IoT Alliance Australia

IoT REFERENCE FRAMEWORK

APPLICATION GUIDE

IoT Reference Framework – Application Guide v1.0

September 2018

IoT Reference Framework v1.0

This *Guideline* was developed by Enabler Workstream #3 (eWS-3) – Cyber Security and Network Resilience of the IoT Alliance Australia (IoTAA) – http://www.iot.org.au/

Disclaimers

1) Notwithstanding anything contained in this *Guideline*:

a) Internet of Things Alliance Australia, (IoTAA) disclaims responsibility (including where IoTAA or any of its officers, agents or contractors has been negligent) for any direct or indirect loss, damage, claim or liability any person may incur as a result of any:

i) reliance on or compliance with this *Guideline*;

ii) inaccuracy or inappropriateness of this *Guideline*; or

iii) inconsistency of this *Guideline* with any law; and

b) IoTAA disclaims responsibility (including where IoTAA or any of its officers, agents or contractors has been negligent) for ensuring compliance by any person with this *Guideline*.

2) The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

IoT Reference Framework – Application Guide v1.0

September 2018

TERMS OF USE

The IoT Reference Framework is available for non-commercial use by organisations and individuals, for purposes such as for communications, IoT architecture references, documentation, capability assessment, etc.

The use of this IoT Reference Framework for commercial purposes, such as marketing, advisory services, creating tools, etc. for financial gains are not permitted, and subject to IP licensing.

Please contact INFYRA if you want to use this IoT Reference Framework for commercial purposes.

IoT Reference Framework – Application Guide v1.0

September 2018

INTRODUCTORY STATEMENT

The Internet of Things (IoT) Reference Framework is a general guide, with the intention that it be adopted for a range of purposes. The IoT Alliance Australia (IoTAA) has already adopted this IoT reference framework for the following purposes:

- As a foundational input to the development of an IoT Security Framework application

As a reference in the following guidelines:

- IoT Security Guideline, by Enabler WS#3
- IoT Platform Selection Guideline, by WS#4

This document provides an overview of the IoT Reference Framework, as well as showing how it could be adopted for a number of different purposes.

Matt Tett

Chair

Enabler Workstream #3 (eWS-3) – Cyber Security and Network Resilience, IoT Alliance Australia (IoTAA)

September 2018

1 GENERAL

1.1 Background – The requirement for a new framework

The Internet of Things continues to drive "smart" innovation in many industry sectors including: cities, utilities, agriculture, transportation, homes and healthcare. The uptake of IoT in so many sectors and aspects of our lives means that the participants in an IoT ecosystem are extremely diverse: from low technical literacy to very high; from manufacturers and developers of the technology to users, including individual consumers and company executives. There is a need for a common framework and language that enables this diverse array of participants to discuss important aspects such as security, privacy, safety, maintenance and interoperability across all sectors and user types from consumers to industry. It is only through a common language and framework that the participants in the IoT ecosystem will be able to understand their role and accountability in these aspects.

An internet search for IoT Reference Architectures returns many different IoT Reference Architectures. These IoT Reference Architectures tend to fall into one of two categories. Either they are quite narrow in their scope because they are vendor-specific or limited to a single implementation/solution, therefore making it difficult to translate to other implementations or industries. Alternatively, they are too high-level, over-simplified or conceptual in nature, therefore making it difficult for users to have a sufficiently detailed conversation on real world application aspects such as security, privacy, safety or operability to determine responsibilities.

The IoT Reference Framework, shown in Figure 1, bridges that gap. It is a framework, rather than an architecture, which is straight forward, vendor-neutral and self-explanatory. The framework presents generic building blocks that are common for all IoT solutions. Organisations can use the framework, as their reference building blocks to design their own solution architecture.

1.2 Attributes and Purpose

The attributes of the IoT Reference Framework are:

- a common terminology (which we call 'language') for describing the elements of an IoT ecosystem; and
- a layered structure that enables an IoT ecosystem to be viewed from different perspectives (which we call 'lenses').

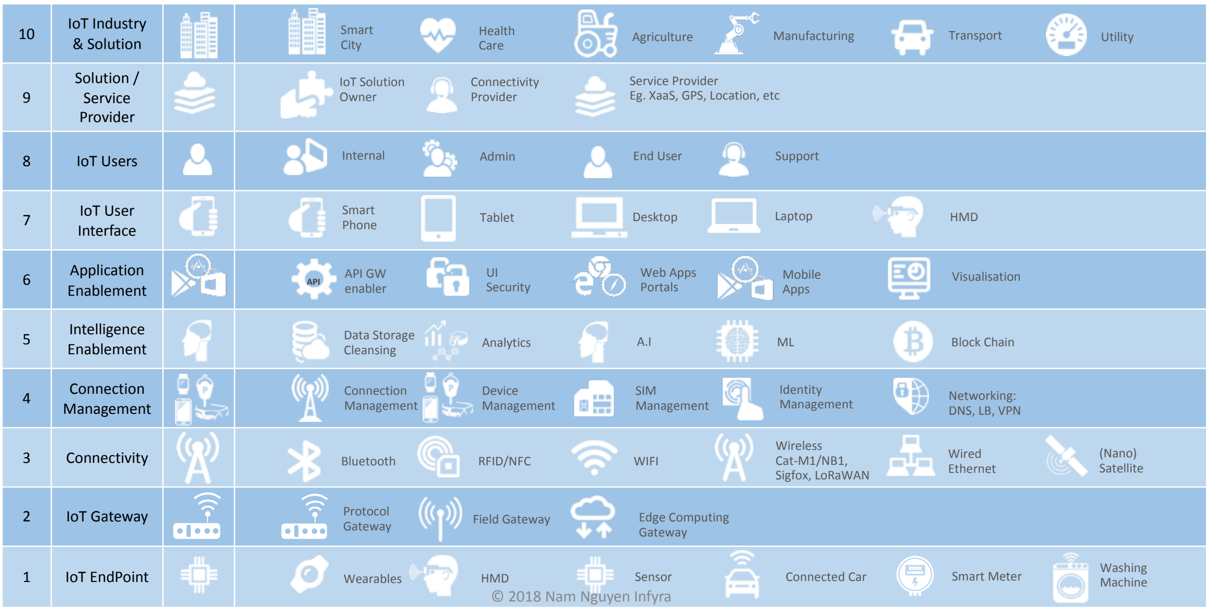
The attributes of the IoT Reference Framework enables participants in the IoT ecosystem develop an understanding of the ecosystem and their role(s) in aspects such as security, reliability, privacy, safety, maintenance, and so on.

As such, the purpose of the framework is to enable:

- clear identification of relationships between participants in the IoT ecosystem so accountability can be understood and assigned;
- implementation of IoT solutions in a timely manner as all necessary components/layers can be identified upfront; and to
- ensure security, privacy, safety, reliability and other aspects to be 'placed front of mind' from solution conception, rather than being added as an afterthought.

1.3 The Framework

Figure 1 illustrates the framework's 10 layers with layer 10 'IoT Industry and Solution' at the top, and layer 1 'IoT Endpoint' at the bottom.



10	IoT Industry & Solution	Smart City	Health Care	Agriculture	Manufacturing	Transport	Utility
9	Solution / Service Provider	IoT Solution Owner	Connectivity Provider	Service Provider Eg. XaaS, GPS, Location, etc			
8	IoT Users	Internal	Admin	End User	Support		
7	IoT User Interface	Smart Phone	Tablet	Desktop	Laptop	HMD	
6	Application Enablement	API GW enabler	UI Security	Web Apps Portals	Mobile Apps	Visualisation	
5	Intelligence Enablement	Data Storage Cleansing	Analytics	A.I	ML	Block Chain	
4	Connection Management	Connection Management	Device Management	SIM Management	Identity Management	Networking: DNS, LB, VPN	
3	Connectivity	Bluetooth	RFID/NFC	WIFI	Wireless Cat-M1/NB1, Sigfox, LoRaWAN	Wired Ethernet	(Nano) Satellite
2	IoT Gateway	Protocol Gateway	Field Gateway	Edge Computing Gateway			
1	IoT EndPoint	Wearables	HMD	Sensor	Connected Car	Smart Meter	Washing Machine

© 2018 Nam Nguyen Infyra

Figure 1 – IoT Reference Framework

1.4 Framework Layer Description

Layer	Function	Intention
10	**IoT Industry Sector & Solution**	IoT industry sector, demonstrates where an IoT solution is part of a bigger ecosystem. The purpose of emphasising IoT solutions and their respective industry sectors is to provide the IoT solutions with context including local laws, regulations, compliance, security, procurement, data privacy, safety, critical infrastructure, etc.
9	**IoT Solution / Service Provider**	Highlights the relationship and collaboration between IoT solution owner/operator and the stakeholders that provide services, or products to the solution.
8	**IoT User**	Details who the real customers are, or who are the main beneficiaries of the solution. An IoT solution could have multiple types of users, and each type of user can have a different usage or consuming requirements.
7	**IoT User Interface**	Refers to the method and means by which users or operators access the solution outcomes (information, data, business intelligence, etc).
6	**Application Enablement**	A set of functions that are often grouped under the broad umbrella term *IoT Platform*, used to describe many IoT core functions including: API gateway, database storage, visualization, device management, application server and more. Because the definition of *IoT Platform* can mean many different things in different contexts, this framework deliberately separates the 'IoT Platform' into three layers; Application Enablement, Intelligence Enablement and Connection Management.
5	**Intelligence Enablement**	Intelligence Enablement is used to provide further clarity around the term *IoT Platform*. It refers to the use of (emerging) technologies such as Analytics, Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL) which adds value through intelligent analysis of massive amount of data collected from the IoT devices and other external sources.
4	**Connection Management**	Connection Management refers to functions that manage connections of devices, device identity and device configuration.
3	**Connectivity**	Refers to different connectivity technologies used for communications between field sensors/devices and core IoT functions described in layers 4, 5 and 6 above.
2	**IoT Gateway**	A field gateway, or protocol gateway that aggregates data from individual sensors/endpoints, before being sent off to a centralised server/IoT platform.
1	**IoT Endpoint**	Ranging from simple sensors, to more complex, stand-alone devices such as tracking devices, smart meters, etc. to embedded devices in complex systems such as those in control systems, autonomous vehicles, and so on.

1.5 Intended Audience

This IoT Reference Framework can be adopted by anyone in the IoT community below, who might be able to use the Framework for their own purposes[1]

- IoT hardware and system vendors
- IoT solution developers and integrators
- IoT service providers
- IoT device developers
- IoT users
- Local, state and federal governments
- Commercial businesses and enterprises

1.6 Examples

Example 1. A municipal council, wanting to save on street lighting costs, is looking to implement an IoT based smart street lighting solution.

In this example, the municipal council is the service provider (layer 9). The council, as the solution owner, is prompted to consider the layers below to identify:

- Users (layer 8) of both the IoT system, including both staff at the council who access the IoT platform to obtain performance data (e.g., electricity usage) and control the system, as well as the 'users' of the streetlights themselves, such as pedestrians and vehicles at night;
- The user interface (layer 7) is the interface through which users access the system. It is important to consider all users, some of whom will have higher levels of more secure access (i.e., administrators) and which may be on-line (to permit access by the general public to see performance data) and may also include a need for mobile device (small screen and mobile) access;
- The application (layer 6) on which the solution is implemented such as the physical or virtual platform, where it is important to identify aspects such as security and visualization;
- The intelligence (layers 5 and 4) or core of the solution that including data storage, analytics, artificial intelligence (AI), or Machine Learning; and
- The connectivity and other physical infrastructure including the IoT devices themselves (layers 3, 2 and 1).

Importantly, the framework also prompts the council to look up the stack and identify that as the owner of a smart-lighting system, they may also be part of a larger ecosystem such as a smart city (layer 10).

Using the framework, the council can clearly identify stakeholders and their responsibilities in the planning, building, and operating of the smart street lighting solution. It also helps the council have conversations with suppliers at each layer on security, reliability, resilience, privacy and safety.

[1] Refer to the IoT Reference Framework's Terms of Use

Example 2. A manufacturer of an IoT gateway that could be used in a variety of applications to aggregate sensor data from energy or water sensors

In this example, the manufacturer makes the IoT gateway that is at layer 2 of the Reference Framework.

Like the council, the manufacturer is prompted to consider the layers above and below, and to recognise that there are more than just the immediately adjacent layers (layers 1 and 3).

The manufacturer needs to consider that their gateway will bring information from IoT Devices back to the IoT platform, where intelligence is added. Importantly, the gateway manufacturer needs to consider that there will be an array of users, often broader than the just the solution owner, and that the IoT data being gathered may be used in a context larger than the immediate application.

Like the example above, the Reference Framework helps the gateway manufacturer consider all the layers and have conversations with the people responsible for each layer on aspects such as security, reliability, resilience, privacy and safety.

2 DEFINITIONS AND INTERPRETATIONS

2.1 GLOSSARY AND TERMINOLOGY

The following terms have special meanings within the context of the Scheme.

Actor

Either an organisation or an individual who plays a role at any layer in an IoT Ecosystem or Solution.

Architecture

Architecture refers to the functions or features, and the relationship and interfaces of these functions within and external to a system, without ties to implementation aspects such as quantity, location, capacity.

Communications Protocols

These refer to the protocols used to transport data from IoT endpoints to IoT backend. When referring to protocols. Examples of protocols referred to in this document include: MQTT, CoAP, HTTP, Websocket, AMQP, etc.

Connectivity Technologies

Refers to an IoT ecosystem, ie. Network, which plays a role in connecting IoT endpoints to backend systems such as IoT platform, or gateway. Examples of Connectivity technologies include Cellular, LPWAN, Bluetooth, RFID, etc.

Industry Sector

Refers to the specific industry vertical where IoT plays a role. For example, Agriculture, Smart manufacturing, Smart Cities, Smart Transport are some examples of industry sectors.

IoT Endpoint

GSMA define [REF10] an IoT Endpoint as "*An Endpoint, from an IoT perspective, is a physical computing device that performs a function or task as a part of an Internet connected product or service*." For example, an IoT Endpoint could be a wearable fitness device, an industrial control system, an automotive telematics unit or even a personal drone unit.

IoT Platform

A multi-layer technology stack, with functions described in layers 4, 5 and 6 in this reference framework, that connects IoT endpoints to IoT users, other IoT endpoints, the internet, business and operational systems. It enables connectivity, management, provisioning, and security of endpoints and solutions. It allows solutions to scale smoothly and adds smartness to the IoT solution.

IoT platforms, or the functions of layers 4, 5 and 6, are commonly implemented in centralised physical servers, such as cloud platform, or on-premise. Certain functions could also be implemented closer to IoT endpoints, on what is referred to as Edge Platform, or Computing.

IoT Reference Framework

A broad outline of an IoT Ecosystem or Solution, which serves as a reference guide to enable actors to use a common language and layered structure to discuss aspects related to the solution such as security and privacy.

IoT Solution / Service Provider

Refers to vendors who sells solutions, or provide services such as solution integration, XaaS providers, software vendors, etc.

Lens

A view through the IoT ecosystem (perhaps vertically through the layers, or horizontally across a layer) to enable users of the IoT Reference Framework to see the solution from different perspectives, such as security, privacy, resilience, reliability, safety and so on.

3 FRAMEWORK DESCRIPTION

The IoT Reference Framework is a 10-layered model, and in the following sections, each layer is explained to provide some guidance as to how the framework could be further expanded to suit an organisation's particular need. In the description below, we use the term ***actor*** to describe either an organisation or an individual who plays a role at any layer in the IoT Reference framework.

Following the description of the layers in this section, section 4 then provides detailed of how the IoT Reference Framework could be adopted to help business prepare for, and deploy IoT solutions.

3.1 LAYER 10 – INDUSTRY SECTORS & SOLUTIONS

Understanding the industry environment

Layer 10 invites actors to look at the industry sector their IoT solution belongs to in order to determine whether there are any specific laws, regulations or other obligations they must comply with.

Take the example of an IoT solution to enable an energy service provider to buy and sell electricity from other suppliers, individuals, corporates, or other service providers. Layer 10 encourages the solution owner (the actor at level 9) to consider the solution's compliance with laws and regulations specific to that industry such as critical infrastructure legislation by considering the security measures that need to be taken into account to protect the critical infrastructure from being exploited. However, layer 10 does more than just encourage the solution owner to consider their own industry. For example, if electricity is being obtained from residential properties (individuals), layer 10 also encourages the solution owner to consider aspects such as privacy and safety and compliance with laws and regulations that transcend the specific industry the IoT solution was developed in.

Extending the analogy, Layer 10 not only encourages the actor at Layer 9 (the solution owner) to consider the broader industry and environment, but it also encourages every actor in the solution through all the layers down to layer 1 to consider the solution's compliance with laws and regulations specific to that industry, as well as laws and regulations more broadly outside the industry.

Contextual information relevant to an IoT solution could encompass social, economic, safety, security, legal and regulatory environment, and how these could affect, and/or dictate the design of an IoT solution.

Some of the ***contexts*** (not exhaustive) that should be considered are shown in Table 1 below.

Industry Context	**Considerations for the IoT solution**
Market	Identify and understand the overall market in which the IoT solution will operate in (e.g., street lighting is part of a Smart City).
Regulatory	Industry specific rules, regulations and compliances. For instance, if the solution operates in an industrial environment, or is a social one such as the health, or disability sector.
Security	Essential for all IoT solutions across all industries. Additional levels of security may be required if the solution deals with sensitive data, and or operates within a national security and/or critical infrastructure space.
Data Privacy	Consumer rights and privacy laws are amongst the key concerns for everyone, and that can also vary from country to country. Regulation on Data Protection is being enforced across many countries.
Safety	An important operational aspect of any IoT solution is to provide a safe product and environment for the people who are operating, and users of the solution. Ensuring that the solution fails "safe" is also a critical requirement.
Social/ Environmental	Social implications and environmental impacts need to be considered.
Time	The period and time to which a solution would be relevant, including the end-of-life and maintenance of security, privacy and safety throughout the lifecycle.
Scale/Size	Volume and scale that would create momentum, or aid efficiency.

Table 1 | Industry and Solution Context

3.2 LAYER 9 – SOLUTION / SERVICE PROVIDER

The business environment

Layer 9 invites the solution owner and/or service providers (along with actors at other layers) to look at the business environment to identify stakeholders of the IoT solution in order to ensure business readiness. Further, not all stakeholders will be direct employees of the business, as stakeholders may include external suppliers.

Stakeholders are anyone that may play a role in the solution, such as Solution Owner/Operator (business, enterprise and government), parts of the business responsible for process design and product implementation, IT department, risk management, privacy and security functions. Stakeholders may also be external service providers such as device developer/supplier, network provider, platform and application providers.

With multiple stakeholders involved, a solution can present complexity that needs careful management. IoT solutions are generally built up from multiple systems and require collaboration from multiple parties.

Understanding the roles and responsibilities of each stakeholder in the solution will equip the business with the knowledge to select the right ecosystem partners.

For instance, knowing the stakeholders and their roles in the solution ecosystem helps the business owner identify challenges such as:

- Who will design, or supply my IoT devices, and in the long run supporting them?
- How will IoT security and data privacy be planned and coordinated through multiple ecosystem partners?
- Is my business operation set up to deal with multiple partners?
- How will I protect sensitive data from collection points, through to transport, storage and usage points throughout the solution ecosystem?

Business Readiness – A second important perspective of layer 9 is business readiness. Here, the solution owner is encouraged to consider aspects of the solution necessary to operate an IoT-enabled business. Business readiness includes business process transformation, staff training, operational procedures, customer support, etc.

3.3 LAYER 8 – IOT USER

Internal and external users

Layer 8 identifies the types of IoT users who interact, either directly or indirectly, with the IoT solution.

The intention of this layer is to help the IoT solution/business owner clearly identify who their real customers are, and what problems they face, and how the solution will solve their problems.

Understanding all the users also enables an organisation to identify how their solution can meet different user requirements. A solution may be designed to meet one specific group of users, but it could also be designed to meet a diverse group of users, in which case, their user requirements and expectations could be very difficult to satisfy.

3.4 LAYER 7 – IOT USER INTERFACE

Accessing your IoT solution, including on-the-go

IoT User Interface (UI) is intended to highlight how users of the IoT solution will access it.

In most cases, commercially available access devices such as smart phones, PC or laptop, are the default choice, however, they are not the only type. Emerging devices such as Headset Mounted Displays (HMDs) used in VR/AR applications, or home devices such as Google Home, Amazon Alexa, or Apple Homepods may also be considered. In certain industrial cases, a UI might have to be completely customised due to specific requirements for the solution.

Importantly, this layer emphasises the importance of mobility as a UI consideration. If the ability to access the IoT solution from mobile devices is necessary, then it is likely that a cloud-hosted solution is required with connectivity over the internet. Again, the user of the IoT Reference Framework is prompted to consider aspects such as privacy, security, reliability, resilience and safety.

This layer also prompts users of the IoT Reference Framework to consider aspects such as User Experience Design, to ensure that users of the system can access the IoT solution (for information or control) in a format that is readily useable from the relevant access device.

3.5 LAYER 6 – APPLICATION ENABLEMENT

Bringing it all together

One of the most important aspects of an IoT solution is the ability for an organisation to 'operate and manage' their IoT solution and devices through a diverse range of activities including: device connection management, data storage and processing, event monitoring and handling, analytics, and interfaces to external systems.

Many adopters of the IoT Reference Framework will likely consider this range of functions as the actions performed by an IoT Platform. However, the authors consider that the term IoT platform creates a risk that the user of the IoT Reference Framework only considers physical hardware, thereby inadvertently overlooking the full range of activities captured by this layer, including the use of virtual (cloud hosted) platforms and the range of foundational services in the IoT solution such as data storage, device data, data analytics, application building, etc.

For this reason, the IoT Reference Framework instead approaches this set of function by defining three groups of functions, described as Layer 6 – Application Enablement, Layer 5 – Intelligence Enablement, and Layer 4 – Connection Management.

Applying the IoT Reference Framework's approach, together with a solid understanding of the business criteria for introducing an IoT solution, when selecting an IoT Platform, can help organisations:

- Understand the business functions that are needed to leverage the IoT solution for business purposes;
- Benchmark and compare the differences between IoT platforms from different vendors;
- Ask the correct questions regarding features, security, implementation, future product roadmap, interoperability, etc;
- Deploy IoT solution cost effectively;
- Scale solution smoothly with growth;
- Provide low-level device control and operations such as communications, device monitoring and management, security, and firmware updates;
- Enable IoT data acquisition, transformation and management; and
- Facilitate IoT application development, including event-driven logic, application programming, visualization, analytics and adapters to connect to enterprise systems.

3.6 LAYER 5 – INTELLIGENCE ENABLEMENT

Obtaining insights

Key to all IoT solutions is the vast amount of data generated from IoT endpoints. The biggest challenge for organisations is how to turn this data into intelligent, actionable information that makes an IoT solution a truly smart solution.

Intelligence, or 'smart enablement' refers to the use of smart technologies across data to analyse, cross reference, observe behaviour and patterns, learn and predict, in order to produce insightful outcomes, and to drive smart actions.

Blockchain and Artificial intelligence (AI) along with its learning techniques like Machine learning (ML) and Deep Learning (DL), enable smart IoT solutions.

Artificial Intelligence and Machine Learning

The key value of AI and ML are their ability to quickly derive insights from data. Some examples of value are:

Avoiding Downtime – ML can help identify patterns from the constant stream of data to predict equipment failure, or unusual behaviour. For example, if a percentage of smart water meters are reporting abnormal data readings, ML can identify unusual patterns and recommend appropriate action(s) to investigate, including looking for leaks or investigating whether the meters have been tampered with.

Increased Operational Efficiency – AI can be used to predict operating conditions and identify parameters that could be optimised to maintain ideal outcomes.

Emotional analysis and facial recognition – AI has been used to provide facial and emotional analysis in a number of places for safe city purposes.

New and Improved Products and Services – designing IoT solution with AI components can also improve existing products and services or pave the way for the creation of new ones. For example, AI-powered drones can be used for monitoring and inspection in sectors such as mining or agriculture, including in previously inaccessible places for humans.

Cybersecurity and risk – AI can be used to predict potential risks, as well as to enable automated, rapid response. This would lead to better management of worker safety, mitigate financial loss, and reduce cyber threats.

Blockchain

The underlying value of blockchain is that the technology allows a Trusted Environment to be created. According to IBM [REF5], there are three benefits of using blockchain for IoT:

1. Greater transparency, which builds trust between devices and parties;
2. Enhanced security because the distributed ledger technology makes it very difficult for hackers to compromise the transaction data;
3. Improved traceability as the blockchain is its own audit trail;
4. Increased speed and efficiency, by enabling secure and instantaneous transactions; and
5. Reduced costs through streamlining operations by reducing overheads associated with intermediaries.

The question that an organisation should ask is whether blockchain is appropriate for the IoT application/solution. Understanding the technology and the potential value that blockchain can bring to IoT applications and products is the first step.

Most IoT Platform vendors now offer AI and blockchain capabilities in their platform, making these technologies more accessible.

3.7 LAYER 4 – CONNECTION MANGEMENT

Scale and security

An important set of functions for any IoT solution is the ability to manage device connection in a scalable and secure manner. This requires the solution to consider the need to possibly support a range of communications protocols in order to enable low level device configuration and provide identity management.

There are quite a number of connection management functions, which are widely supported by service providers. More details can be found in Appendix C.

Assessing connection management functions in layer 4 should be done as part of an overall strategy, and in particular, work in conjunction with devices (layer 1), and connectivity choice (layer 3).

3.8 LAYER 3 – CONNECTIVITITY

Coverage, mobility, cost and security

Layer 3 in the framework presents various options for network connectivity technologies that provide connection to IoT endpoints.

There are several classifications for connectivity technologies, including: wired connectivity, Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN) such as Wi-Fi, Low Power Wide Area Network (LPWAN) which is optimized for low powered IoT devices, and Wireless Wide Area Networks such as cellular based 3G and 4G networks. More details can be found in Appendix C.

Understanding the pros and cons of these technologies is one of the key factors that will help an organisation make correct decisions for their IoT business. Organisations can also use this framework to aid the assessment of the ecosystem that supports a particular technology.

Coverage Footprint and Mobility – where will your IoT devices be located? Will they be stationary or fixed in certain locations, or will they be mobile in large geographical areas? Will they only be in indoors or can they move outdoors? If the IoT device is portable, does it matter if there are time periods when it moves out of coverage?

Network Capacity – Will your connectivity network hit its capacity threshold (either number of devices, or bandwidth, or both)? Will it be possible to augment capacity if the capacity is reached?

Build or Buy – Do you want to build and operate your own connectivity network, or is it possible to obtain network connectivity from a service provider?

Power Consumption – Are your IoT devices battery powered? If yes, what is the expected battery life for your devices? How regularly does your device need to transmit? Is encryption used, and will the CPU power requirements increase due to this?

Bandwidth – What type of data your IoT devices will be sending, such as text, images or video? What is the frequency of transmission, e.g., minutes hours or daily?

Radio Network – Will you connect over public or private networks? Will the radio network use unlicensed (i.e., class-licensed) or licensed radio spectrum?

Other factors – Data packet size, encryption, real time triggering, downlink capability, bi-directional transmission, secured and acknowledgement of data transmit.

Connectivity technology consideration is not the only factor when making technology choice. It must be considered together with other business criteria. Organisations can engage expert help if they do not have in-house expertise.

3.9 LAYER 2 – IOT GATEWAY

Joining the endpoints

IoT Gateways are not always necessary, depending on the type of connectivity technology and/or the types of devices being used, as some devices will directly connect with the IoT platform.

Gateways are used for a number of purposes, and more detail can be found in Appendix C under Layer 2.

A gateway could be a field gateway, an aggregator/concentrator, a protocol conversion gateway, or an Edge Computing gateway, where the latter can also perform certain functions as specified in layers 4, 5 and 6.

3.10 LAYER 1 – IOT ENDPOINT

Obtaining the IoT data

The term IoT Endpoint is chosen as it can represent a number of things. An endpoint can be a single connected sensor, an actuator, or it can be a device such as a tracker or wearable device. It can also be part of a much more complex industrial system.

Different organisations will approach the procurement of IoT endpoints in different ways, either procuring individual IoT endpoints directly from manufacturers, or by outsourcing the design and development of their overall IoT solution, which will include IoT endpoint procurement.

Some of the key attributes that most organisations/consumers would look for in an IoT endpoint device are:

Power Consumption –Battery powered endpoints need to conserve power to ensure the longest possible battery life.

Technology/Comms Module – Different LPWAN technologies such as Sigfox, LoRaWAN, NB-IoT and Weightless, have different efficiencies in terms of protocol overhead (the amount of data in a communication that is not the actual payload) with implications for battery life.

Security – Often an afterthought, security must be designed in at the outset. For simple devices without much processing power, the ability to build in security features such as encryption is often limited. Encryption needs to be considered for all data, and may affect CPU processing power, bandwidth overheads and battery life.

FOTA – Firmware update Over The Air. For certain IoT applications, where there are tens of thousands (or more) devices out in the field, it is critical to have the ability to update firmware over the air.

Display-less – Many IoT endpoints do not have a display, which can make security and transparency more challenging.

Costs – The cost of the communications module, as well as the overall product (device) cost is an important consideration, especially for LPWAN devices.

4 APPLICATION GUIDE

This section provides a guide on how the IoT Reference Framework can be applied to enable businesses to prepare for and deploy an IoT solution.

4.1 Framework Viewpoints

IoT solutions, using this IoT Reference Framework, can be viewed through different lenses, by different audiences, for different purposes.

Four viewpoints are presented in Figure 3, Contextual, Business, User and Architectural/Implementation, which can be useful for an organisation when looking to introduce IoT solutions.

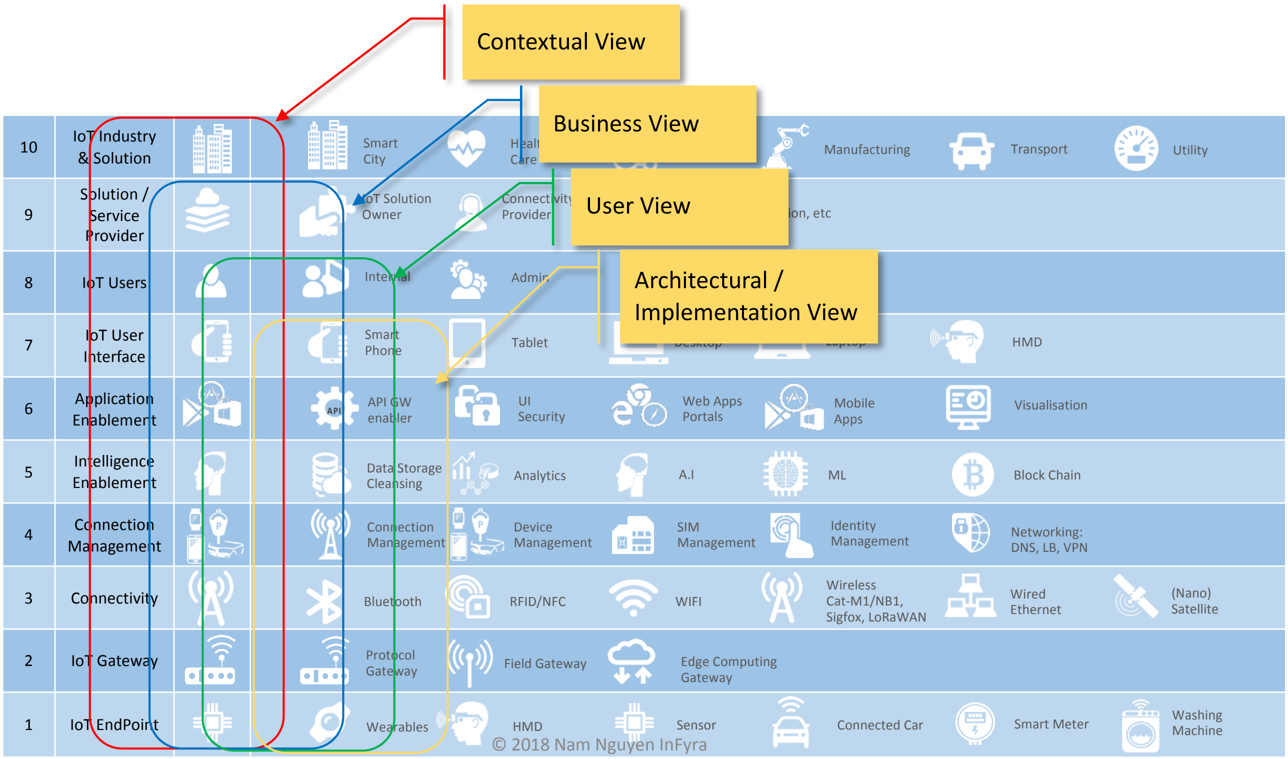


Figure 2 | *Solution Viewpoints – Using IoT Reference Framework*

Contextual View

The contextual view provides a complete picture of the industry, solution, ecosystem players and the technology used to deliver the solution. The contextual view enables a business to be well prepared for the development and operation of their IoT solution by allowing it to consider the regulatory environment that the business (and solution) operates within, along with aspects such as privacy, security and safety.

Business View

The business view focuses on business aspects of the solution, and includes stakeholders involved in implementation and operation of the solution, business processes, organisational capabilities and management of the solution, industry collaboration, legal and regulatory compliance, risks, cyber security compliance, strategy and processes.

User View

This viewpoint is useful to look at an IoT solution from a user's point of view. This will help the business and solution owner consider aspects such as customer experience, user access and security, authentication, and data privacy.

User view can include all segments: consumer, business, government, communities, service providers, ecosystem providers, developers, and so on.

Architectural/Implementation View

This viewpoint is most useful for technical purposes, where technical aspects of an IoT solution are considered, predominantly in layers 1 to 7 of the IoT Reference Framework.

Any IoT solution can be broken down into, or built up from, components that belong to layers 1 to layer 7.

The implementation view can:

- be used to visually represent an IoT solution building blocks; and/or
- drilled down to expand further on each layer to show network, architecture, function, interface, system, sub-system, and component views

4.2 Examples of Applications

Figure 3 illustrates a number of potential applications, shown as coloured wrap-around bands for different purposes. These applications can be developed using the IoT Reference Framework, as a foundational structure.

In the following sections, the purpose of each of these applications is explained.

Organisations can implement these concepts and/or develop their own to assist their IoT businesses, be it to communicate the IoT solution, plan their IoT project implementation, or to achieve better collaboration between ecosystem suppliers.

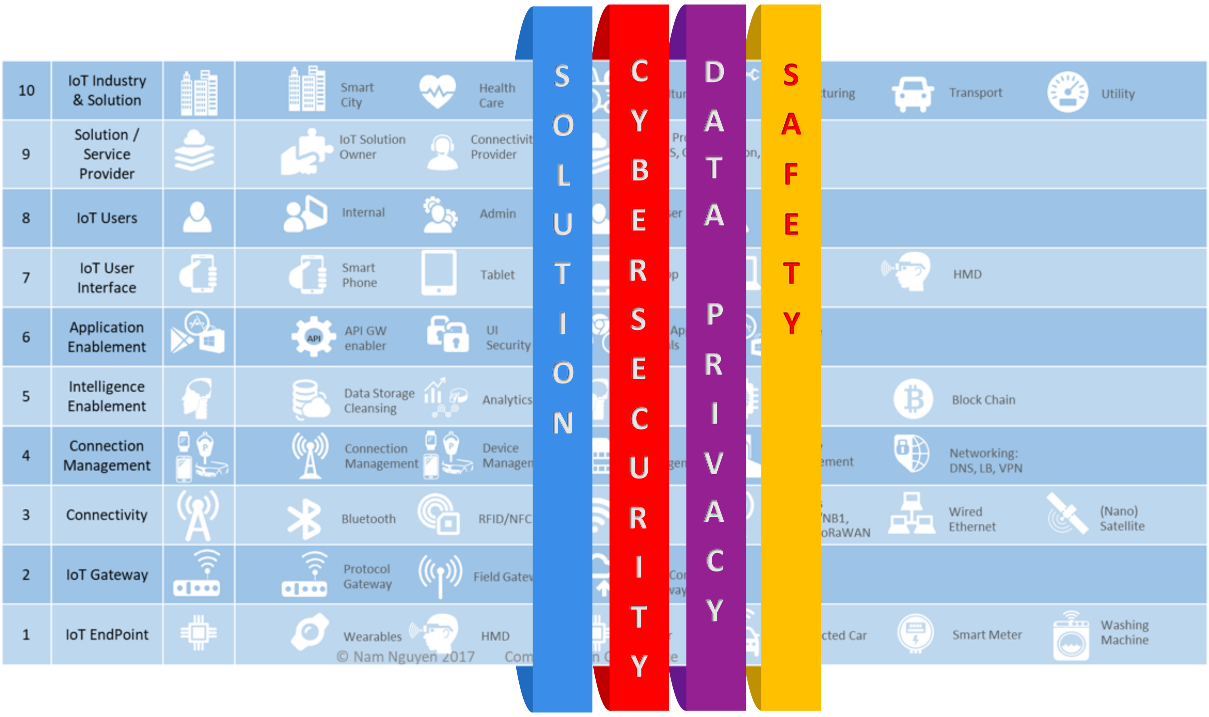
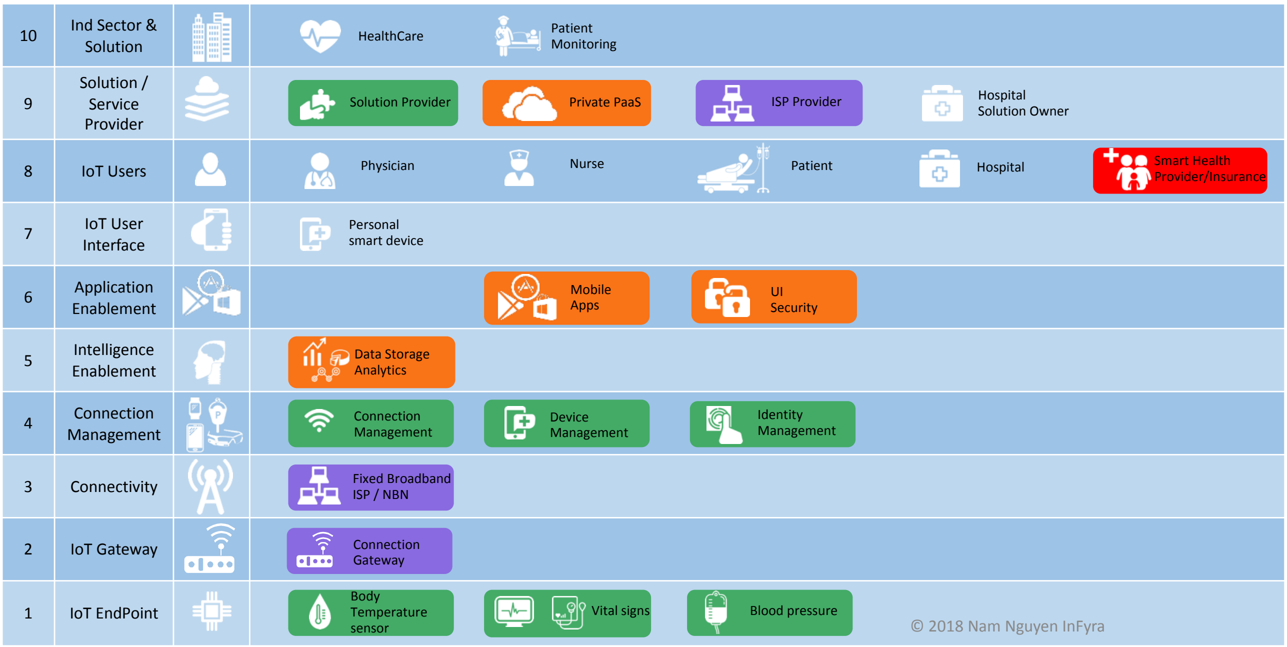


Figure 3 | *Examples of Applications of IoT Reference Framework*

Solution

The purpose of the IoT Reference Framework is to develop a common language and to identify the relationship between the various layers in an end-to-end IoT solution, in a simple and unambiguous way for all stakeholders. For example, the framework can be used to show a corporate executive a plain view of an IoT solution's building blocks, and the solution stakeholders, as seen in the example of a hypothetical solution in the healthcare sector in Figure 4 below.



10	Ind Sector & Solution	HealthCare	Patient Monitoring			
9	Solution / Service Provider	Solution Provider	Private PaaS	ISP Provider	Hospital Solution Owner	
8	IoT Users	Physician	Nurse	Patient	Hospital	Smart Health Provider/Insurance
7	IoT User Interface	Personal smart device				
6	Application Enablement		Mobile Apps	UI Security		
5	Intelligence Enablement	Data Storage Analytics				
4	Connection Management	Connection Management	Device Management	Identity Management		
3	Connectivity	Fixed Broadband ISP / NBN				
2	IoT Gateway	Connection Gateway				
1	IoT EndPoint	Body Temperature sensor	Vital signs	Blood pressure		

© 2018 Nam Nguyen InFyra

Figure 4 | *Example of an IoT Solution Building Blocks*

IoT Security

This framework can also be used to develop an end-to-end IoT cyber security strategy for a particular IoT solution.

Organisations can assess the security vulnerabilities of their IoT solution, by examining the security features (or lack thereof) of their IoT solution at each layer of the framework to see how security features are implemented end-to-end across the layers.

Figure 5 shows an example of how security can be approached by examining the solution using this framework.

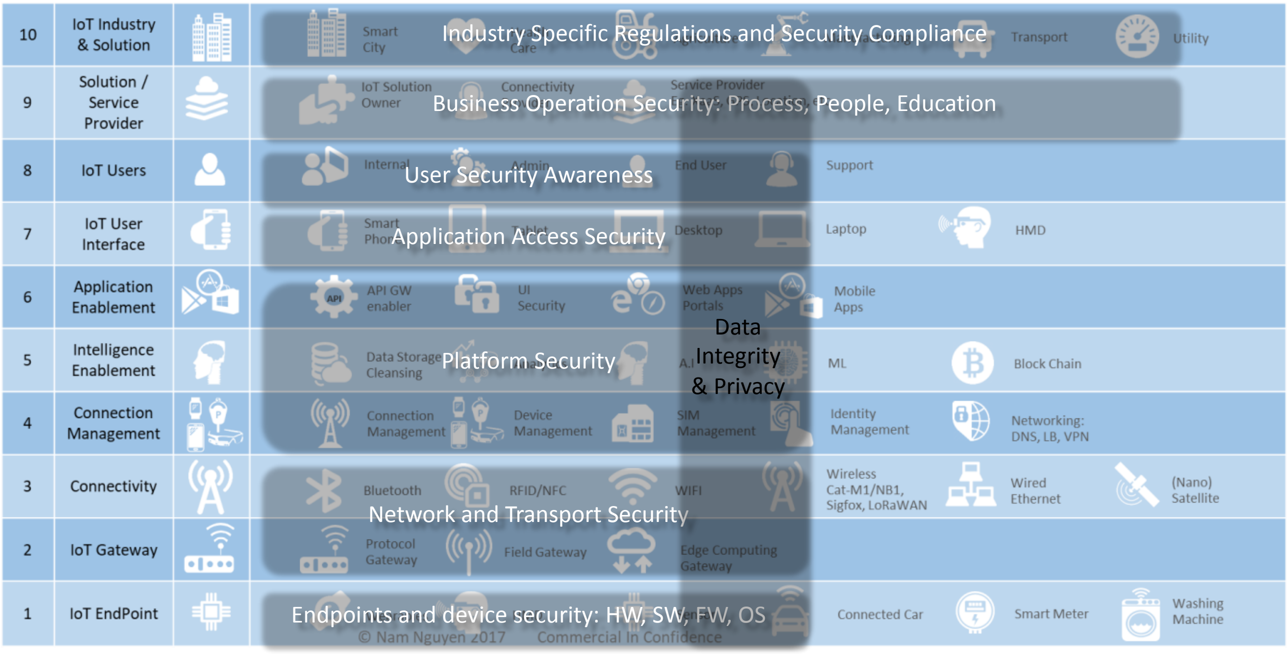


Figure 5 | *IoT Security Framework*

For example, an organisation can use layer 1 as a guide to assess the security of their IoT Endpoints. There are many aspects of security relating to endpoints that could be examined. Below are some examples:

- Can the IoT endpoints be identified uniquely?
- What communications protocols are supported? For example, can secure transport such as TLS supported?
- Is a default password used, and can it be changed?
- Is data encryption supported?
- Do the IoT Endpoints have secure booting? Have they been tested to ensure only verified software will run on them?
- Do the IoT endpoints act as a root of trust? To protect sensitive information and credentials, e.g., through the IoT modules' implementation of chip security?
- Does the IoT endpoint product have physical security protection to prevent physical tampering of the device?

Many IoT security guidelines already exist from organisations such as the IIC, NIST, IoT Security Foundation, OWASP and the GSMA.

IoT Data Privacy

Data security and privacy is an important aspect cyber information, and every country has laws and regulations on how to protect the security of data and the privacy of individuals.

In IoT, the amount of data collected will be on a massive scale, and it becomes even more challenging to manage the security, integrity and privacy of data, when it's at rest in storage, when it's being transported between systems and databases, and when it's being accessed for use.

Using the framework as a guide will also help an organisation address questions such as:

- What types of sensitive data does your organisation store?
- Where does your organisation store data? Is it secured?
- How does your organisation transport data securely?
- Who has access rights and authority to use your data?
- Does your organisation know where your data is accessed and when?
- Is my organisation compliant to data protection regulation, and other laws and regulations such as Consumer Laws and Privacy Laws?

In Australia, privacy is governed under the Australian Privacy Act 1988 [Ref11] and Australian businesses are required to comply with this legislation. The GDPR may apply to businesses outside the European Union if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU. The OAIC's Business Resource on GDPR [REF12] provides further information for Australian businesses on GDPR. Additionally, the OAIC's website [REF13] provides further information about privacy compliance and best practice and the Australian Privacy Principles.

The IoTAA has also produced a Good Data Practice - A Guide for B2C IoT Services for Australia, Nov 2017 [Ref14]. The guide describes the necessary practices for data storage, transmission and use that will embed security and privacy into an IoT solution.

IoT Safety

IoT is not just about the cyber world; IoT is a product of cyber-physical world, and if an industrial IoT solution is hacked, it could be maliciously used to endanger people's lives.

Advances in technology have seen a proliferation of different types of IoT devices and solutions, but not everyone is designing IoT devices with security in mind, let alone safety. Unfortunately, this is not uncommon across a number of industry sectors, from consumer to enterprise devices and applications.

Safety concerns that organisations should ask are:

- Does my IoT solution, or endpoint make the user's life safer?
- Does the IoT endpoint make the user or others around them unsafe?
- If an IoT endpoint stops working, or part of the IoT solution goes off-line, is there a risk of injury (or death) for an individual?
- Will it be safe for the IoT endpoint to operate in its environment, for example, a sensor in a flammable environment such as a fuel tank?
- If the security of the IoT solution or endpoints are compromised, will it cause an accident? Or put someone's life in danger?

The Industrial Internet Consortium, or IIC, has produced an IoT Trustworthiness Framework [REF2], which not only deals with the cybersecurity issue, but also the safety around IoT endpoint device, as well as other issues.

There are five key areas that the trustworthiness framework considers:

1. Security
2. Reliability
3. Resiliency

4. Privacy, and
5. Safety

The IoT AA strongly recommends organisations to consider design their IoT solutions with security and safety upfront.

APPENDIX A – Acronyms & Abbreviations

6LoWPAN	IPv6 Low-power wireless Personal Area Network
AI	Artificial Intelligence
API	Application Programming Interface
AMQP	Advance Message Queuing Protocol
AR	Augmented Reality
Cat-M1	3GPP standard for narrowband machine communications, a variant of LTE
Cat-NB1	3GPP standard for narrowband machine communication, also known as NB-IoT
CoAP	Constraint Application Protocol
DL	Deep Learning
DNS	Domain Name Server
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GSMA	GSM Association
HTTP	Hyper Text Transfer Protocol
HMD	Headset Mounted Display (as in VR/AR headsets)
IaaS	Infrastructure as a Service
IDE	Integrated Development Environment
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IoT	Internet of Things
IoTAA	IoT Alliance Australia
IP	Intellectual Property
LB	Load Balancing
LoRaWAN	Long Range Wide Area Network, operating in unlicensed (ISM) band
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution, also known as the 4G, a 3GPP standard
M2M	Machine to Machine
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
NFC	Near Field Communications
NIST	National Institute of Standards and Technology
OAIC	Office of the Australian Information Commissioner
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
RAT	Radio Access Technology
RF	Radio Frequency
RFID	Radio Frequency Identification
SaaS	Software as a Service
SDK	Software Development Kit
SigFox	A proprietary LPWAN technology, also known as Ultra-narrowband technology, operating in unlicensed band (ISM)

SIM	Subscriber Identity Module (used in Cellular phones)
TLS	Transport Layer Security
UE	User Equipment
UI	User Interface
VPN	Virtual Private Network
VR	Virtual Reality
Weightless	A LPWAN standard operating in unlicensed bands (e.g. 138MHz, 433MHz, 470MHz, 780MHz, 868MHz, 915MHz, 923MHz).
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
XaaS	Anything as a Service

APPENDIX B – REFERENCES

Ref No.	Description
REF1	The Industrial Internet Consortium, "*Volume G1: Reference Architecture*", January 2017. https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf
REF2	The Industrial Internet Consortium, "*Volume G4: Security Framework*", September 2016. https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf
REF3	NIST initiatives in IoT, https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot. In particular the following documents • Cybersecurity framework • Network of Things SP800-183 • Low Power Wide Area IoT
REF4	Towards a definition of the Internet of Things (IoT), Revision 1, IEEE, https://iot.ieee.org/definition.html
REF5	IBM blockchain blog, 22 Feb 2018. https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/
REF6	Amazon Web Services (AWS) IoT, https://aws.amazon.com/iot/?nc2=h_iot
REF7	Introduction to the Architectural Reference Model for the Internet of Things, https://iotforum.org/wp-content/uploads/2014/09/120613-IoT-A-ARM-Book-Introduction-v7.pdf
REF8	Microsoft Azure IoT Reference Architecture Guide, https://devicepartner.microsoft.com/en-gb/assets/detail/microsoft-azure-iot-reference-architecture-pdf
REF9	OWASP IoT Projects, www.owasp.org
REF10	GSMA, "IoT Security Guidelines for Endpoint Ecosystems", Ver 1.0, February 2016, Page 6. https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.13-v1.0.pdf
REF11	Australian Privacy Act, 1988. https://www.legislation.gov.au/Details/C2014C00076
REF12	OAIC Business Resource on GDPR. https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation
REF13	OAIC website. https://www.oaic.gov.au/
REF14	Good Data Practice - A Guide for B2C IoT Services for Australia, Nov 2017. IoTAA. http://www.iot.org.au/wp/wp-content/uploads/2016/12/Good-Data-Practice-A-Guide-for-B2C-IoT-Services-for-Australia-Nov-2017.pdf
REF15	INFYRA, www.infyra.net
REF16	IT Reference framework, Richard Diver, at www.rdiver365.com
REF17	A Reference Guide to IoT – Bridgera, https://bridgera.com/ebook/

APPENDIX C – IOT REFERENCE TABLES

This appendix contains a table of examples for each layer of the IoT Reference Framework.

Layer 10 Reference Table

LAYER 10	IOT INDUSTRY SECTOR & SOLUTION	DESCRIPTION
	SMART CITIES	Smart Cities is quite broad, and includes Smart Street Lighting, Smart Bin, Smart Parking, Smart Building, Assets Management, etc. There's no one definition of what a Smart City entails. It's really up to each city to define its own Smart City plan.
	AGRICULTURE	This category can include anything from farming to livestock to aquaculture. Typical solutions today include temperature and humidity sensing, soil moisture sensing, stock monitoring, and so on.
	HEALTHCARE	Smart Healthcare solutions cover anything from family healthcare, community health, personal care to aged care, and disability. Typical solutions include in-home age care, tracking for disability and dementia clients.
	TRANSPORT	Anything from traffic monitoring, road condition, vehicle to vehicle/X, drone, intelligent transport systems, etc.
	UTILITIES	This industry includes gas, water, electricity, alternative energy, etc. An example of a utility solution is smart Water leakage detection and monitoring.
	MANUFACTURING	Manufacturing has been pioneering M2M, or IoT for quite sometimes with automation in their manufacturing process, and this trend will continue, especially under the umbrella term Industry 4.0 or IIoT.
	EDUCATION	Solutions in this sector are more the result of progressing smarter digital technologies and increasing connectivity, rather than a direct implementation of IoT.
	ENTERTAINMENT & SOCIAL	AR and VR and location based IoT services are emerging in this field. Along with solutions focusing on children and their safety, such as devices that will track movement and or activities. IoT solutions in this area often involve social, fitness and/or entertainment factor.

Table 2 | Layer 10 – IoT Industry Sectors & Solutions

Layer 9 Reference Table

LAYER 9	STAKEHOLDER	DESCRIPTION
	SOLUTION OWNER	Business owner of the IoT solution
	CONNECTIVITY PROVIDER	If solution uses the service of a provider such as a cellular network operator (Cat-M1/NB1 connectivity), or a Sigfox network operator, etc.
	SERVICE PROVIDER	This can be any service/solution provider that the IoT solution uses. Service provider can be (but not limited to) a SaaS, IaaS, PaaS, Cloud provider, Analytics solution provider, AI solution, Cybersecurity solution provider, managed service provider, etc.
	IOT DEVICE SUPPLIER & DEVELOPER	Device manufacturer/supplier, or developer.

Table 3 | Layer 9 – IoT Solution / Service Provider

Layer 8 Reference Table

LAYER 8	IOT USER	DESCRIPTION
	CUSTOMER	Those whose business depends on the output of their IoT solution, which enables informed business decisions. The end customer could also be the solution owner.
	ADMIN & SUPPORT	Those who would be responsible for operating and managing the solution.
	SOLUTION OWNER	Business decision makers who would benefit from business intelligence derived from the solution.

Table 4 | Layer 8 – IoT User

Layer 7 Reference Table

LAYER 7	IOT USER INTERFACE	DESCRIPTION
	SMART PHONES	Today's standard computing device to access IoT solutions via apps. Virtually everyone has a smart phone.
	TABLETS	Tablets such as Android and Apple are also common, especially in enterprise environment. Apps developed for smart phones and tablets are similar.
	PC/LAPTOPS	The next most common device are PCs and laptops, which are widely used in enterprise and consumer environments. There are also third party software apps that IoT solution might incorporate as a part of their solution, such as visualisation software (eg. Tableau etc).
	CUSTOM-MADE DEVICES	Traditionally common in industrial IoT applications, where specific and rugged devices are required for harsher environment and tougher handling. There is also a move to IoT interfaces being embedded in household consumer products, such as home hubs, fitness watches/monitors/trackers, electronic assistants (Alexa, Siri, Google) and smart watches, TVs and speakers.

Table 5 | Layer 7 – IoT User Interface

Layer 6 Reference Table

LAYER 6	APPLICATION ENABLEMENT	DESCRIPTION
	API GATEWAY	One of the key features of the Application Enablement layer is the API gateway, which enables third parties, or external Apps, to access to the underlying features, services, security, information, etc. within Layers 6, 5 and 4 of this framework.
	UI SECURITY	Provides security services to protect communications between devices and cloud platforms. These services vary depending on the type of security, and also different from provider to provider. Security may include: AES 128/256 encryption, secure networking, session management, permissions, authentication and auditing.
	WEB/MOBILE APPS SERVER	Apps are an integral part of an IoT solution, that allows users (of different types and authorities) to access and manage the solution. These are achieved through apps, 3rd party software platforms.
	INTEGRATION	Enables integration of the platform to other back office systems.
	RULES ENGINE	Solution owner can define smart device interactions based on rules APIs. Using the Rules APIs, developers can programmatically create and manage Rules for a device owner within an application.
	EVENT MANAGEMENT	An important function that captures and manages (status) events from IoT devices in the field and is used for the management of IoT devices.
	VISUALISATION	Data visualisation platform/server that enables users to query or create reports.
	IDE/SDK	Provides an environment for developers to create and test application developments.

Table 6 | Layer 6 – Application Enablement

Layer 5 Reference Table

LAYER 5	INTELLIGENCE ENABLEMENT	DESCRIPTION
	DATA STORAGE & SYNCHRONISATION	Support for data storage and synchronisation.
	ANALYTICS	One of the key value adding components of an IoT solution is analytics, enabling insights and informed business decision making. Analytics could be done in-house or outsourced to a service provider.
	STREAMING (REAL TIME) ANALYTICS	Provides ability to perform real time analytics based on live data streaming. A number of IoT platforms is offering this capability today.
	ARTIFICIAL INTELLIGENCE (AI)	AI capability is being considered as an important technology to go hand in hand with industrial IoT solutions. AI capability and services are now on offer by service provider such as IBM, AWS and Google, as well as other niche service providers all offer AI on their platform.
	MACHINE LEARNING (ML)	Similar to AI, ML is also within reach of IoT solutions. Many IoT solutions have already been designed and implemented with ML capability, and it is expected that ML will become more common. ML services are commercially available on many cloud providers such as Google, IBM, AWS, and Microsoft.
	DEEP LEARNING	Sometimes grouped together with ML. It’s part of a broader function of ML, based on learning data representations.
	BLOCKCHAIN	Blockchain is an emerging technology that can enable new standard and innovative ways to implement trust in cybersecurity and/or cybersecurity services (amongst other things). Blockchain is still a developing technology, and one can expect to see more IoT solutions that will be incorporating blockchain in coming years.

Table 7 | Layer 5 – Intelligence, or Smart Enablement

Layer 4 Reference Table

LAYER 4	CONNECTION MANAGEMENT	DESCRIPTION
	CONNECTIVITY MANAGEMENT	Refers to the management of connection between devices and the core platform, with regard to protocol mapping (MQTT, CoAP, HTTP, etc), conversion, monitoring, etc.
	PROTOCOL SUPPORT	Provides protocol support/conversion capability. Typical protocols are MQTT, CoAP, AMQP, HTTP, Websocket, etc). Secure transport support, eg. SSL, SSH, TSL. Semantic support is also required, such as JSON-LD, Web Thing Model, etc).
	DEVICE MANAGEMENT	Capability to manage multiple remote devices over the air. Device management includes: • Device registration & support • Device configuration/reconfiguration • Secure device authentication • Multi-device connectivity and messaging support • Device firmware support and updates.
	IDENTITY MANAGEMENT (SIM)	The ability to securely and uniquely identify each device, either through SIM or unique ID, which enables effective device management.
	AUTHENTICATION SUPPORT	Supports secure authentication of devices, identity management (above), asymmetric key authentication over TLS, role base access control, and protocol level authentication.
	ASSET MANAGEMENT	Device specification assets are used to describe the hardware information/configuration for a type of device. They are used to describe an entity associated with a device.
	REST API SUPPORT	To manage registration, deployment and operation of devices at scale. Also to retrieve and update device properties and device state.
	(F)OTA	(Firmware) Over The Air update. Support OTA updates to devices. Note that certain connectivity types are not supporting OTA.
	NETWORKING SUPPORT	VPN, DNS, Load Balancing (LB) support

Table 8 | Layer 4 – Connection Management

Layer 3 Reference Table

LAYER 3	CONNECTIVITY	DESCRIPTION
	FIXED/WIRED	Provide fixed, wired connectivity to IoT devices and gateways. • Typically wired networks uses Ethernet, Modbus, wires, etc. to connect sensors and devices to a gateway
	WPAN	**W**ireless **P**ersonal **A**rea **N**etwork • Short range (meters) / small area / personal space • Low power consumption • Low cost • Bluetooth/BLE 6LoWPAN, RFID, NFC, Z-Wave, ZigBee, wireless USB, etc
	WLAN	**W**ireless **L**ocal **A**rea **N**etwork • Most often known as WIFI • Coverage of a WLAN is typically for homes, offices, cafes, and public WIFI hotspots • WIFI, DECT
	LPWAN	**L**ow **P**ower **W**ide **A**rea **N**etwork • Wireless (ultra) narrow band networks, designed for low power consumption and low data payload network. • From small to large to extensive coverage footprints • Public or private networks • Licensed or Un-licensed radio spectrum LPWAN Technologies: Sigfox, LoRaWAN, Cat-M1, Cat-NB1, Weightless-P, Wi-SUN, Ingenu, etc
	WWAN	**W**ireless **W**ide **A**rea **N**etwork • Large cellular networks owned and managed by operators such as Telstra, Optus, Vodafone • Extensive coverage footprint • Licensed spectrum • GPRS, 3G, 4G (LTE)[2], Cat-1, 5G[3], Satellite

Table 9 | Layer 3 Connectivity

[2] There are Private LTE networks operated by mining companies and public/private sectors

[3] 3GPP has categorized Cat-M1 and Cat-NB1 (NB-IoT) as 5G

Layer 2 Reference Table

LAYER 2	GATEWAY	DESCRIPTION
	FIELD GATEWAY	Represents the **Aggregation Point** for a group of sensors and actuators to coordinate the connectivity of these devices to each other and to an external network such as a connectivity network.
	PROTOCOL GATEWAY	A **Protocol Gateway** that performs protocol conversion between devices and the core platform.
	EDGE GATEWAY	**Edge (Computing) Gateway** may perform analytics, make time sensitive decisions (reduces latency), enforce security, etc, at the "edge", without having to send data to the core platform, which resides at a centralised location.

Table 10 | Layer 2 – IoT Gateway

Layer 1 Reference Table

LAYER 1	ENDPOINT	DESCRIPTION
	SIMPLE STANDALONE	These endpoints are simple devices, usually just sensors, on/off relays, that perform a single function such as detecting a change in a condition. Examples include agricultural sensors, environmental sensors, asset tracker, etc.
	SIMPLE EMBEDDED	These endpoints can be sensors and/or communication module that are embedded in a device that is performing several functions. Examples include Smart Meter (Water, Gas, Electricity), Smart Buildings, etc.
	COMPLEX	Often, the sensors, and electronics are designed as part of a complex system, such as an industrial control system.

Table 11 | Layer 1 – IoT Endpoint

ABOUT IOT Alliance Australia, (IoTAA)

IoTAA is the peak industry body representing IoT in Australia. Over 420 participating organisations and 800 individual participants are working to accelerate the adoption of IoT across the Australian economy and society.

IoTAA's purpose is creating and developing sectoral IoT advancement and alignment with key sectors, including through Government Industry Growth Centre activities, Infrastructure Australia, state Governments and key sectoral bodies with an initial focus on water and energy resource management, food and agribusiness, transport and Smart Cities.

IoTAA's Terms of Reference

- Providing an IoT strategy and policy recommendations with focus sectors to align with government and industry priority areas.
- Engage and collaborate with key stakeholders including major sector aligned Growth Centres, Industry Associations, Major Government Influencers
- Align IoT solutions to meet the needs of industry and consumers
- Create more IoT awareness, engagement and education for consumers, markets and governments.
- Apply the learnings of global best practice sector initiatives such as the US Smart Cities IoT initiative.

IoTAA's work-program spans 11 workstreams which focus on industry vertical sectors and key IoT enablers. They are:

Sectoral Focus

1. Smart Cities
2. Food and Agribusiness
3. Water
4. Energy
5. Transport
6. Manufacturing
7. Health

IoT Enablers

1. Collaboration
2. Data Use, Availability and Privacy
3. Cyber security and Network Resilience
4. Platforms and Interoperability
5. IoT Start-ups

http://www.iot.org.au/