the data subject. A data subject may also set restrictions in the licensing of raw data sets for distribution and re-distribution when negotiating IoT usage agreements[43].

4. Admissibility of electronic evidence

87. There are a number of challenges associated with the collection and preservation of IoT data for e-discovery and in using the data as evidence. For example, identifying the IoT systems and devices where relevant data is stored can be difficult given that the initial data creation often takes place in multiple stages (especially when edge computing and/or machine learning is used).

88. Another challenge is the authentication of digital evidence in legal proceedings[44]. The factors that are considered in evaluating the integrity of digital data include who created the evidence, what processes and technology were used, and what was the chain of custody throughout the entire life cycle of the digital evidence.

5. Dispute settlement

89. As IoT continues to expand its reach, so too will its impact and the need for dispute settlement. Some examples of the impact of IoT on dispute settlement follow:

- First, conflict is often a by-product of innovation (i.e. the IoT can, itself, generate disputes[45]); for instance, faulty IoT devices can trigger disputes based on product liability.
- Second, IoT can prevent disputes since automation has the potential to reduce or remove human error[46].
- Third, as a new source of digital evidence, IoT can serve as a tool to prove a case[47]. For example, IoT devices can provide increased visibility of parcel and cargo journeys in addition to providing real-time tracking information[48]. This increased availability of information provides a unique opportunity for counsel and prosecution to argue and prove a case. That said, counsel and prosecution must learn how to extract relevant information effectively while being mindful of the operational and privacy challenges inherent to this new source of digital evidence[49]. In addition, there is little guidance available since there are few written decisions addressing the use and handling of IoT data in litigation or arbitration.

[43] David Tollen, 'The Big Data Licensing Issue-Spotter', Tech Contracts Academy (08 December 2015), available at https://techcontracts.com/2015/12/08/the-big-data-licensing-issue-spotter/#_ftn4 (accessed 17 July 2022).

[44] See Lucy L Thomson, 'Mobile Devices: New Challenges for Admissibility of Electronic Evidence', *The SciTech Lawyer* Vol. 9 No. 3 (Winter/Spring 2013), available at https://cdn.ymaws.com/birminghambar.org/resource/resmgr/retreat/2019_forum/2.1_digital_evidence_in_the_.pdf (accessed 17 July 2022).

[45] Ethan Katsh and Orna Rabinovich-Einy, 'Digital Justice: Technology and the Internet of Disputes' (Oxford University Press, 2017).

[46] *Ibid.*

[47] Samantha V. Ettari, "United States: Handling Internet of Things Data in Litigation", *Practical Law,* (Thompson Reuters, 17 January 2019), available at https://www.kramerlevin.com/images/content/4/6/v3/46579/ Handling-Internet-of-Things-Data-in-Litigation.pdf (accessed July 18 2022).

[48] Manish Choudhary, "How IOT is Transforming the Shipping Industry", Entrepreneur, 17 April 2019, available at https://www.entrepreneur.com/article/332392, accessed 7 August 2019.

[49] As an example, please refer to In Re Apple, Inc. 149 F. Supp. 3d 341, 364 n.26 (EDNY 2016).

90. In the resolution of disputes arising from the digitization of things, such as those that may arise in the context of IoT ecosystems, arbitration offers several important advantages. For example, it offers parties the flexibility to select the location of arbitral proceedings, which is of particular benefit in disputes of a transnational nature (for example disputes involving IoT devices that have travelled through different jurisdictions, like smart freight containers). In addition, the opportunity to appoint expert arbitrators means that IoT disputes can have access to specialized expert knowledge and judgment not available in a traditional court of law.

III. Conclusion

91. IoT technology introduces the ability to design many novel applications in support of trade facilitation and better government. Applications incorporating IoT devices have the potential to increase efficiency, improve services, and in some cases safety, while also reducing costs. At the same time, it is critical that IoT-based solutions be designed to mitigate not only ICT and physical risks but also legal risks such as those related to data security, safety and privacy while ensuring performance, usability and scalability. Achieving this trade off may require the development of new standards as well as the redesign of existing tools and methods to cater to the specific challenges created by IoT ecosystems.