A guide to IoT terminology

WHAT IS IOT?

IoT Basics for your Business

2021 Edition

telenor IoT

CONTENTS

Here’s a guide to help you understand what is what in the age of connected things

Have this guide at hand to stay smart about everything smart: from smart devices, through communication technologies, to terms associated with the Internet of Things!

But first, what is the **Internet of Things**?

> *The concept of connecting any device (i.e “thing”) to the Internet (and/or to each other) to make it talk, listen and/or perform tasks. This includes almost anything else you can think of.*

Internet of Things encompasses a complex array of acronyms and terminology that can over-complicate understanding of the core technologies and functions that enable IoT deployments. This glossary sets out definitions for popular technology, terms, acronyms and systems to demystify the IoT industry and to serve as a handy guide to explain the background of IoT and introduce the newest terminology. We have divided IoT into four key sections for this glossary which include:

IoT Communications, IoT Connections, the IoT Market and IoT Security.

These four areas neatly segment the market so you can quickly locate relevant terminology in the glossary. IoT is always moving and continuously innovating so even IoT industry veterans will encounter new technologies, acronyms and descriptions. We have included commonly used terminology in this glossary to provide a comprehensive yet still easy-to-use tool to help increase understanding and awareness of the technology, connectivity, markets and security that enable IoT.

COMMONLY USED TERMS

M2M

Machine to Machine

A communications style emphasizing data transfer between large (sometimes industrial) machines that makes use of near-instantaneous data transfer to facilitate higher efficiency and pre-empt problems.

IOT

Internet of Things

Coined in 1999, this refers to the active exchanged of information between devices previously unconnected.

IOE

Internet of Everything

Another term for IoT coined by and still used by Cisco, implies that IoT is not only made up of things, but also of data, process and people.

IIOT

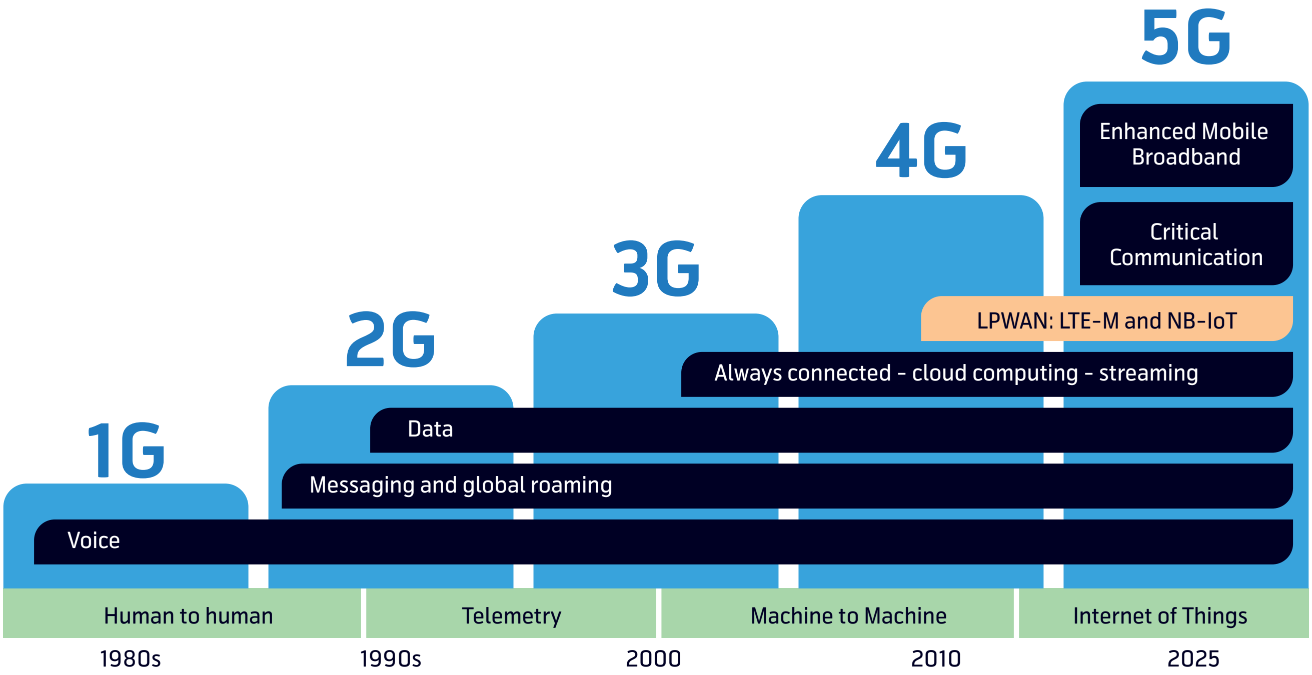
Industrial Internet of Things

An umbrella term for M2M technology when it is focuses exclusively on industrial machines.

MOBILE CONNECTIVITY

1G to 5G and LPWAN: From people to people and things

First a short overview of the development of mobile connectivity technologies. Mobile connectivity has evolved from being the infrastructure for human communication to telemetry, machine-to-machine and the internet of things applications.



The first version of mobile connectivity – 1G – introduced wireless voice.

In 2G, roaming and SMS messaging were introduced and were later enhanced with GPRS for data communication. SMS messaging and GPRS became widely used for basic telemetry. Roaming made mobile technology suitable for deployments in multiple countries. Telenor was one of the first operators to offer M2M communications with things connected over the 2G network as early as the 1990s.

3G became a truly global standard and combined the best of competing technologies in a single standard. 3G evolutions were mainly centered around high speed data applications.

4G introduced LTE technology used for devices constantly connected to the internet. 4G answered the consumer need for bandwidth and speed and introduced a new way to handle voice, replacing 2G voice.

LTE-M and NB-IoT (Mobile IoT) are especially designed for the Internet of Things. LTE-M and NB-IoT support devices that need a long battery life and devices that need good network access in areas that are difficult to reach.

5G networks use a combination of existing 4G LTE and new 5G New Radio (5G NR) technology. 4G and 5G have been designed to co-exist and applications designed for 4G, including LTE-M and NB-IoT, can be expected to have a very long life. Today most networks that claim to be 5G networks are in fact using 4G LTE.

5G enhances 4G in three main use case areas; enhanced mobile broadband, critical communications and mobile IoT. Enhanced mobile broadband is currently targeted towards consumers that need ever-increasing bandwidth. It also enables new IoT use cases that require high data volumes, for example streaming video.

Critical communications demands a much faster response and increased quality of service and security. 5G introduces 5G New Radio Technology which uses a higher radio frequency.

Mobile IoT - LTE-M and NB-IoT - are forward compatible with the 5G NR technology, which means that LTE-M and NB-IoT technology can be used throughout the complete 5G life cycle.

IOT COMMUNICATIONS

What infrastructure is necessary for IoT communications in 2021?

The IoT connection is the enabling technology that powers IoT but it's the communication of the IoT device via the internet that really enables an IoT solution to create value. Communication between the IoT device and IoT gateway and onward into the cloud makes it possible to perform data processing, analytics and storage. IoT bridges both telecoms and IT protocols and several IoT-specific protocols have emerged to help standardize and streamline IoT communication processes.

The role of an IoT gateway is important here because it acts as an aggregator of data from connected IoT devices which can then communicate onwards to the cloud. The IoT gateway is a device that connects IoT endpoints, equipment systems, sensors and cloud resources. An IoT gateway can be an item of hardware or a virtual device and in either case is a fundamental enabler of IoT communication.

Cloud and IoT go hand-in-hand because cloud resources enable IoT organizations to process data from the IoT device to IT systems and then also communicate data from the cloud to the IoT device. This necessity for two-way communications is a vital enabler of IoT benefits, especially for applications that are continually adjusting and need inputs from a centralized administrator – whether automated or human.

Communications protocols used in IoT deployments include Lightweight M2M which is a device management protocol designed for sensor networks and the device volumes associated with M2M environments. Machine Type Communications (MTC) and massive Machine Type Communications (mMTC) also cater for this high device volume end of the IoT market and allow fully automated data generation, exchange, processing and actuation among intelligent machines, with low or no human intervention.

Typically, the protocols utilized in IoT comprise low power and low processing burdens which fit with the requirements of sensor devices and devices such as smart meters that have long lifecycles. However, as greater complexity becomes a requirement for more sophisticated IoT use cases, protocols that demand more processing power and greater power consumption are set to be adopted. Advanced message queuing protocol (AMQP) is one example of an IoT protocol for receiving and placing messages in queues and setting up a relationship between components. However, it is not suitable for IoT devices that have limited memory.

Another example is data distribution service (DDS) which is a scalable IoT protocol that enables high-quality IoT communication. In comparison to IoT DDS allows for interoperable data exchange independently of a hardware and software platform. However, there are many options for communication and data protocols in IoT. Which of these are selected will be dependent on the application and use case.

In common with the connectivity selected for a use case, the IoT communications protocol stack offers options for all levels of IoT requirements and is maturing rapidly. An important aspect of this maturity is to bridge the differences between connectivity, internet and data protocols. This enables improved communications between all the systems involved and also prepares the architecture for additional cloud-based and virtualized functions including artificial intelligence, machine learning and greater reliance on open source systems in future.

COMMUNICATION PROTOCOLS

AMQP

Advanced Message Queuing Protocol
AMQP is an open standard application layer protocol used for transactional messages between servers. Main functions include receiving and placing messages in queues, storing messages and setting up a relationship between components. It is not suitable for IoT sensor devices with limited memory.

CoAP

Constrained Application Protocol
CoAp is an application layer protocol that has been designed to address the needs of HTTP-based IoT systems. HTTP is foundation of data communication for the World Wide Web but, while it is freely available and usable by any IoT device, it can consume too much power for IoT applications. CoAp has addressed this limitation by translating the HTTP model into usage in restrictive devices and network environments.

DDS

Data Distribution Service
DDS is a scalable IoT protocol that enables high-quality communication in IoT. Similar to the MQTT, DDS also works to a publisher-subscriber model. In contrast to MQTT, DDS allows for interoperable data exchange independent of the hardware and the software platform.

LPWAN

(Low-Power Wide Area Network) A network based on mobile communications technology which uses a low bit rate typically catering to smart devices.

Lightweight M2M

A device management protocol designed for sensor networks and the demands of a machine-to-machine (M2M) environment.

MOBILE IOT

refers to low power wide area (LPWA) 3GPP standardised secure operator managed IoT networks in licensed spectrum. In particular, LPWA are networks designed for IoT applications that are low cost, use low data rates, require long battery lives and often operate in remote and hard to reach locations.

Modbus

A serial communications protocol for use with programmable logic controllers (PLCs) that is used to connect industrial electronic devices.

MQTT

(Message Queue Telemetry Transport) is a lightweight, publish-subscribe network protocol that transports messages between devices. The protocol usually runs over TCP/IP.

MTC

Machine Type Communications
A descriptive term for fully automatic data generation, exchange, processing and actuation among intelligent machines, with low or no intervention by humans.

MULTICAST

describes the updating of many devices at once. It works similarly to public broadcasting of TV and requires devices to be ready to receive updates at the same time. TCP/IP. The Internet Protocol suite is the computer networking model and set of communications protocols used on the Internet and similar computer networks.

NR

(New Radio) is a new radio access technology developed by 3GPP for 5G, designed to be the global standard for the air interface of 5G networks.

PSM

(Power Save Mode) is a functionality to reduce power consumption by allowing IoT devices to go into sleep mode when not active. The PSM feature was introduced in 3GPP Release 12 and is available for all LTE device categories.

SCEF

(Service Capability Exposure Function)
Network operators can expose the SCEF service to find devices that do not use the IP protocol.

TELEMETRY

is the process of recording and transmitting the readings of an instrument.

ARTIFICIAL INTELLIGENCE

AI

Artificial Intelligence
The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition and decision-making. AI also enables machines to learn from experience.

Computer vision

A part of computer science working to enable computers to see, identify and process images in a manner similar to human vision.

Deep learning

A machine learning technique that teaches computers to learn by example.

Machine learning

Machine learning is a method of data analysis that automates construction of analytical models, based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention.

Neural networks

A computer system modelled on the human brain and nervous system that is designed to help machines reason more like humans.

COMPUTING AND THE CLOUD

API

Application Programming Interface
A set of routine definitions, protocols, and tools for building software and applications. An API connects your business processes, services, content, and data to channel partners, internal teams, and independent developers in an easy and secure way. APIs are becoming the de facto standard by which companies exchange data and build consistent cross-channel customer experiences.

APN

Access Point Name
A gateway that translates communications between telecommunications and computer networks (most often the Internet).

Cloud computing

Internet-based computing that allows for data access from distinct computers or devices. Typically referred to as though the 'cloud' itself is storing the data, but data is stored on physical computers that allow access at any time to the data via the Internet.

Edge computing

A model in which computation is largely or completely performed on distributed device nodes known as smart devices or edge devices as opposed to taking place in a centralised cloud environment.

Firmware/FOTA

A specific class of computer software that provides the low-level control for the device's specific hardware. FOTA refers to the capability of upgrading firmware over-the-air.

Fog computing

Also known as edge computing or fogging, Fog computing is a term created by Cisco that refers to extending cloud computing to the edge of an enterprise's network.

Flow-based programming

A type of dataflow programming in which programme steps communicate with each other by transmitting data through some kind of channel. The channels are managed by the larger system, leaving the connected components free to focus on processing input and producing output.

Hybrid cloud

A cloud computing environment that uses a mix of on-premise, private cloud and third-party, public cloud services with orchestration between the two platforms.

Java/JSON

A general-purpose computer programming language designed to produce programs that will run on any computer system. JavaScript Object Notation is text-based lightweight technology for generating human readable formatted data.

OTA

Over-the-Air

OTA provisioning refers to various methods of distributing new software, configuration settings, and even updating encryption keys to devices of sorts.

Open source

Describes software for which the original source code is freely available and can be redistributed or modified.

Peer-to-peer

Peer-to-peer computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application.

RESTful API

Also referred to as a RESTful web service a RESTful API is based on representational state transfer (REST) technology, an architectural style and approach to communications often used in web services development.

SOAP API

Simple Object Access Protocol (SOAP) is a communication protocol for the exchange of information between various operational systems using Extensible Markup Language (XML).

DATA

Big data

Amounts of data that are so large that traditional technologies cannot handle their transfer or analysis. Certain IoT technologies specialize in handling and transferring big data as it is seen as key to large companies' goal to maximize efficiency.

Blockchain

A growing list of records, called blocks, which are linked using cryptography. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks.

Data filtration/filtering

Describes a wide range of strategies for refining data sets so they provide what a user, or set of users, needs without including other data that can be repetitive, irrelevant or even sensitive.

Data janitor

A data janitor is a person who takes large amounts of big data and condenses it into information that businesses can act upon.

DDDM

Data Driven Decision Making

An approach to business governance that values decisions that can be backed up with verifiable data.

Hadoop

An open source distributed processing framework that manages data processing and storage for big data applications running in clustered systems. Pervasive computing, also called ubiquitous computing

The embedding of computational capability into everyday objects to make them effectively communicate and perform useful tasks in a way that minimizes the end user's need to interact with computers.

SCADA

Supervisory Control And Data Acquisition
A computer system for gathering, analyzing and controlling real-time data.

TCP/IP

The Internet Protocol suite is the computer networking model and set of communications protocols used on the Internet and similar computer networks.

IOT CONNECTIONS

What connection types are IoT devices utilizing in 2021?

IoT connected devices are creating a world in which data is exchanged between physical objects such as sensors, on-device software and adjacent technologies with other systems and devices. The essential enabling technology is the connection between the 'things' of IoT which enables these exchanges to happen. Immense value is now being derived across the value chain as organizations take advantage of new opportunities, new business models and new revenues which are enabled by IoT connections.

Different IoT connection types are utilized depending on the requirements of the IoT devices involved which can range from IoT and connected devices that need to communicate infrequently with small amounts of data to always-connected IoT devices that require large amounts of data to be communicated at high speed and with low latency. There are a wide variety of IoT connections that can be used to connect a thing as small as a dental implant to something as large as a tractor.

Connecting all these different things in IoT and adding sensors to them adds a new level of digital intelligence, enabling connected devices to communicate in real-time and to participate in automated processes at immense scale. As IoT matures, the number of connections is accelerating rapidly and IoT connected devices forecasts show the growing trend for deployments that involve large volumes of devices connecting to the internet.

There are now approaching 14 billion connected IoT devices in deployment, which exceeds the number of non-IoT connected devices, such smartphones, tablets, PCs and fixed line telephones. This number is expected to grow to 30 billion in 2025[1] as the Internet of Things makes the fabric of the world around us even smarter and more responsive and digital and physical universes merge.

The types of IoT devices that can be connected range from sensors and actuators that perform relatively simple functions, such as turning a light on or off or notifying authorities that a trash bin is full, to complex always-connected devices, such as ride-sharing vehicles that can be geo-fenced and tracked. Continuous monitoring has proven its value in assuring uninterrupted cold chain logistics, for example, but even newer applications will rely on high bandwidth, low latency connections to enable use cases such as remote medical procedures or video-enabled security.

With tens of billions of devices connected by 2025, the number of use cases will also accelerate rapidly, taking IoT into new markets. At the same time, connection types are diversifying to take account of the different needs of IoT devices. The cellular market has been on a journey from 1G to 5G and 5G is now available, alongside earlier cellular generations, to connect devices that require very high speed, very low latency as well as the capability to connect huge numbers of IoT devices in densely packed areas.

There are many different IoT connection types to choose from and there is likely to be an optimum solution for all IoT device types that matches IoT device requirements with the application, the system, software and devices it needs to connect to and which takes account of coverage and availability at the deployment location.

Different connection types and devices are now coming together to create the hyperscale Internet of Things, driving innovation and increasing the scope of what is possible to achieve by connecting devices and bridging the digital and physical worlds.

[1] https://iot-analytics.com/wp/wp-content/uploads/2020/11/Insights-Release-Connectivity-tracker.pdf

GLOSSARY

LPWA

Low power wide area networks typically utilise unlicensed radio technologies to enable relatively low capacity over sites such as factories, campuses and mines. Most offer a cost-effective, low power alternative to cellular connectivity, with the exception of NB-IoT, and are well-suited for IoT applications that require modest throughput. Key types of LPWA connectivity include:

Bluetooth

Bluetooth is a short-range wireless technology mainly used for exchanging data between fixed and mobile devices over short distances using UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz, and building personal area networks. Its characteristics make it suitable only for short distance deployments.

Bluetooth Low Energy (BLE)

Bluetooth Low Energy is aimed at applications in healthcare, security, home entertainment and wireless beacons. Independent of Bluetooth, BLE offers reduced power consumption while maintaining the range of classic Bluetooth.

LoRaWAN

LoRaWAN is a networking protocol for connecting wireless battery operated devices to the internet in regional, national or global networks. It addresses IoT requirements such as bi-directional communication, end-to-end security, mobility and localisation services. LoRaWAN baud rates range from 0.3 kbps to 50 kbps.

Narrowband IoT (NB-IOT)

NB-IoT is a low power wide area (LPWA) technology developed to enable a wide range of IoT devices and services. NB-IoT significantly improves the power consumption of user devices, system capacity and spectrum efficiency, especially in deep coverage in contrast to cellular networks. Battery life of more than 10 years can be supported for a wide range of use cases. It provides a simpler, lower bandwidth alternative to cellular connectivity.

Sigfox

Sigfox is similar to LoRaWAN in that it is a technology designed for global roll-out to provide wireless networks to connect low power objects such as smart meters. It has low power characteristics and utilises the 900MHz band with networks in 72 countries, covering 5.8 million square kilometres, as of November 2020. Sigfox communication supports up to 140 uplink messages a day, which can carry a payload of 12 octets at a data rate of 100 bits per second.

Wi-Fi

Wi-Fi is commonly used for local area networking of devices and for internet access. Well known in home and small office networks, the technology is also utilised in enterprises to connect devices and provide public internet access for mobile devices. Wi-Fi has a range of 20-150 metres and some versions can achieve speeds of more than 1Gbps.

Zigbee

Zigbee is a communications protocol used to create personal area networks with small, low power digital radios. Typical applications include home automation, medical device data collection and other low power, low bandwidth use cases. The technology is limited to transmission distances of 10-100 metres with a line of sight in order to keep power consumption low. Zigbee has a defined data rate of 250Kbps and is suited for intermittent data transmission.

THE THINGS IN IOT

Access point

A wireless network device that acts as a portal for devices to connect to a local area network.

Beacons

Small transmitters that connect to Bluetooth and Bluetooth Low Energy (BLE)-enabled devices such as smartphones or tracked packages.

Device

A device is a unit of physical hardware or equipment that provides one or more computing functions within a system.

eDRX

(Extended Discontinuous Reception) is an extension of an existing LTE feature that can be used by IoT devices to reduce power consumption. eDRX can be used without PSM or in conjunction with PSM to obtain additional power savings.

Gateway

A "hub that translates" communication between two computers or devices that allows these to understand each other´s data transfer and communication.

Hub

A hardware device that connects other data-transmitting devices to a central station.

IOT MODULE

A small electronic device embedded in objects, machines and things that connect to wireless networks which sends and receives data.

Sensor

A device that measures a physical input from its environment and converts it into data that can be interpreted by either a human or a machine.

THE PHYSICAL WORLD MEETS THE DIGITAL

Actuator

A component that is responsible for moving and controlling a mechanism or system, such as opening a valve.

Cyber-physical systems

Integrations of computation, networking and physical processes with feedback loops where physical processes affect computations and vice versa.

Contactless

Describes technologies that allow a smart card, mobile phone or other device to connect wirelessly – without contact – to an electronic reader, typically in order to make a payment.

Digital twins

A digital replica of physical assets, processes, people, places, systems and devices that can be used for various purposes and integrates historical machine data into a digital model.

Geofencing

The use of GPS or RFID technology to create a virtual geographic boundary in which devices can operate.

GIS

Geographic Information System
A system designed to capture, manipulate, analyze, manage and present spatial or geographic data.

GNSS

Global Navigation Satellite System
A constellation of satellites providing signals from space that transmit positioning and timing data to GNSS receivers

GPS

Global Positioning System
A technology created by the US Government that allows for location services.

Haptics

The science of applying tactile sensation and control to interaction with computer applications.

HAV
Hardware-Assisted Virtualisation
The use of a computer's physical components to support the software that creates and manages virtual machines (VMs).

IMU
Inertial Measurement Unit
A device that measures and reports a body – such as a drone's – specific force, angular rate, and sometimes the magnetic field surrounding the body.

LIDAR
Light Detection and Ranging
A remote sensing technology which uses the pulse from a laser to collect measurements which can then be used to create 3D models and maps of objects and environments.

Mechatronics
Engineering of both electrical and mechanical systems which includes a combination of robotics, electronics, computing, telecoms, systems, control and product engineering.

RADAR
Radio Detection and Ranging
A detection system that uses radio waves to determine the range, angle, or velocity of objects.

Telematics
A method of monitoring an asset by using GPS and onboard diagnostics to record movements on a computerised map.

HARDWARE & SOFTWARE

eSIM
The embedded SIM (also called eSIM or eUICC) is a secure element designed to remotely manage multiple mobile network operator subscriptions and be compliant with GSMA specifications.

ICCID
Integrated Circuit Card Identifier
The unique serial number embedded on a SIM card.

IMSI
International Mobile Subscriber Identity
A unique number, usually fifteen digits, associated with identifying a GSM-connected device.

IoT module
A small electronic device embedded in objects, machines and things that connect to wireless networks which sends and receives data.

IP Address
An Internet Protocol Address is a unique designating number assigned to a computer (or other device) that is connected to a network, most notably the Internet

Modem
A hardware device that allows a computer to send and receive data over a telephone line or a cable or satellite connection.

Router
A hardware device designed to receive, analyse and move incoming IP packets to another network.

SIM
Subscriber Identity Module
A smart card that stores including identity, location, phone number, network authorisation data and security keys that is installed into a wireless device.

SOC
System on chip/Single-board computer
A microchip with all the necessary electronic circuits and parts for a given system, such as a smartphone or wearable computer, on a single integrated circuit.

Wireless modem
A modem that bypasses the telephone system and connects directly to a wireless network, through which it can directly access the Internet connectivity.

IOT MARKET

How is the global IoT market developing in 2021?

The global Internet of Things market is predicted to be worth US$900 billion in revenue by 2025 and this figure has trebled since 2019, GSMA Intelligence reports[1], demonstrating the momentum that IoT has. Inevitably revenue has taken a hit because of COVID-19 but, at the same time, IoT has had the opportunity to prove its value in the pandemic, notably in connected logistics to ensure vital supplies and vaccines are delivered to those that need them.

The IoT market is complex, sophisticated and multi-layered with different use cases and categories requiring different services and relying on different business models. Thing to person business models are different to thing-to-thing models and provision of connected mobility has different costs and requires more complex connectivity that connecting static objects such as those in connected manufacturing and to enable Industry 4.0.

IoT benefits come in many forms. First there is revenue generated by the applications, platforms and services that exploit the insights generated by data. This can either be monetized by charging for improved services, better products or enhanced quality or a return can be achieved in operational efficiency. Often an IoT business case is a blend of both models and business models can involve multiple parties with benefits flowing in several directions simultaneously.

The immense scale of IoT can make competitors collaborators and transform product-focused companies into service organizations. This makes it a challenge to define the IoT market because many IoT-related functions also fit into wider digital transformation initiatives. For instance, the traditional transaction of buying power from an electricity company has been altered by home generation using renewables which is also sold back to the grid.

This has resulted in connected utilities and smart grids that are managing different demand profiles caused by charging cars alongside different generation profiles caused by solar and wind generation. The growth in useful data alongside innovation in artificial intelligence and machine learning and advances in AI and machine learning will continue to increase the applicability and value of data analytics, uncovering additional use cases and functions that the IoT market can support. Scale and flexibility requirements means the IoT market is moving away from selling equipment and software to selling business outcomes as-a-service. The XaaS market provides the means to scale up rapidly, access the latest innovation and avoid capital intensive investment in hardware such as servers and IoT equipment.

The market is maturing away from requiring organizations to create IoT systems and processes themselves by buying everything from IoT modules, gateways, terminals and devices to providing these as-a-service. To an extent, IoT is practising what it preaches in terms of servitization and thereby lowering barriers to entry by identifying the goals of a use case or the enterprise and then assembling the combination of software and hardware necessary to make the business case operational.

As always, the market determines the success of failure of an IoT project, and the XaaS model matches the need to accelerate time-to-market but also to experiment and fail fast with limited commitment to hardware and services.

[1] https://www.gsma.com/iot/resources/gsmai-iot-revenue-2020/

X AS A SERVICE

IaaS

Infrastructure as a service (IaaS)
A form of cloud computing that provides virtualized computing resources over the internet.

MaaS

Management-as-a-Service
The management of a network and systems, presented to the client in a web interface. In a sense, it's a specialized version of SaaS, where the first "S" involved is management software.

PaaS

Platform as a service (PaaS)
A cloud computing model in which hardware and software tools are delivered to users over the internet.

SaaS

Software as a Service
A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.

Servitization

Describes industries using their products to sell an outcome as a service, usually for a recurring subscription, rather than as a one-off sale of a product.

CONNECTED MOBILITY

ECU

Electronic Control Unit
A generic term for any embedded system that controls one or more of the electrical system or subsystems in a transport vehicle.

ITS

Intelligent Transportation Systems
Advanced applications which (without embodying intelligence as such) aim to provide innovative services relating to different modes of transport and traffic management, and enable various users to be better informed and make safer, more coordinated, and "smarter" use of transport networks.

CONNECTED LOGISTICS

Barcode

A machine-readable code in the form of numbers and a pattern of parallel lines of varying widths, printed on a commodity and used especially for stock control.

Cold chain

An unbroken cold chain is an uninterrupted series of refrigerated production, storage and distribution activities, along with associated equipment and logistics, which maintain a desired low-temperature range.

EDI

Electronic data interchange
The transfer of structured data from one computer application to another by electronic means and with a minimum of human intervention. It also describes the electronic exchange of documents between businesses and organizations including government agencies.

Fleet management

A function which allows companies to remove or minimize the risks associated with vehicle investment, improving efficiency, productivity and reducing overall transportation and staff costs (see also Fleet management in the mix of a great and complex IoT ecosystem)

CONNECTED MANUFACTURING

AMI

Advanced Metering Infrastructure
A digital architecture that allows for two-way communication between a smart meter and a provider, by way of an IP Address.

AMR

Automatic Meter Reading
The technology of automatically collecting consumption, diagnostic, and status data from water meter or energy metering devices and

transferring that data to a central database for billing.

BOM

Bill of Materials
A comprehensive list of parts, items, assemblies and other materials required to create a product.

CAD

Computer-Aided Design
A technology that designs a product and documents the design's process. CAD may facilitate the manufacturing process by transferring detailed diagrams of a product's materials, processes, tolerances and dimensions with specific conventions for the product.

CONNECTED UTILITIES AND SMART GRIDS

A utility supply network that uses digital communications technology to detect and react to local changes in usage.

CPS

Cyber physical production systems

Systems that connect physical and digital entities are connected, monitored and managed with computer programming and algorithms.

ERP

Enterprise Resource Planning
The integrated management of core business processes, often in real-time and mediated by software and technology.

Industry 4.0

A name given to the current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of things, cloud computing and cognitive computing. (see also IoT trends in industrial manufacturing)

JIT

Just In Time
An inventory management method whereby materials, goods, and labor are scheduled to arrive or be replenished exactly when needed in the production process.

Kanban

A visual system for managing work as it moves through a process. Kanban visualizes both the process and the actual work passing through that process.

MES

Manufacturing Execution System
An information system that connects, monitors and controls complex manufacturing systems and data flows on the factory floor.

PLM

Product Lifecycle Management
The process of managing the entire lifecycle of a product from inception, through engineering design and manufacture, to service and disposal of manufactured products.

QMS

Quality Management System
A formalized system that documents processes, procedures, and responsibilities for achieving quality policies and objectives.

Smart factory

A broad category of manufacturing with the goal of optimizing the manufacturing process.

Smart manufacturing

Describes an environment in which computers are in charge of decision-making. In a smart manufacturing environment, physical and digital are connected and communicate with one another to improve production.

Smart meter

A meter in a house or building that measures electricity, gas, or water consumption. It is termed 'smart' because it responds to usage and will increase or decrease flow according to the general consumption data from the utility company as well as the individuals within the building.

IOT SECURITY

What are the IoT security risks, considerations and issues for 2021?

With IoT now part of everyone's lives, our things are connected to each other and centralized systems via networks but these are all at risk from weak IoT security which threatens the security of users' and organizations' data, leaving them open to threats from malicious actors. The IoT industry has been fighting back for many years by enabling IoT security tools that protect devices and systems from threats and breaches.

IoT security risk can be mitigated by identifying and monitoring common threats before they become reality, helping to protect availability, integrity and confidentiality. Even so, cybercrime continues to grow with IoT deployments under threat from weak passwords and facing IoT security issues caused by the radically enlarged threat surface of IoT. We have seen examples such as tire pressure monitors being used to hack into vehicle systems or even a connected fish tank pump being used as a means to access financial systems at a Las Vegas Casino.

IoT security awareness is high and continuing to increase but this can also be damaging to the market place and decrease trust in IoT. Many organizations are therefore focusing on fixing vulnerabilities and helping to foster confidence by detailing best practice and conforming to various legislation and regulation initiatives that are being developed specifically for IoT across the world.

As IoT device numbers scale up further, the risk profile becomes higher. We have already seen the 2016 Mirai botnet attach on more than half a million unsecured IoT devices around the world which caused a flood of traffic and made many websites temporarily inaccessible. The scale of this attack underscored the need to address IoT security issues by ensuring their integrity and confidentiality while mitigating security risks.

Organizations that deploy IoT face substantial security risks as criminal target their operations, utilizing ransomware attacks to extort payments. Checkpoint Research has uncovered that the average number of daily ransomware attacks increased by 50% in Q3 of 2020 in comparison to the first half of 2020[1].

Organizations such as GSMA have published IoT security guidelines and in California and Oregon in the US, as well as in the UK, IoT Cybersecurity Laws have been put in place since 2020 which require IoT devices sold in their countries to be fitted with reasonable security features. These include having unique password, offering regular security updates and disclosing vulnerabilities.

The concept of integrating IoT security by design is now well understood and a vital consideration for devices that will be in the field for up to 20 years. This lifecycle means that security must be easy to update regularly and offer flexibility to counter new threats. Lifecycle management of device credentials, cryptographic keys, software patches and upgrades, and digital certificates are fundamental foundations of a new era of enhanced IoT security.

[1] https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/

IOT AND DATA SECURITY

Botnet

A network of private computers infected with malicious software and controlled as a group without the owners' knowledge.

GDPR

General Data Protection Regulation
This came into force in May 2018 and imposes rules on controlling and processing personally identifiable information.

IPSec

A secure network protocol suite that authenticates and encrypts the packets of data sent over an internet protocol network. IPSec uses cryptographic security services to protect communications over IP networks.

ICS

Industrial control systems
A collective term used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate or automate industrial processes.

IAM

Identity and access management
A framework for business processes that facilitates the management of electronic or digital identities.

NIST

National Institute of Standards and Technology
US regulatory body NIST has offered frameworks for IoT security and Congress passed the IoT Cybersecurity Improvement Act in December 2020. It also requires NIST to publish standards and guidelines on the use and management of IoT devices.

PAM

Privileged Access Management
Organizations implement privileged access management (PAM) to protect against credential theft and privilege misuse. PAM describes a comprehensive cybersecurity to control, monitor, secure and audit all human and non-human privileged identities and activities across an enterprise IT environment.

PKI

Public Key Infrastructure
A set of roles, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. PKI is a critical enabler of secure communication, data and money exchange.

TLS Transport Layer Security

(TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network.

Ransomware

Ransomware is a type of malware that extorts victims for financial gain. Once activated, it prevents users from interacting with their files, applications or systems until a ransom is paid.

Shadow IoT

Terms to describe IoT devices in active use without the knowledge of the owner or their IT departments.

TLS

Transport Layer Security
An encryption protocol used to protect data in transit between computers enabling two computers to agree to encrypt the information in a way they both understand.

Zero Trust

Describes a security model designed to protect digital businesses. Zero Trust sets out that organizations should not automatically trust anything regardless of whether it is outside or inside their operation. Zero Trust demands that everything trying to connect to your systems must be verified before access is granted.

TRACKING AND IDENTIFICATION

IMEI

International Mobile Equipment Identity (IMEI)
A unique identification or serial number that all mobile phones and smartphones have. It is normally 15 digits long.

International Article Number / EAN

A barcode symbology and numbering system used in global trade to identify a specific retail product type, in a specific packaging configuration, from a specific manufacturer.

MEID

Mobile Equipment Identifier
A globally unique number identifying a physical piece of CDMA2000 mobile equipment.

RFID

Radio Frequency Identification
RFID devices are used for data transmission and capture by way of radio waves.

Smart label

An enhanced version of a bar code. Unlike traditional bar codes, a smart label can contain much more information about a product. Smart labels take the shape of RFID tags, Electronic Article Surveillance (EAS) tags, or the most commonly seen, QR codes

UID

Unique Identifier
A number given to any device within any system to allow the ability to interact with it.

URI

Uniform Resource Identifier
A string of characters that unambiguously identifies a particular resource.

IOT INDUSTRY ORGANIZATIONS

3GPP

3rd Generation Partnership Project is a collaborative project established in 1998 aimed at developing globally acceptable specifications for third (and future) generation mobile systems.

AECC

Automotive Edge Computing Consortium
An organization focused on driving the network and computing infrastructure needs of automotive big data.

IEEE

The Institute of Electrical and Electronics Engineers
Describes itself as the "world's largest technical professional society." It aims to promote standardization through international electronics development.

ITU

International Telecommunications Union
The United Nations specialized agency for information and communication technologies – ICTs. The ITU allocates global radio spectrum and satellite orbits and develops the technical standards that ensure networks and technologies seamlessly interconnect.

GSMA

The GSM Association represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in adjacent industry sectors. The GSMA organizes the largest annual event in the mobile industry, the GSMA Mobile World Congress.

W3C

The World Wide Web Consortium is the main international standards organization for the World Wide Web (abbreviated WWW or W3).

telenor IoT

TELENOR CONNEXION

Telenor Connexion is the specialized IoT company within the Telenor Group, one of the world's major mobile operators. Building on more than 20 years of experience, Telenor Connexion provides global IoT connectivity and cloud services to enterprises with large fleets of connected devices as well as third-party service providers.

Telenor Connexion manages more than 10 million connected things in more than 190 countries for global customers including Volvo, Scania, Hitachi, Verisure Securitas Direct and Husqvarna. With headquarters and tech centre located in Sweden, the company has regional sales representation in the UK, US, Germany, Italy, South Africa, Singapore, South Korea, China, and Japan.

telenorconnexion.com

✉ sales@telenorconnexion.com