United Nations ECE/TRADE/C/CEFACT/2022/12

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: Guide to Internet of Things Technology, Communications and Connectivity

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: Guide to IoT Technology, Communications and Connectivity*, which provides an overview of the technologies used in IoT for trade-related applications—the objective being to provide explanations that are accessible to managers responsible for implementing information technology.

Document ECE/TRADE/C/CEFACT/2022/12 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 internet of things 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-based data about location and the conditions under which goods have been transported can be used to simplify insurance claims for everything ranging from late delivery to goods damage (due to temperature, humidity, excess motion, etc.). IoT data 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 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[3];
- *IoT in Trade Facilitation: Guide to IoT Technology, Communications and Connectivity*, 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 (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; and

[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: The Internet of Things in Supply Chains and Government Services" (ECE/TRADE/C/CEFACT/2022/11), 2022.
[4] UN/CEFACT, "White Paper on Internet of Things Standards in Trade Facilitation" (ECE/TRADE/C/CEFACT/2022/9), 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. 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 elements are 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.

6. 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 the Internet of Things in Trade Facilitation: the Internet of Things in Supply Chains and Government Services.

II. Overview of IoT technologies

7. What is the internet of things? An IoT system is a network of networks where, typically, a massive number of objects, things, sensors or devices are connected through communications and information infrastructure to provide value-added services via intelligent data processing and management for different applications (e.g. smart cities, smart health, smart grid, smart home, smart transportation, and smart shopping).

8. In order to part of the internet of things (IoT), the above mentioned “objects” or “things” (hereafter referred to as “devices”) must have unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction[6].

9. IoT devices may:

- Include one or more sensors (for temperature, humidity, movement, etc.);
- Transmit the device’s location (using calculations or GPS);
- Both transmit information and receive instructions (e.g. sending signals to a refrigerated transport container in order to adjust the temperature);
- Include some processing intelligence (e.g. analysing sensor data and transmitting alerts when it exceeds an expected value range);
- Collect data from other IoT devices for transmission or initial analysis (if they analyse data, they are called edge-computing devices); 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

[6] Alexander S. Gillis, "What is the internet of things (IoT)?" TechTarget, March 2022. Available at https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. (Accessed 17 July 2022)

- Be embedded in a living entity such as an animal (e.g. monitoring the health of animals during transport).

10. The following are types of data collected by IoT devices:

- *Status data*: This is the most basic type of IoT data and is primarily used as raw material for more complex analyses, but can also have a significant value of its own. A common trade example is sensors in shipping containers that indicate their internal temperature or humidity;
- *Location data*: This is data that identifies the location or position of an object of interest. International trade has many examples of IoT for tracing trucks, containers and products;
- *Automation data*: This is sensor data that supports the control of processes and carries out functions like monitoring and adjusting heating systems, lighting, warehouse conditions, etc.;
- *Actionable data*: This is IoT data that, when analysed, results in actions to optimize solutions such as identifying available parking or storage space; cutting excess energy consumption (e.g. using sensor data on water depth, currents and wind so that a vessel can adapt its speed to use less fuel); improving preventative maintenance of equipment (e.g. trucks or forklifts) and the performance and monitoring of maritime systems over the lifespan of a ship; and
- *Feedback data*: IoT can also create feedback loops for evaluating and adjusting changes in the processes for handling and transporting goods.

11. The data captured or generated by an IoT ecosystem may be transmitted directly to an application (on the cloud, a blockchain or a private server) or it may be fully or partially analysed locally before being transmitted. When IoT ecosystems generate large volumes of IoT data, the applications that use this data are often located in the cloud and/or may use artificial intelligence to analyse the data.

12. IoT applications often deploy devices in networks (ecosystems). For example, a smart ship has an IoT ecosystem to inform it of environmental conditions (wind, currents, etc.) as well as cargo, equipment and operating information that reduces (or even eliminates) the need for a human crew. In another example, a smart warehouse building has an IoT ecosystem that monitors a range of building conditions and controls equipment in order to maintain a certain temperature and humidity range to minimize costs and to alert management to any problems.

III. IoT devices and technology

13. In order to be effective, IoT devices have a wide range of requirements, some related to the devices themselves and some to the IoT ecosystems in which they operate. The main requirements of IoT devices are as follows: They should:

- Include sensors and/or transmitters and/or receivers;
- Be small, low cost and use no or low power (with long battery life);
- Have a unique identity and an identifiable location;
- Transmit data either over short-range distances to other IoT devices, or over medium- to long-range distances;
- Communicate and share data with other systems (which requires interoperability);
- Be maintained both in their hardware and software;

- Be secure and protected from unauthorized access and data falsification; and
- Operate in a legally correct way.

14. There are new technologies being discovered every week, if not every day, that can impact these different IoT requirements. In this section an attempt is made to look in more detail at the above requirements and related technologies, with the exception of legal issues, which are looked at in the UN/CEFACT Report of the eDATA Management Domain on the Internet of Things in Trade Facilitation: the Internet of Things in Supply Chains and Government Services.

A. Kinds of IoT devices

15. There are many different types of IoT devices, the broad categories looked at here include those with sensors, those without sensors, edge-computing devices and IoT gateways.

1. IoT devices with one or more sensors or actuators

16. Sensing technologies combined with IoT devices provide the means for creating information that reflects a characteristic of the physical world. IoT sensors collect information which is processed at one or more layers in an IoT ecosystem. For example, the collecting IoT device may decide if a temperature reading is within range or it may transmit it to a nearby IoT edge-computing device for this decision. Then, only "out of range" temperature readings are communicated to a further computing layer for additional analysis and processing.

17. The growing number and kind of sensors which can be included in small IoT devices is made possible by developments in nanotechnology and, more specifically, in micro-electromechanical systems (MEMS). These are miniature machines with electronic and mechanical components such as springs, channels, cavities, holes and membranes. They range in size from several millimetres to less than one micrometre (i.e. much smaller than the width of a human hair).

18. From an IoT standpoint, the most interesting MEMS are sensors (to detect a state) or actuators (to control a process). Microsensors exist for a multitude of tasks including the sensing of temperature, pressure, humidity, motion, chemicals/gases, magnetic fields, radiation, etc. Existing types of micro actuators include microvalves and pumps for control of gas and liquid flows; optical switches and mirrors to redirect or modulate light beams, micro flaps to modulate airstreams on aerofoils and many others.

19. Progress in MEMS depends on developments in microfabrication techniques (including for their incorporation into integrated circuits) as well as on clever design. MEMS are also referred to as micromachines, micromachined devices or microsystems technology (MST) [7].

2. IoT devices without sensors

20. Some IoT devices do not include sensors and, instead, only receive and/or transmit information. An example of the receiving type is an actuator that receives instructions from a distance to unlock or lock a door, start a machine, etc. The second type of IoT device may

[7] See TechTarget definition at https://internetofthingsagenda.techtarget.com/definition/micro-electromechanical-systems-MEMS. For more information on MEMs, visit the MEMS and Nanotechnology Exchange website: https://www.mems-exchange.org/MEMS/what-is.html (both accessed 18 July 2022).

be passive or active and includes radio frequency ID (RFID) and near-field communication tags which allow other IoT devices to read information.

3. Edge-computing devices

21. Edge-computing IoT devices collect data from other IoT devices and provide a range of benefits (described below), including several which reduce overall IoT system costs. These include the following:

- **Reduced device costs:** This is accomplished by moving more expensive analytic computing tasks away from individual IoT devices and allowing connected devices to be equipped with only short-range transmission capabilities.
- **Reduced data transmission costs:** This is accomplished by analysing IoT data and only transmitting data which meet defined criteria.
- **Lower latency**: Because computation is performed closer to data origin, there is less transfer time. This is beneficial in manufacturing process and medical applications where real-time feedback and quick responses are essential.
- **Data privacy**: Edge computing creates more options for data treatment. For example, it has the potential to solve some personal data protection issues by processing personal data locally and only transmitting forward anonymous results for further processing or storage.
- **Higher security**: Centralized architectures are vulnerable to distributed denial of service (DDoS) attacks. A decentralized edge-computing architecture makes it difficult for a single disruption to take down the entire system.
- **Scalability**: Edge-computing architecture can offer a more flexible expansion of computing resources, as more devices are added to an IoT system, by reducing the computing, transmission and storage burden on a central system. For example, an edge-computing device could analyse the results from many sensors on a second-by-second basis and only forward averages over set periods of time and/or readings that are outside of a prescribed “normal” range.
- **Reduced maintenance costs and environmental impact**: By deploying simple IoT sensors in the field and pushing computing functions to the IoT Edge, the field-deployed IoT devices require less computing power, which increases battery life. This results in less frequent servicing and, by extending battery life, reduces waste.

4. IoT gateway devices

22. An IoT edge-computing device which is dedicated to data transmission is called an IoT gateway device. These are used to reduce the cost of telecommunications by receiving long distance communications and then distributing them onward to less expensive IoT devices with lower power needs and shorter-distance communications capabilities (e.g. Bluetooth) as well as collecting data from these IoT devices and then transmitting them onward over longer distances.

B. IoT energy requirements

23. One of the key operational challenges when implementing an IoT network is power consumption. Many IoT components (especially when used in transport) need to be relatively simple and able to operate for long periods of time, unattended and in remote locations. This highlights the need for low-power consumption, long battery life and strategies for maintaining signal (communications) integrity.

24. These requirements result in a number of design considerations which depend upon the IoT application and the communication channel being used for data transmission. For instance, the best way to conserve power for an IoT device with a wireless radio is to ensure that the radio is only fully powered when in use. Similarly, in the case of cellular channels, it is important to choose an efficient and secure communication protocol that requires minimum overhead. In most cases, low energy transmitters are available which allow devices to be in sleep mode and only become active when an event occurs, or they are programmed to "awaken" and take measurements.

25. Despite the availability of technologies that enable low power consumption, large IoT deployments involving thousands of devices can still present serious energy-related maintenance challenges, such as the need to detect and change devices that fail or whose batteries have died[8] and the likelihood that many of these mass-deployment devices may need to be replaced in a short period time as their lifespan ends; for example, if 10,000 devices with a 3-year battery life are put into use over a 2-year period, then 5000 devices will need to be replaced in the 4th and 5th years.

C. Location of devices and target objects

26. The location identification needs for a device are determined by the IoT application/ecosystem. If an IoT device is relatively immobile (such as a sensor in a traffic light or a fixed RFID at a warehouse) then it may need to transmit its location only upon installation or being moved (or its location may be registered by the installer, thus removing the need for transmission). On the other hand, if the IoT device is attached to an asset that is being tracked such as a package or a shipping container, it may need to transmit its location several times, or more, a day. Most IoT devices are low-power, so the more power needed to determine and transmit location, the more expensive the IoT device and the more often it will need maintenance.

27. If only the approximate location of the IoT device is needed (e.g. if stock has passed through a loading dock or is in an identified building or site), then having an IoT gateway device to detect the presence of simpler, more passive IoT devices (such as RFID tags) may provide sufficient location information.

28. More precise location information is determined using radio-signal transmitters and receivers. The shorter the range of radio-signal transmitters and receivers, the less power they need. This makes GPS one of the most expensive solutions. One way the cost of GPS can be minimized is by using low-energy devices in conjunction with a more powerful edge-computing device. The edge computing device then to (1) collects IDs from the less powerful devices that are within a low-energy transmission distance (and, if needed calculates their exact position), (2) receives a GPS signal and uses this to calculate the positions of the other, low-energy devices, and (3) transmits the calculated position(s) of the low energy devices with their IDs (perhaps via satellite). Such edge-computing devices can be installed on vehicles such as trucks or ships to collect location information about the packages and/or the containers they carry.

29. The principal methods for determining location with radio-signals are GPS and registered signalling devices. GPS is a system in which a radio-signal receiver listens for radio signals transmitted by various satellites, which it then uses to calculate its position.

[8] The majority of IoT devices are waterproof, which makes it necessary to replace these devices when their batteries die, since it is impossible to change the batteries.

30. Registered signalling devices are used to determine (via an online database[9]) or calculate (based on a method called triangulation or trilateration[10]) the location of the radio-signal receiver in an IoT device. The exact steps to be taken vary depending on whether the registered signalling is from a Wi-Fi access point, a Bluetooth access point, or a cellular base station.

31. Once the location of an IoT device has been determined, it may need to transmit the position of other "target" objects (for example, pallets inside of a warehouse). If the IoT device is attached to the target object, such as a container, this is relatively easy, but attaching an IoT device to every target object can be expensive relative to the cost of the object and, in some cases, may not be physically possible.

32. In those cases, there are two principal ways to associate target objects with an IoT device:

- The radio signal receiver in the IoT device reads individual identification information attached to the target objects such as radio frequency IDs (RFIDs)[11] or near field communication (NFC)[12] tags, and
- Individual identification features of an object are obtained via image analysis (which requires that either the IoT device or a connected edge-computing device have more expensive computing capabilities).

IV. Communications and connectivity

33. In IoT, it is essential to have data transfer between the IoT layers that acquire physical information (such as location, temperature, chemical composition, etc.) and cyber layers that aggregate physical information and perform various calculations and analytical processes. At the same time, data transmission capabilities add costs, both to the IoT device and for the communication itself. In addition, the efficiency, effectiveness, and security of data transmission can be affected by technology choices, as discussed below.

A. Communications

1. Communications – wireless technology

34. Most of the communication methods used between devices in an IoT system are based on wireless communication. The two most frequently used types of wireless communication methods are

- **2.4 GHz band:** This is for short/medium-range transmission and is easy to implement for smartphones and IoT gateway devices. Examples include Wi-Fi, Bluetooth, Zigbee, etc. It is the most convenient communication method because a licence is generally not required, making global deployment easier.

[9] see https://cellidfinder.com/articles/how-to-find-cellid-location-with-mcc-mnc-lac-i-cellid-cid.
[10] For For more information on trilateration techniques: Ana Roxin, Jaafar Gaber, Maxime Wack, Ahmed Nait Sidi Moh. Survey of Wireless Geolocation Techniques. 50th IEEE Globecom07, Nov 2007, Washington DC, United States. ffhal-00701118f - https://hal.archives-ouvertes.fr/hal-00701118/document
[11] For information on how RFID works, see https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm (accessed 18 July 2022).
[12] NFC tags can only be read from a distance of 4 cm (about 1.5 inches) or less but are highly secure. For more information see https://nfc-forum.org/what-is-nfc/about-the-technology/ (accessed 18 July 2022).

- **920 MHz band:** This allows for medium to long-range transmission. Examples include EnOcean, Z-Wave, Wi-SUN and Low-Power Wide Area (LPWA[13]) networks (i.e. LoRaWAN, Sigfox, NB-IoT), etc. A radio station licence is not required in many countries, but available bandwidths vary so global implementations are difficult to implement[14].

2. Communications – formats/standards (i.e. protocols)

35. Of the wireless communication methods used within IoT systems, the only method included in the Internet protocol suite[15] is Wi-Fi. For this reason, IoT gateways, which collect information from nearby IoT devices, often need to convert the data received into a format that belongs to the Internet protocol suite so that it can be transmitted via the Internet.

36. The primary Internet protocols used in IoT are HTTP and MQTT, followed by UDP:

- **HTTP**: Originally a communication protocol used for sending and receiving content, such as HTML. It is very simple and versatile, so it is often used in IoT. However, it requires that a message header be attached to both requests and responses, so it tends to be avoided when there are large volumes of data and a need to prevent transmission costs from increasing.
- **MQTT**: A data delivery protocol that allows messages to be kept lightweight, and also includes a specification, called QoS, where a guarantee of delivery level can be specified.
- **UDP**: The lightest weight protocol, however it does not guarantee reliability, order, or data integrity, so it is used only for data transfer (i.e. not for the transmission of instructions/code) and only when delivery confirmation is not needed.

37. In addition to creating transmission compatibility with Internet protocols, IoT gateways can also provide encryption in order to protect the data within the networks and during data transmission. In this context, gateways can be thought of as an extra layer between the cloud and IoT devices which can filter out attacks and illegal network access attempts.

B. Connectivity

1. Connectivity - network technologies

38. A virtual network is made up of hardware and software which are not physically connected but communicate together according to set a set of standards/rules, usually over the Internet. Characteristics that are important design considerations when developing a virtual IoT network (ecosystem) include signalling, presence detection, bandwidth, communication channel and security.

39. With increasing demand to achieve lower latency (times between transmission and reception) and higher security, virtual network standards are starting to play a huge role in IoT systems.

[13] For more information on LPWA, see https://www.paessler.com/it-explained/lpwa (accessed 18 July 2022).
[14] For information on frequency types, see http://www.ginsei-jp.com/920MHz_vs_24.html. For info on LoRaWAN visit https://www.emnify.com/iot-glossary/lorawan (accessed 18 July 2022).
[15] The Internet protocol suite, commonly known as TCP/IP, is the set of communication protocols used for the Internet and similar computer networks.

40. For example, **software defined wide area networks** (**SD-WANs)**[16] are often utilized in the telecommunication sector to offer higher bandwidths with faster throughput and the ability to offer lower cost services. In addition, even faster virtual network technologies, such as those that use mesh networks, are starting to surface. **Mesh networks**[17] allow any individual node to communicate directly using peer-to-peer (P2P) encrypted communications with every other node, or individual nodes on the same network segment, in a fast and reliable manner that resembles that of a LAN (local area network), but over nearly any distance.

41. Another important network technology, often used in IoT, is **low-power wide-area networks**[18] (LPWANs). Many IoT applications need to transmit data over long distances and for long periods of time, sometimes years. Examples include agricultural sensors, warehouse sensors and urban sensors for garbage collection, lighting, parking, etc. The trade-off is that transmissions on LPWAN networks can fail to complete due to interference—so it cannot be used for "mission-critical" applications such as in healthcare or industrial processes—but if information from an irrigation sensor or a garbage bin are a little late, no harm is done.

42. Highlighting the importance of both connectivity and standards to support IoT use in trade, the Digital Container Shipping Association (DCSA) has published recommended IoT gateway connectivity standards[19] which are fully compatible with related UN/CEFACT interoperability standards.

43. Each IoT connectivity option has its own benefits and trade-offs related to data transmission (e.g. amount of data and frequency), latency, power consumption, cost and security, to name a few. High-volume, fast data transfers generally use more power. The trade-offs for low power consumption are generally shorter range and less bandwidth.

44. The best option will depend upon the application: Does an organization collect meter readings across a city or a large facility like a port? Maybe they should consider LoRa[20], which is a good option for sending small amounts of data at regular intervals. In an industrial setting that needs to connect millions of small, real-time sensors or requires ultra-reliable, low-latency connectivity, 5G may be best. For agricultural businesses that want to capitalize on IoT, cellular isn't an option, so low-power, long-range WAN may be the best bet.

2. Connectivity - data flows

45. The core of any IoT ecosystem is the orchestration of data flows. In other words, the routing and interactions between "data packages" coming to and going from IoT devices, including edge-computing and gateway devices, the cloud, other databases/blockchains and operations and/or analytical software applications (including AI systems). In establishing this orchestration, the following should be considered:

- **Interoperability**: In the context of IoT, this refers to the ability of systems or components of systems to communicate with each other regardless of their manufacturer or technical specifications. Why is interoperability needed? Imagine in an IoT ecosystem in an office building where the system that regulates the air conditioning unit speaks a different language from the one spoken by the system that controls the windows blinds (as programmed by their manufacturers). In that case, these two systems would not be able to communicate with each other or act in a

[16] For info on SD-WANs, see https://www.networkworld.com/article/3031279/sd-wan-what-it-is-and-why-you-ll-use-it-one-day.html (accessed 18 July 2022).
[17] For info on mesh networks, see https://computer.howstuffworks.com/how-wireless-mesh-networks-work.htm (accessed 18 July 2022).
[18] For further inf on LPWAN, see https://www.iotforall.com/what-is-lpwan-lorawan.
[19] DSCA website: https://dcsa.org/standards/iot-connectivity.
[20] LoRa (short for long range) is a spread spectrum modulation technique derived from chirp spread spectrum (CSS) technology. For more info, see https://www.semtech.com/lora/what-is-lora.

coordinated manner—resulting in the owner having higher than necessary electrical bills. Given that the technology ecosystem is still in a nascent stage and the market for IoT devices is fragmented, interoperability is a key issue.

- One example of a standard addressing interoperability issues is IEEE P2413-2019[21], which describes an architecture framework for the internet of things (IoT). This description is focused on concerns shared by IoT system stakeholders across multiple domains (transportation, healthcare, smart grid, etc.) such as security requirements for IoT communications.
- Another example is the United Nations Core Component Library[22] standard which supports **semantic interoperability** through standardized data definitions. This interoperability layer ensures that data from different systems use the same definitions—for example for temperature or time or for more abstract concepts such as "out of range".
- Interoperability at the level of **data formats** often requires conversions between the standards and communication formats used in a local IoT network and those used on the Internet. In most cases, this process is performed on gateway devices, but it may also need to be incorporated in application programming interfaces (APIs) which are used for communicating instructions and data between software programmes.

- **The aggregation of data** with defined characteristics from various locations in order to identify trends needs to be considered. Data aggregation may take place in either a local gateway device or a cloud-based central data centre.
- **Transferring data to various data storage locations and media** may be needed for multiple reasons and requires careful planning to ensure that data versions are tracked and when data should be identical in two different places –they are identical, or it is possible to easily identify that they are not – and why.
- **Eventual changes to data flows**: IoT ecosystems need be designed flexibly so that data flows can be modified at any point in order to take advantage of new technologies, new applications, and changes in service providers.
- **Generation of learning data for artificial intelligence (AI)**: IoT can continuously generate data for use by AI systems for learning and developing inference models. These AI processes can take place continuously or in batches at set times (i.e. once a day, week, etc). This is usually done at a cloud layer because edge-computing devices typically do not have the needed processing power. For more info, see the section on artificial intelligence below.
- **Communicating data to blockchains** (distributed ledgers): This is used in the automatic execution of smart contracts (to be discussed later in the section on blockchain technology).

[21] The IEEE P2413-2019 Standard for an Architectural Framework for the Internet of Things (IoT) is available for purchase or subscription at https://standards.ieee.org/content/ieee-standards/en/standard/2413-2019.html.

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

V. IoT management and security

46. Security in IoT ecosystems needs to protect data against external attacks that could compromise or bring down the ecosystem and protect the confidentiality and integrity of the data. Some of the more important risks for IoT ecosystems include the following:

- Man-in-the-middle attacks where hackers intercept and steal or change data as it is transmitted over open networks;
- Botnet attacks where a hacker takes control of a number of devices by exploiting security vulnerabilities within those devices in order to use their computing resources; and
- Ransomware or other malware which, if installed on IoT devices, can jeopardize an entire IoT ecosystem.

47. A cybersecurity framework to address these threats should include a well-defined naming and registration process for devices, a strong system to authenticate devices, protocols for devices to securely communicate within the network, and a platform for managing devices throughout their life cycle including the ability to shut down or isolate a device if it goes "rogue". One secure framework is the zero trust design philosophy – which only allows components within an IoT architecture to communicate when they have been specifically granted the right to do so, thereby drastically limiting the ability of components to impact other services, should they become compromised.

48. Device management is a key challenge both from a security and an operational standpoint. Unlike conventional IT systems, IoT systems have many devices that can be scattered across various locations, and devices can be in environments that makes them vulnerable—either physically and/or in terms of their network connections. In addition, IoT systems need to be easy to reconfigure because of changing technology and applications. For these reasons, it is good practice to always know the current state of each IoT device and the software it contains and to have secure mechanisms for giving remote instructions, including for changing parameters and updating their software.

A. Device operations and updating

49. In order to ensure easy updating and reconfiguration of IoT systems, a secure mechanism for updating the software in IoT devices is essential. To reduce the cost of updates, IoT software should be written in modules, with parameters and settings that can be remotely updated. The ability to change only parameters, or only individual modules, minimizes updates and allows them to be implemented in a more granular manner, thus reducing telecommunications and other costs. Remote updating of devices is called "over-the-air" (OTA) firmware[23].

50. The following are two important technological solutions to device management and updating:

- A **message broker**[24] (like in the MQTT protocol described above) acts somewhat like a trusted third party to enhance security because the broker only receives messages from authorized "publishers". Then, IoT devices "subscribe" to the broker and periodically request information that they have "subscribed" to receive (i.e.

[23] For more information, see https://predictabledesigns.com/how-to-update-embedded-firmware-over-the-air-ota.

[24] For more information on message brokers, see https://www.ibm.com/cloud/learn/message-brokers#.

distribution works on a pull, as opposed to a push, basis). For software updates, a message broker can send an address for a software update (instead of sending the entire update) which the IoT device can then access in order to download it. Message brokers simplify management, in particular through the use of asynchronous communications, so that if an IoT device is temporarily out of service or busy it will still receive the message or update when it comes back online or is able to update—and the message broker keeps track of which subscribers have received the message and which have not. There is also no need to keep a central list of all devices to be updated, as they are registered with the message broker as subscribers at the time of installation; and

- IoT software and updates can be designed to implement **idempotency**[25]. This means that when an action is repeated, the result is always the same as when it was implemented the first time. For example, if the same software update or parameter change is accidentally done twice (or even 100 times) on the same IoT device, the result is always the same.

51. Many elements in IoT architectures rely on open source software components which means that security vulnerabilities are often fixed quickly. At the same time, in the period between the vulnerability being discovered and the patch being applied, the device is susceptible to the vulnerabilities. This makes the systems and speed with which IoT devices are updated particularly important.

52. When designing systems for the management of IOT ecosystems, it is also important to keep in mind the following needs:

- Designs and updates should be based on experience-derived **incident-management models** for IoT ecosystems. Standards for incidence management for IoT ecosystems do not yet exist, but one can be sure that there will be incidents as real-life operations never run perfectly. There are also no standards for IoT incident management when it is used with for blockchain technology, nor guidance on how existing incident management models might be applied to these technologies. There are only generic standards for information sharing such as ISO/IEC 27010, 20614, 20247 and 19592[26].
- Legal considerations should be taken into account when designing for the activities of collecting, retaining, analysing, deleting, and sharing data.

Device state monitoring

53. In addition to a mechanism to update the software (firmware) of an IoT device, a mechanism is needed to correctly know the state of that device. This means, at a minimum, a log showing the current software configuration as well as past software configurations, a software operations log, and the communications status of the device.

B. Device security and audit

54. Because IoT data can be used to make decisions (for example, to pay an insurance claim or not) and the data can be used for developing AI inference models or smart contracts on blockchain networks, there is a need to guarantee that the data is true and is from the real world.

[25] For an explanation of idempotency, see https://medium.com/@ahmadfarag/idempotency-764f7bb6e4e2.

[26] IS/IEC 27010 - Information Security management for inter-sector and inter-organizational communication; ISO 20614 – Data Exchange protocol for interoperability and preservation; ISO 20247 – International Library Item Identifier; ISO 19592 – Security Techniques – Secret Sharing.

55. Technical solutions to support this guarantee include the following:

Network security

56. In communication between a device and a system, or between devices, security measures for network vulnerabilities are generally provided by placing a firewall around the IoT network (i.e. extra security for communications passing the firewall) and by encrypting communications.

Device identity

57. The receiver of data from the IoT device must verify that the sender is the correct partner. This is usually done through public-private key cryptography for communicating device identities. To make this even more secure, in the future, the use of blockchain mechanisms for issuing public-key certificates may become common place.

Software audit

58. Although impersonation can be prevented through the use of device identities, there is still the possibility of unauthorized data being transferred due to tampering with a device's software. This can be prevented via continuous auditing and recording of the state of the software in the device. For example, the software on the device can be periodically hashed[27] and recorded in a blockchain or another secure database where it cannot be changed (software is just a set of numbers, so you can hash it as though it were one very big number). Then, any time there is a change in the hash, it can be compared to the device log to see if the new hash matches the expected result from an update. For additional security, software audits can be run in trusted execution environments which use both hardware and software to isolate a software programme from external interference.[28]

VI. Complementary technologies

A. Artificial intelligence

59. Artificial intelligence (AI) is becoming an essential part of many IoT systems as data and system owners seek to use and make sense of large volumes of IoT-generated data. In addition, AI when combined with IoT data, can provide a range of benefits to trade facilitation, particularly in the area of risk analysis. For example, it could allow shippers and insurance companies to determine which shipments are at the greatest risk of having been damaged or tampered with. It could also support comparative analyses of shipping routes and methods that were previously not economically feasible.

60. Artificial intelligence uses "deep learning" processes with very large volumes of data (big data) which it then uses to develop "rules" for evaluating new data. These rules are called an "inference model" and the model can be updated as deep learning processes receive and analyse additional data.

61. Deep learning is very computationally intensive, requiring significant computing power and resources. Application of the inference model is much less resource intensive.

62. As result, in more advanced IoT systems that use AI, decentralization of workloads can be seen. In other words, deep learning takes place on the cloud or another centralized

[27] For a definition/description of hashes, see https://techterms.com/definition/hash.
[28] For more information on trusted execution environments, see https://blog.quarkslab.com/introduction-to-trusted-execution-environment-arms-trustzone.html.

platform and then the resulting AI inference models are deployed onto IoT edge-computing devices to "make decisions" (e.g. to identify defective products). These edge-computing devices and their AI models can also perform a preliminary evaluation of new data before it is sent onwards for use in further "deep learning", thus reducing the burden on the cloud AI processing side.[29]

63. If the data collected by IoT is subject to privacy regulations, one way to ensure respect for privacy rules is to use federated learning in AI, which consists of different techniques for maintaining the privacy of data through local processing and/or encryption[30].

1. Some steps in preparing and saving data for use in AI

64. Most of the data acquired by IoT for monitoring, operations or other purposes can be considered time-series[31] big data. Thus, the data has potential for AI and machine learning uses, even if that was not the original purpose for which it was collected. As the cost of AI declines, companies will increase their use of AI, and this will increase the value of existing, older data sets. As a result, even if a company is not using AI to analyse its IoT data today, it may want to consider storing its IoT data in "AI friendly" formats for possible use in the future. To do this, two considerations need to be kept in mind:

65. The first is how to continuous collect data in a state which would allow for its processing in the future. The following are two possible technology solutions for storing large quantities of data for future:

- **Data lakes**[32]: data storage that accumulates raw data acquired by IoT
- **Data marts**[33]: data storage that stores data extracted and processed from the data lake for a specific purpose or subject area

66. The second consideration is preparing AI data for processing. For this, two commonly used technologies are **MapReduce** and **stream processing**:

- **MapReduce**[34] is an open source big data programming model that supports parallel computing – i.e. computation on the same "problem" undertaken simultaneously on a cluster of computers to speed up processing and analysis. MapReduce is commonly used to create the structured data needed for AI and to save the results to a data mart for use as AI learning data.

[29] For an article on training versus inference, see https://blogs.gartner.com/paul-debeasi/2019/02/14/training-versus-inference/.

[30] For more info on federated learning, see https://towardsdatascience.com/how-federated-learning-is-going-to-revolutionize-ai-6e0ab580420f ; on inference, see https://www.steatite-embedded.co.uk/what-is-ai-inference-at-the-edge/; and on AI generally, see https://simpliv.wordpress.com/2018/08/14/what-is-ai/?.

[31] Time-series data is collected over time and each piece of data has its own time stamp, meaning that events, sequences of events, and the regular or irregular spacing of these events over time can be plotted and analysed. As in long-term studies, the value of the data increases relative to the length of time over which it was collected. For more information, see https://www.influxdata.com/what-is-time-series-data/.

[32] Forbes, "What is a Data Lake?" https://www.forbes.com/sites/bernardmarr/2018/08/27/what-is-a-data-lake-a-super-simple-explanation-for-anyone/#7122bc1b76e0.

[33] For a definition of data mart, see https://searchdatamanagement.techtarget.com/definition/data-mart . (accessed 11-10-2020)This reference also contains a nice table comparing a data lake, data mart, data warehouse and relational database.

[34] For more info about MapReduce, see https://medium.com/edureka/mapreduce-tutorial-3d9535ddbe7c.

- **Streaming data**[35] is continuously generated time-stamped data. The process of generating streaming data is referred to as **stream processing** and it can be done through AI inference (to pick out data of interest) or it can be as simple as showing an alert if a certain value exceeds a threshold.

B. Blockchain technology

67. Blockchain technology enables separate parties to place a higher degree of trust in a transaction because the entries in an electronic ledger (database) cannot be easily falsified (i.e. once data is written it is extremely difficult to change, keeping in mind that veracity depends on the data being correct from the outset). This 'immutability' is due to a combination of factors as described in the ECE Whitepaper on Blockchain in Trade Facilitation[36] which provides a detailed overview of the technology.

68. As a result of these qualities, blockchain systems can be used as an independent umpire in processes that might otherwise expose participants to the risk of one party not living up to its contractual obligations (counterparty risk) and where third-party guarantors are reluctant to intervene and assume part of that risk.

69. An additional feature of many blockchains that makes IoT/blockchain combinations attractive as a trade facilitation solution is the ability to implement "smart contracts". Smart contracts are programmes that automatically execute once a set of agreed conditions are met, guaranteeing rapid implementation with minimal human interaction (and thus, often, lower costs). For example, an IoT device communicating GPS coordinates to a blockchain may trigger recognition in a smart contract that a shipment has arrived. This, in turn, may trigger an automatic payment. This decision-making automation results in faster execution while reducing human handling and the potential for error and/or fraud. In addition, the use of blockchain technology has the advantage of providing a transparent and auditable information trail.

70. To take advantage of the tamper-resistant nature of distributed ledgers, it is necessary to make direct entries from the IoT devices that are the source of the data (or their IoT gateways). This is to protect the generated data from being suspected of alteration (by an intermediate system).

1. Advantages of combining IoT and blockchain technology for trade facilitation

71. The core of any IoT ecosystem is the orchestration of data flows. This involves the interactions between data and the routing of that data as it comes and goes from IoT devices, including interfaces with edge-computing and gateway devices; the cloud; databases/blockchains; and operations and/or analytical software applications (including smart contracts registered on a blockchain).

72. While the technical aspects of this orchestration were considered above, the following sections will look at factors to consider when evaluating the benefits of deploying blockchain technology in an IoT ecosystem, taking into consideration its strengths and weaknesses and concluding with a few examples of how IoT is already being combined with blockchain to create improved trade facilitation.

[35] For and intro to stream processing, see https://medium.com/stream-processing/what-is-stream-processing-1eadfca11b97.

[36] UNCEFACT, White Paper on Blockchain in Trade Facilitation (ECE/TRADE/457), 2020, available at https://www.unece.org/fileadmin/DAM/trade/Publications/ECE-TRADE-457E_WPBlockchainTF.pdf.

73. As discussed in the introduction, 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 payment".[37] Trade processes are characterized by a high volume of repetitive activities and transactions, carried out by a large number of stakeholders – textbook conditions for the use of both IoT and blockchain technology with the advantages for trade facilitation that are described below.

Simplification

74. IoT used in conjunction with blockchain technology, and particularly the use of smart contracts, can simplify processes by removing intermediary actors whose primary purpose is to ensure the authenticity of data and/or to request action based on that data. Now the data can come from IoT devices, the "requests" for action can come from an IoT ecosystem and/or a blockchain smart contract, and the authenticity can be ensured via registration on a blockchain.

Standardization

75. Blockchains can increase confidence in shared (or common) data from IoT ecosystems via their ability to do the following:

- Facilitate a common understanding among stakeholders such as between shipping and receiving companies or between a trade financing bank and an exporter. For example, stakeholders can access and use the same, verifiable data to describe objects/events related to containers if the containers have installed IoT devices or IoT readable tags/codes such as NFC, RFID or QR codes[38]. These can be read by other IoT devices and selected information can be stored on a blockchain for access.
- Reliably identify the time and origin of every entry from an IoT ecosystem. For example, a trade financing bank could identify exactly when goods arrived at the importer's warehouse, or an insurer could exactly identify when goods were damaged (and who had possession of them at that moment).
- Verify IoT data with high levels of confidence because of their resistance to cyberattacks due to their use of cryptology.

Harmonization

76. Blockchain technology when used with IoT supports harmonization for the following reasons:

- All stakeholders with "read rights" for blockchain data view the same IoT data, which is available to everyone at the same time, thus injecting clarity and increasing the potential for collaboration.
- The same IoT information is recorded on all nodes across the blockchain.
- Blockchains strengthen the integrity of data captured from IoT devices through their high level of reliability. A blockchain cannot verify data (although smart contracts can have a role in verification); however, a blockchain eliminates the risks associated

[37] From the Trade Facilitation Implementation Guide, available at https://tfig.unece.org/details.html.

[38] Near-field communication (NFC) enables short-range communication between compatible devices. Radio frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. A quick response (QR) code is a type of matrix barcode that, in this case, links the reader to a specific URL.

with the single point of truth (single source of data) created when IoT data is recorded on one database.

2. Blockchain and IoT disadvantages

77. The limitations and drawbacks of using blockchain are well documented. The following are relevant to the use of blockchain technology with IoT for trade facilitation:

- There is a need for quality data because 'garbage in, garbage out' remains true with blockchains—although this can be partially alleviated by using blockchain smart contracts to evaluate the quality of data before they are written to a blockchain.
- Security standards are immature for platform configurations that support the shared use of software by multiple users who each have access to only their own data (multi-tenancy).
- Data privacy regulations may require examining if data generated by IoT devices is written to a blockchain that is shared with multiple stakeholders.
- Interoperability between blockchains may not be easy to establish. Where more than one blockchain solution exists (for example, one used by a shipping chain and one used by customs), if these two systems cannot 'communicate', then information may remain in silos.

78. The introduction of IoT has been a boon for trade facilitation because it has generated hitherto untold volumes of granular data on trade—surpassing by far previous manual data collection systems. Nonetheless, gaps in data remain, and where there are gaps, distortions or inaccuracies, these shortcomings remain an issue in the data registered on a blockchain.

79. In addition, unless a blockchain's governance or smart contracts dictate otherwise, blockchains are data takers, recording all the trade data they receive without any analytical selection process. This could be an issue if all the data coming from an IoT ecosystem were written to a blockchain, because the sheer volume of data generated could cause system failures and/or cost hikes on networks that charge a small fee each time data is written to a blockchain.

80. This is why, although IoT devices can be a useful way to capture data; generally, not all IoT data is written to a blockchain. Data from IoT devices is often filtered so that:

- Only data that goes outside of defined ranges is communicated, or
- The data is communicated as a total set of readings at the end of a process, or
- A "hash" [39] of a large volume of data, gathered over a precisely defined period, is saved on the blockchain while the data itself is saved elsewhere. This last option works because if you want to verify the data, you put it through the hashing mathematical functions and if the result is different than the result saved on the blockchain, then the testing party knows that the underlying data has been changed.

3. Two examples of using IoT with blockchain technology to facilitate trade

Temperature sensing for insurance purposes

81. Fruit is temperature sensitive and is best kept between 4 and 15 degrees Celsius during shipment. If, for example, during transportation an IoT device in a cargo container records

[39] A "hash" is a sort of cryptographic fingerprint that changes if even one character in the hashed data changes. This means that if a gigabyte of data or even one digit or one space in that data is changed, then the hash for the entire gigabyte of data will change. The process cannot, however, be used to identify where the change was made.

that fruit was kept at 0°C for two entire days, this can trigger insurance-related actions. In other words, when the IoT device transmits temperatures falling outside the range, this information, recorded on the blockchain, can activate a smart contract, which notifies the insurance company that a payment should be made to the exporter to compensate for the goods destroyed by the excessively low temperature. That payment will automatically be made by the smart contract without any further intervention by either the importer, the exporter, or the transport company. This significantly decreases the cost for insurance companies in processing claims because they do not have to reconcile information submitted by the shipper/exporter with the insurance policy, evaluate the truth of the insurance claim (the IoT data registered on a blockchain provides the proof) and then request payment. In addition, it reduces the costs for the shipper/exporter as they do not have to undertake any further documentation of the problem that occurred and they will receive their insurance payment more quickly[40].

Trade finance

82. The traditional system of trade finance involves the transfer of a bill of lading (BoL) to the cargo owner, either physically or through email, and matching that BoL data with warehouse receipts of cargo (both of which can be forged) to raise finance. A common form of fraud is issuing multiple warehouse receipts for the same goods and then using these fraudulent receipts to raise financing. IoT can combat fraud by monitoring, in real time, cargo in transit and at the warehouse. Data collected by the IoT devices and written to a blockchain (to prove authenticity) can then be traced by stakeholders with 'read only' access. In addition, as in the previous example, when conditions are met (e.g. cargo arrived on time) smart contracts can be triggered to execute trade finance contracts. By providing stakeholders with a secure and immutable source of data, the combination of IoT and blockchain technologies doesn't eliminate fraud, but it does make it harder to commit.

VII. Conclusion

83. Economic transactions involving cross-border trade depend on access to timely, trustworthy data. IoT devices writing to a blockchain can provide a solution, enabling real-time access to information for users ranging from sellers and buyers to intermediaries such as third-party logistics providers and customs officials. Smart contracts—a feature of blockchain technology—can act as an automatic reconciliation mechanism, facilitating the rapid execution of payments against a given set of conditions. In addition, blockchains are relatively resilient to cyberattacks due to their use of cryptography. While issues of data quality and interoperability are common to both IoT and blockchain technology, the use of this combination can be a highly effective instrument for trade facilitation.

[40] This example, along with a more comprehensive analysis, can be found in the UNCEFACT White Paper on Blockchain in Trade Facilitation (ECE/TRADE/457), 2020, available at https://www.unece.org/fileadmin/DAM/trade/Publications/ECE-TRADE-457E_WPBlockchainTF.pdf.