entelect

DEMYSTIFYING IOT

DEMYSTIFYING IoT

Developments in cheaper and more powerful computing chips, solid-state storage and communication electronics have led to an explosion of specialised devices. This in turn has opened huge opportunity to leverage devices for automation and connecting the physical world to the digital world, with the Internet of Things (IoT).

In this publication, we'll introduce you to what IoT is, what components and projects are common and popular, and give you an overview of designing an IoT solution and the difficulties and complications inherent in this type of IT project.

CONTENTS

A BIRD'S-EYE VIEW

DIGGING INTO THE DETAIL

TAKING A STEP BACK

CHAPTER 1 | A BIRD'S-EYE VIEW

CHAPTER 1

A BIRD'S-EYE VIEW

WHAT IS IOT?

"IT'S THE BEGINNING OF MACHINES TAKING OVER THE WORLD."

With the explosion of the internet in the 1990s, we finally had a network of computers that could communicate and share information easily. The internet has evolved into a much more sophisticated network where any intelligent device can be connected and communicate, gather data, and process valuable information. **This information can be used to make more informed decisions by either machines or people.**

The term IoT was originally coined in 1999 by the Radio Frequency Identification (RFID) development community and is still reasonably a young participant in the internet. With the realisation of how valuable data and information is in recent years, IoT has become quite a sensational trend within commercial and industrial streams. [1]

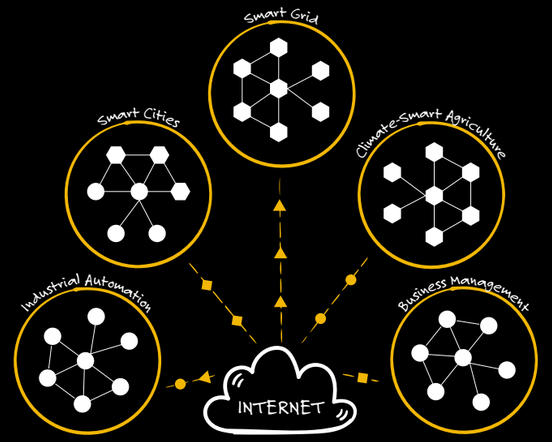
Cisco defines the term IoT as the **network of physical objects accessed through the internet**. These objects contain embedded technologies to interact with internal states of other devices or object, like the on/off state of a door bell, or the external environment, like the ambient temperature of a room.

This information can influence how and where decisions are made as well as who makes them. These physical objects or "things" can range from a variety of devices such as thermostats, doorbells, video cameras, weather sensors, water pumps, and more.

IOT DEVICES AND NETWORKS HAVE THESE **FUNDAMENTAL CHARACTERISTICS:** [2]

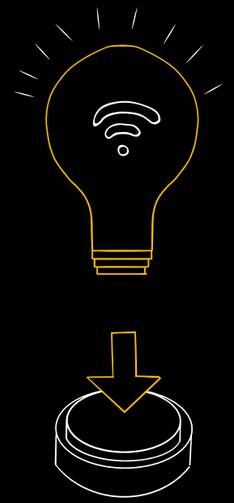
INTERCONNECTIVITY

Connectivity is what makes IoT devices so valuable. The ability to share the information it generates or captures, and can be shared through connectivity to other devices or networks.



HETEROGENEITY

The intrinsic diversity and modularised nature of the different hardware and networks allow this characteristic. The different devices should be able to interact with each other through different networks.

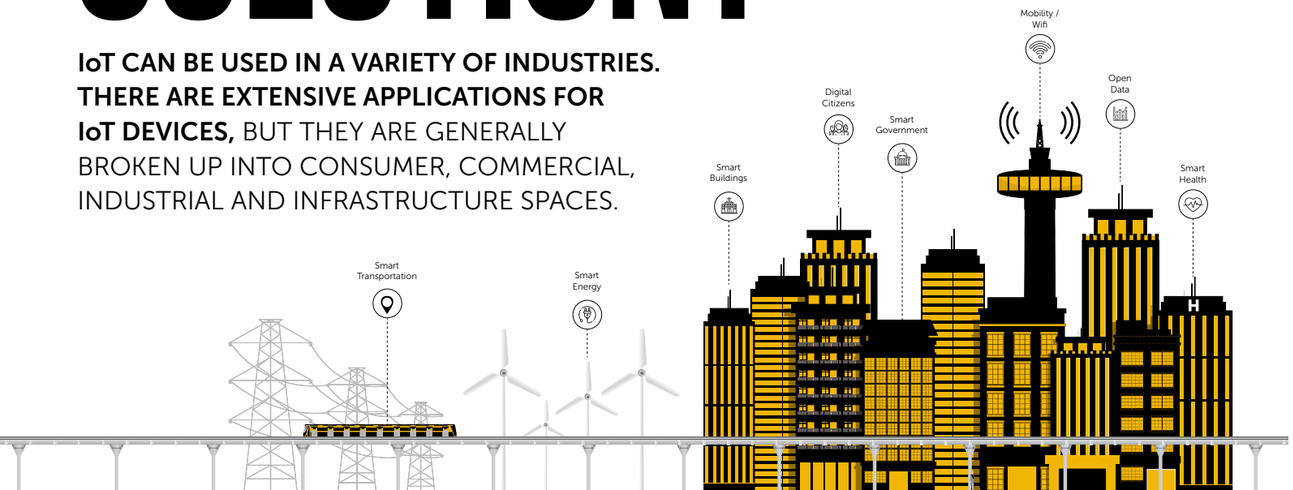


DYNAMIC CHANGES

Devices can be added or removed from the network as it operates. The state of each individual IoT device also changes dynamically within the network. Anything within the environment that the devices are monitoring can influence the state of the IoT device and the data it produces.

WHERE WOULD YOU USE THIS TYPE OF SOLUTION?

IoT CAN BE USED IN A VARIETY OF INDUSTRIES. THERE ARE EXTENSIVE APPLICATIONS FOR IoT DEVICES, BUT THEY ARE GENERALLY BROKEN UP INTO CONSUMER, COMMERCIAL, INDUSTRIAL AND INFRASTRUCTURE SPACES.



CONSUMER

These are solutions aimed at the general public. It's possible to monitor the energy consumption of a smart home, and switch off lighting, heating and air conditioners at a certain time or when certain conditions are met. For elder care, homes can be fitted with motion sensors which can alert elder care workers or guardians to potential problems.

COMMERCIAL

In the commercial industry successful IoT solutions have been implemented in the medical and healthcare system, transportation, vehicle-to-everything (V2X) communications, and building and home automation.

In the healthcare field, IoT solutions can enable remote health monitoring and emergency notification systems. IoT devices can be used for smart traffic control, smart parking, logistics, and fleet management.

If IoT is combined meaningfully with machine learning, it can help in reducing traffic accidents by introducing drowsiness alerts to drivers, providing driver-assist features, and eventually fully autonomous driving and connected road infrastructure.

IoT solutions have been applied to general manufacturing and agriculture. Applications such as monitoring crops, windspeed and humidity are collected. This data can be used to make decisions on when to plant crops, fertilise them, and harvest them.

INFRASTRUCTURE AND GOVERNMENT

In the infrastructure sector, IoT is successfully used for energy management, environmental monitoring and metropolitan scale deployment. Smart cities are another use of scaled IoT solutions. This can enable governments to make decisions based on the data being transmitted from thousands of sensors. An example of this: governments can determine how much energy is used on a monthly basis in different areas for different applications, based on different behaviour, and can make informed decisions on conserving and optimising energy production, and what policies to drive around energy management.

DATA COLLECTION

IoT can be useful in many ways; it simplifies the users' lives and can be used to make valuable decisions. It can sometimes overload the user with a lot of data to review in order to make informed decisions. IoT can greatly impact the economy of a country because with smart cities implemented, the government can reduce expenses and focus their money on more important matters.

Concerns of IoT systems:
The one major aspect of IoT systems is that they are always collecting data. This data could mistakenly be leaked. Anything with IoT devices implemented can be hacked, so security and privacy should always be a concern when implementing such solutions.

IOT PROJECTS COME IN ALL SHAPES AND SIZES, AND ARE GENERALLY PURPOSE-BUILT FOR SPECIFIC TASKS.

At its core, IoT is made up of a lot of small things working together, to achieve a greater goal. This can be as small as switching on a light using Wi-Fi, or as large as monitoring an entire city's energy usage. There are typically two distinct actions being done by devices and sensors: controlling other devices and objects, or collecting data.

Large-scale IoT projects can be broken down into many small devices communicating with each other. While this does not sound overly complex, every new device added to a network brings in more data to manage, another device to monitor, and another connection to maintain.

55% OF ALL **DATA** IS FORECAST TO BE GENERATED BY IoT IN 2023

43% OF **AI TASKS** WILL HAPPEN ON EDGE DEVICES IN 2023

70% OF **ENTERPRISES** WILL RUN VARYING LEVELS OF **DATA PROCESSING** AT THE IoT BY 2023

[Source: Intel.com]

FROM THE SMALL TO THE REALLY BIG

3 EXAMPLES OF IOT PROJECTS

LET'S USE THESE EXAMPLES TO UNDERSTAND WHERE COMPLEXITY CAN CREEP IN, AND THE CONSIDERATIONS THAT OFTEN NEED TO BE MADE WHEN DESIGNING AND IMPLEMENTING THEM.

1. HOME AUTOMATION

Simple, can range from cheap to expensive, low-volume and low-frequency data.

For the home automation system, the user simply wants to be able to control and monitor their homes from wherever they are, as well as improving their quality of life at home. This does not require many devices and setup to execute, as most devices and sensors needed are already readily available, and are fairly cheap. There is very little complexity involved, even though devices are both collecting information and controlling other devices. **One of the biggest choices that need to be made would be: where does the data processing occur**, as this can be done on the devices themselves (edge computing) allowing devices to act alone, or it can be done in the cloud (cloud computing) where the resulting decisions are fed forward to the devices to act upon them.

2. RACING CAR TELEMETRY

Expensive, real-time data processing and analytics, high-volume and high-frequency data.

Telemetry forms part of most IoT systems, as telemetry focuses purely on data collection. Racing cars often use onboard telemetry systems to allow their pit crews to monitor and assess the car's health, allowing the driver to focus on the race. There are hundreds of finely tuned sensors constantly collecting data and transmitting this information to either a central hub for processing before being uploaded to the cloud, or being sent directly to the cloud for processing. **How the data is managed is where the most complexity arises and is fully dependent on what the users want to achieve with their data**. If the goal was simply to collect data for processing in the future, then not much more needs to be done. However, if the crew wanted to make real-time decisions based on current and historic information, the complexity increases dramatically.

3. SMART CITIES

Mix of high to low data volumes and frequency, cost can vary widely depending on end goals.

Smart city projects are essentially a mixture of both home automation projects and real-time telemetry projects. There are components where you would want to control certain devices. For example, switching on street lights only when it is sufficiently dark outside or adjusting the brightness of traffic lights depending on the surrounding light levels. These components behave similar to that of home automation systems, with the key difference being the sheer number of them implemented across a city. This adds the first layer of complexity, as the volume of data needing to be processed is increased dramatically, and requiring much more robust infrastructure to handle the level of traffic required.

Additionally, these projects also include surveillance components, monitoring activity and behaviour. This data not only needs to be managed in a much more secure manner, but also requires a real-time component. Achieving this at scale is a mammoth task, not only because of the infrastructure that needs to be put in place but also the amount of work and effort required to correctly manage the data streaming in. Further complexity can be added in if real-time decisions need to be made using analytics in conjunction with historic information.

CHAPTER 2

DIGGING INTO THE DETAIL

TYPES OF IOT PROJECTS

HOME AUTOMATION

SECURITY AND ALARMS

INDUSTRIAL

HEALTH

FINANCE

THE WORLD OF IOT DEVICES IS FAR-REACHING AND EVER GROWING

Many businesses are starting to, and in some cases, have already invested resources into the utilisation of IoT devices for further business growth. More consumers are also making use of the power of IoT devices to improve their standard of daily living. This is where the power of IoT devices comes in – its vast application into so many sectors. Below we highlight how IoT is used in everyday work and life, and highlight not only the impact that it has, but also its vast potential.

HOME AUTOMATION

Smart homes are becoming more popular as they increase the comfort and quality of life. The majority of smart home systems are controlled by phones, tablets or "micro-servers." An app is used to control and monitor home "states" and "functions" via wireless communication (Wi-Fi).

A "smart home" involves the control and automation of all its associated technology. A smart home can be made up of appliances, lighting, heating, cooling, TVs, computers, audio systems, large appliances (like washing machines and dryers or refrigerators and freezers), alarms, and camera systems.

The smart home becomes possible with the integration of various IoT devices and cloud services, by embedding intelligence into sensors and processors.

There are three main components for any smart home: IoT devices, cloud services and rule-based processing. Each of these blocks contributes its core functions and capabilities to make up a smart home.

IoT devices provide internet connectivity and remote management of appliances, attached with a range of sensors. Sensors can be connected to most home appliances like air conditioning units, lighting, gates, fridges and a variety of other home devices. By making use of IoT, we now "allow" computer intelligence into our home devices to provide monitoring and metrics on the home environment and our now, smart, appliances.

Cloud computing provides processing power as and when we need it, scalable storage and applications, for creating, maintaining and running home services. Cloud computing also makes accessing home devices anywhere, at any time, possible.

The **rule-based processing** system (or service) provides the control and orchestration of the smart home, responding to changes in sensor readings and triggering specified actions on connected devices. These are often controlled by mobile apps or background rules.

These appliances consist of IoT enabled switches and sensors connected to a central server which can be controlled by using your phone or tablet. Many homes also integrate into the popular smart assistants (Amazon Alexa, Google Home) adding additional functionality like voice activated control.

The idea and implementation of the smart home provide additional intangible benefits like increased security monitoring, energy efficiency, lower utility bills and the convenience of turning your lights on from anywhere in the world. In most cases, these devices are flexible enough to integrate with different providers and protocols.

The popularity of the smart home is growing, as it becomes part of modernisation and reduction in monthly costs. An important part in achieving this is the ability to have a centralised event log store, execute artificial intelligence (AI) processes to indicate high-cost appliances, cost-saving recommendations and other useful analytics.

SECURITY AND ALARMS

There are many potential applications and use cases for IoT projects in the security space, from integrating into existing alarm systems to extending functionality, and creating backbones for new security systems. Arrays of sensors can be monitored remotely and integrated with each other, such as detecting carbon monoxide and rapid temperature changes. These type of applications and sensors could be integrated with smart home devices such as Amazon Alexa or Google Nest to give you a wider range of capabilities.

These are some of the more common sensor types that form part of a physical security system.

Infrared or ultrasonic proximity sensors can be used to detect the proximity or the distance between a sensor and an object. A potential use case in a security system would be placing an infrared sensor behind a door to monitor if it has been opened, or if you place it above the doorway you could monitor if anything is moving through the door.

Ambient light sensors monitor light levels. This sensor could be utilised to detect if lights have been switched on or if there are sudden changes in light level from an intruder's torch, or even a fire.

Microphones to monitor ambient noise levels and in certain applications to store any sound data they collect. A microphone could be incorporated to trigger alarms if there was a sudden loud noise.

Temperature sensors are often used when the risk of fire is high, these can be set up so that they will detect sudden increases in temperature but won't be affected by daily fluctuation in temperature.

Gas particle sensors are used to monitor for harmful and dangerous levels of gasses, such as carbon monoxide or carbon dioxide. These sensors could give you early warnings to gas leaks and prevent further damage. They are particularly important as many toxic chemicals are not visible with the naked eye. This type of sensor could play a key role in keeping you safe if you are working in a confined space that is prone to carbon leaks.

Cameras can be integrated into IoT-based security systems. These could feed data back to a data centre or, utilising cutting edge computer vision tech, the collected data can be analysed immediately to detect any anomalies. Potential applications could include facial recognition and number plate readers.

One important aspect to keep in mind is what is being shared with the devices. Some data such as a car license plate number for example may not be so important or sensitive (in that it can be changed). However, what needs to be considered are aspects such as the location of your child [3], the conversations that take place in your home [4,5], your fingerprint or other sensitive information that these devices are able to collect as they become an integral part of modern life. When developing or utilising IoT systems, it is crucial to understand what data is being stored, by who and for what duration of time.

It is also critical to ensure systems fail safely. If a 'smart lock' loses power, does it automatically lock all doors to secure the property and consequently trap all occupants, or does it unlock and allow unfettered access onto the premises? IoT devices can provide a level of security that was inconceivable not too long ago, but when using these systems, we need to ensure that there are backups and contingencies in place, as they can (and will) fail. [6, 7, 8]

INDUSTRIAL

IoT solutions offer a myriad of novel applications in the industrial world. The industrial use of IoT systems can immensely enhance the automation, service delivery, customer experience and operational efficiency of many corporations.

The following is a collection of examples where IoT systems are actively and successfully contributing to the success of corporations [9]:

Hitachi aims to implement a commercially available predictive maintenance platform. This system provides Hitachi with a means of predicting which equipment shall require maintenance and when [10].

Amazon pushed the boundaries of automation by incorporating robots with IoT sensory devices to search and locate products on shelves. The incorporation of IoT technology resulted in a 20% operational cost saving [9, 11].

Bosch incorporated IoT technology to track and trace power tools to minimise the amount of time spent to locate and acquire tools by maintenance staff [9,12].

Thyssenkrupp Elevators uses their MAX system to transmit elevator telemetry such as door movements, error codes, power-ups and trips via IoT devices. MAX enables Thyssenkrupp Elevators to detect when elevator machinery fails and dispatch the appropriate maintenance staff when necessary [13].

The industrial use of IoT can revolutionise the operational efficiency, automation and customer experience of corporations.

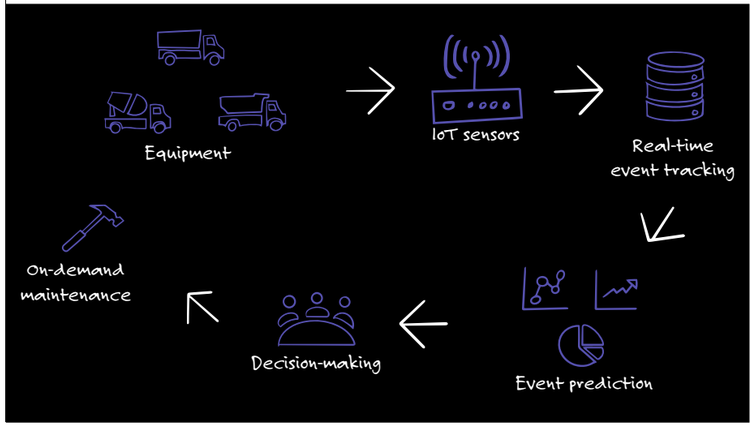
The following section gives an abstract overview of how predictive maintenance systems enhance the operational efficiency and customer experience of a corporation.

PREDICTIVE MAINTENANCE

The implementation of predictive maintenance systems using IoT technology can aid businesses to improve their maintenance, costing and business processes:

- Predictive maintenance can detect the sub-optimal performance of machinery or equipment, and predict imminent failures, inefficient or cost-ineffective equipment [10].
- It aids technicians to identify, prioritise and plan maintenance tasks across a wide range of equipment [14].
- It can aid corporations to improve overall business processes such as customer care, cost-effective maintenance and maintenance reporting [14].

The use and implementation of an IoT predictive maintenances system demonstrate how IoT technology can automate and enhance the various operational processes within corporations. Be it from a maintenance perspective, operational perspective or by simply enhancing customer experience.



"THE OPPORTUNITY WE HAVE IS TO BUILD A SECURE, INTELLIGENT PLATFORM THAT SOLVES SOME OF THE WORLD'S GREATEST PROBLEMS AT SCALE. THAT'S WHAT'S POSSIBLE WITH HUNDREDS OF BILLIONS OF CONNECTIONS AND THE CAPABILITIES THAT WE CAN DELIVER TOGETHER."

— CHUCK ROBBINS

HEALTH

IoT devices in the health space have the potential to impact our lives in a positive way and improve our overall quality of life. From the ability to detect conditions early, to assisting with better management of existing conditions. They give us the data to gain insights we previously would not have had. This section aims to give an overview of devices that are currently available, explain how they work, and look at new developments in the field.

The most well-known devices in this category are probably fitness trackers. These can range from simple pedometers to top of the line smart watches.

Regardless of the capabilities or cost, fitness trackers all have the same aim; to track physical activity, gauge fitness levels and measure improvements over time.

Naturally, data is important, and the more data that can be measured the better. A top-of-the-line device uses a wide array of sensors to measure steps walked, distance travelled, heart rate, sleep and even maximum volume of oxygen that is transferred to the blood [15,16]. Common sensors include:

3-axis accelerometer
Records movement in every direction. Used to infer steps taken (which can be used to estimate calories burned) and to measure the quality of one's sleep (lots of movement during sleep leads to a lower rating) using a process called actigraphy.

Gyroscope
Tracks orientation and rotation.

GPS
Records position and speed. Measure routes taken and distance travelled. Can be used to infer elevation gain and loss when used in conjunction with GIS data [17,18,19].

Altimeters
Monitors elevation changes since exercising at high elevations can influence heart rate and blood oxygen levels [20].

Optical sensor
Tracks heart rate by shining a light beam on the skin to the pulse and measures the maximum volume of oxygen that is transferred to the blood [21].

Electrocardiogram
Electrical activity of the heartbeat. The Apple Watch Series 4 included the ability to notify you if it detected an irregular heartbeat, which can be a major risk factor for a heart attack [22].

Temperature
Monitors body temperature or ambient temperature.

Bioimpedance
Records the resistance of skin to electric current, to infer skin water content, body composition (training nutrition) and cardiac output [23].

These devices sync the data captured to online platforms where complex analytics can be performed. This is done either by tethering to a PC or making use of a Bluetooth connection to a smartphone. While the information gathered is usually for your own reference and tracking, some companies are incentivising you to give them access to your data, allowing them to track your overall health and activity levels [24].

THE NOT-SO-SECRET BASES

A somewhat amusing story emerged in the press last year, where soldiers and military personnel were recoding their fitness activities in military bases. When these were uploaded to Strava, an exercise tracking app, their bases were clearly visible and gave away the location of some secret bases. This kind of story just goes to show the wealth of personal data that smart devices such as Fitbits and smart watches collect as well as the level of insight and analysis that can be extracted when this data us aggregated.

Fitness wearables have become commonplace and very popular in the last few years. So popular that the global revenue worldwide for devices sales in 2016 was 2.49 billion USD [25] and the estimated sales in 2020 were 2.76 billion USD.

Now we can move on and look at some of the more specialised form factors and niche devices, as well as some prototypes that hold a lot of promise.

Smart scales
These offer tracking of weight at the very least, but can also include lean mass, BMI, and more. They usually pair with a smartphone companion app to upload data and to display metrics and progress. Most of these are straight-forward, and there are guidelines online that show how to create your own version using a simple ESP32 [25,26,27].

Jewellery
Rings are emerging as a potential form factor for smart devices. Motiv managed to cram an accelerometer and a heart rate monitor into this tiny device and while the price tag is still a bit high, the potential is there. Oura ring on the other hand (or finger) plans on becoming an illness early-warning system by monitoring sleep and temperature to detect flu-like symptoms. These rings were worn by NBA athletes during the Coronavirus pandemic [28,29].

Cosmed's K5
This device measures oxygen consumption, heart rate and energy expenditure from your breath. There is a lot of valuable data in your breath and while the tech is mostly available to top athletes it could potentially make its way to consumer devices in the future [30].

Contact lenses
Mojo Vision has a smart contact lens that they say can enhance your sight. They are aiming it at people with limited vision, but it is easy to see the technology finding use in other areas [31]. Google is working on a diabetes tracking contact lens. A sensor housed in the soft lens measures the glucose levels in tears at regular intervals and communicates this data to other devices using RFID [32].

Artificial Pancreas
These devices help people with diabetes, primarily type 1, automatically and continuously control their blood glucose level. The Open Artificial Pancreas System project (#OpenAPS) is an open and transparent effort to make safe and effective basic Artificial Pancreas System. OpenAPS communicates with an insulin pump to obtain details of all recent insulin dosing by communicating with a Continuous Glucose Monitor. It then sends commands to the insulin pump to adjust temporary dosage rates as needed [33,34,35].

Judging by the sheer amount of fitness trackers sold in the last few years and the various form factors in development it is easy to call this category one of the most widespread IoT markets for the general consumer.

FINANCE

The financial service industry is one that has been massively impacted by the rapid state of technological advancement. In many areas, IoT devices have been seamlessly integrated into businesses and form a substantial part of their product and feature offerings.

The insurance sector has seen a lot of businesses innovate with regard to how they utilise the power of IoT devices.

In the health and car insurance industries IoT has allowed a whole new form of rewards integration and in some instances entirely new reward programmes. With the use of IoT devices, insurance businesses can gather time series data to track users' goals and offer rewards for meeting certain behaviours.

The ease of integration of these devices also plays a big role in maintaining the experience for customers. Given a certain platform and certain IoT device, users are often able to utilise that device and seamlessly integrate it into their daily lives. A local example of this is Discovery Ltd.

Banking is another sector that has been enabled by the IoT. Banks using IoT devices have been able to provide access to services and products to more people at more locations and to also improve the security while doing so. A recent trend has been the adopting of tap and pay functionality negating the need for others to handle one's bank card. This has not only seen rise to the tap and pay enabled bank cards for both credit and debit customers, but also the rolling out of new and updated card machines. For a large part of a customer's banking experience, physical cash has been done away with in favour of digital and safer alternatives.

ATMs have also become far more feature rich, and in many ways, attempt to mimic the online banking experience of many companies. Banks are also able to provide kiosks in places to give further access to services to many more customers than before.

A big use of IoT devices comes in the forms of trackers, which provide time series data for financial service companies to use. However, sensors also form a big part of IoT devices used. In particular sensors such as fingerprint scanners along with remote controlled cameras provide a number of options around biometric authentication. Financial services can be a sensitive business area when pushing the envelope on the IoT and later we will discuss how this uptake of IoT device utilisation impacts the security of the devices as well as the privacy of the people using them.

OPEN-SOURCE IoT PROJECT

An open-source project that genuinely highlights the complexity of designing an IoT system and analysing the sheer volumes of IoT data in real-time fashion is the Microsoft Azure Remote Monitoring Solution with Azure IoT. This project from Microsoft Azure is a fantastic resource to delve into the real-time monitoring and analysis of IoT devices. It provides a platform to create triggers that execute alerts and actions and to perform remote diagnostics and maintenance requests on IoT devices.

This project incorporates several design patterns and Azure cloud-based resources to accomplish its objectives. It incorporates micro-services architecture with docker containers for scalability, Azure IoT hub for large-scale dual-communications with IoT devices, Azure Stream Analytics to process, aggregate and analyse incoming streams of IoT device data and Cosmos document database to store and process data.

This project may not be a silver bullet project as a large-scale, real-time IoT monitoring system. However, it does provide excellent insights into the complexities and approaches to design and implement a large-scale distributed IoT system, using mature and efficient cloud-based resources.

COMPONENTS THAT MAKE UP AN IOT SOLUTION

CAMERAS + SENSORS

ACTUATORS

DRONES

EVENT PROCESSING

DATA STORAGE

CLOUD COMPUTING

STREAM PROCESSING

EDGE COMPUTING

NETWORK

E V E R Y T H I N G

T H A T C A N B E

A U T O M A T E D

W I L L B E

A U T O M A T E D

AN IoT SOLUTION IS NOT A SINGLE THING, **RATHER IT IS A COLLECTION OF INTERCONNECTED COMPONENTS AND DEVICES.**

A sensor's data is collected and continuously transferred via the network to a server or other data processing component. The sensors' data is then processed by the server. APIs allow external applications to control the sensors, given it follows a pre-defined format. Actuators execute commands in the server or control other devices. It translates the activity to a language that the device can use to carry out a task. The received sensor data is processed to determine if any rules have activated. Databases store the processed data collected from the sensors and makes it available for data analysis, presentation, and visualisation.

CAMERAS AND SENSORS

Sensors are one of the key components to an IoT solution. There are a number of different sensors, including:

- Fire detection
- Leak detection
- Windows/doors opening and closing
- Temperature and humidity
- Motion
- Garage doors and gates
- Weather

Sensors collect internal and external home data and measure environmental conditions. These sensors can either be connected to an IoT hub or directly attached to appliances or devices.

The data gathered by these sensors may be stored for later analysis or used to trigger behaviours within the system.

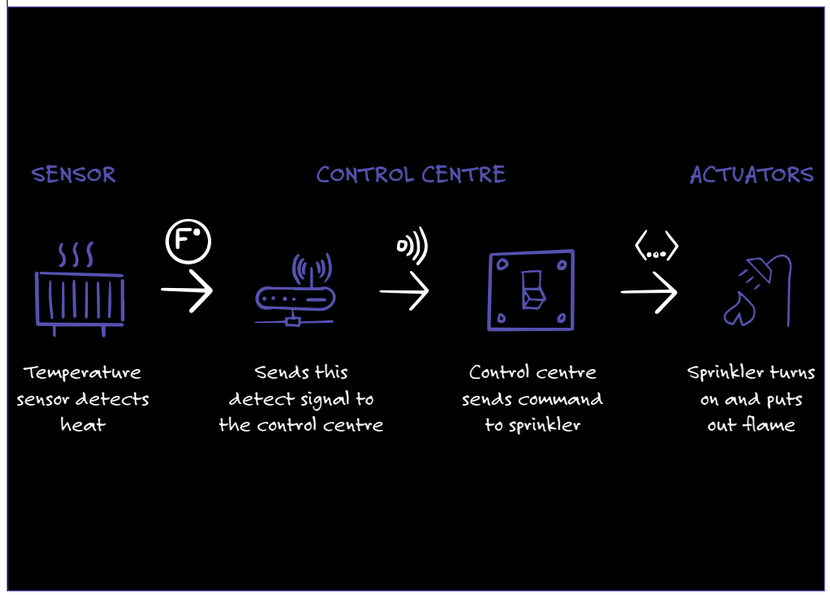
Cameras are also a form of sensor, but one that deserves specific attention. Modern connected cameras are a long way from the grainy, poor-quality CCTV cameras. A large percentage of IoT applications use some form of camera, to track movement in a store, detect when a door is open or to look for anomalies in pipes or cables.

The ease of surveillance however has implications for privacy and the storage and use of such data should be carefully considered.

ACTUATORS

If an IoT solution needs to act on the physical world, instead of observing and reporting on it, then one or other type of actuator will play a part in the solution.

Actuators are things like motors, pumps, switches, or anything that turns a signal into a physical action. A simple example would be a sprinkler switch, which is activated when one or more types of sensors detect a possible fire.



DRONES

Drones are not the first thing that comes to mind when thinking about IoT, but recent advances in computer vision and on-board machine learning capabilities are turning drones from a flying toy to an industrial workhorse.

The primary advantage drones have is their mobility. Their ability to fly allows them to be used in areas where fixed cameras or other sensors simply cannot be placed.

Drones can be fitted with GPS, radio, and cameras for recording the positions of objects or people. They can be fitted with temperature and wind sensors as part of weather monitoring. They can be fitted to carry cargo payloads, to distribute seeds or fertiliser to fields, and more advanced drones can fly routes automatically, without the need for manual control.

Some uses that drones have seen recently include:

Farming
Planting seeds and distributing fertiliser, as well as mapping the fields and checking on crops and livestock.

Delivery services
Amazon's plans to use drones for deliveries are well known, but that's far from the only use in this area. From delivering emergency supplies in disasters to flying floatation devices to swimmers in distress, drone delivery isn't just about getting a pizza without getting off the couch.

Industrial
Oil and gas plants have vast amounts of piping, much of it in difficult to reach places, and then there's the kilometres of pipelines that stretch between the refineries and factories. This piping needs to be monitored for leaks or other problems, but that's expensive and tedious. With drones however, the pipes can be checked from the air, and with recent improvements in on-board image recognition, the drones can even recognise problems with the pipes without human intervention. Nordic energy companies have been using drones to monitor power lines for a few years now [36].

EVENT PROCESSING

Event processing, or more generally known as complex event processing (CEP) is used to process huge amounts of primitive events (data generated through sensors) as they happen, in near real-time, by making use of methods (statistical data analysis), techniques (machine learning) and tools (in-memory processing). One can easily get confused by the definitions of CEP and big-data processing because of how strongly related these two topics are. Event processing can use a pre-defined model to filter out parts of data that are of no interest as well as combine selected data from multiple different source streams and prepare the combined data for further big-data processing.

The application of CEP, especially in the research fields, have been focused on improving environmental and medical environments or even making connections on the impact environmental factors can have on certain medical conditions. Smart and sustainable cities are another area where CEP is being applied in specific domains such as smart electricity grids and smart traffic control systems.

DATA STORAGE

Data storage in IoT solutions is often more about what not to store, than what to store.

If, for example, there was a monitoring system in a factory with thousands of sensors, the detail of normal sensor readings is probably not of value and will make analysing the data more difficult. Instead, data points that fall within acceptable criteria could be discarded and only readings outside of those acceptable criteria stored.

Even with techniques like this the volume of data can be a problem. Typically, the first data store should be a distributed, write-optimised database, not a traditional relational database. Depending on the scenario, a time-series data store may be necessary, especially for situations where multiple data streams are being received from different IoT devices, and correlations between those events are interesting.

Relational databases still have their place here, but it's as a secondary data storage, for processed data. This may be the output of stream processing, or it may be the result of transformations made on the raw data.

The data that comes out of an IoT implementation is immensely valuable, and it's well worth spending some time getting the data storage done properly to ensure that future analytics performed on the data produce value.

CLOUD COMPUTING

All the data that is generated from these IoT devices also needs to be stored, processed and accessed. This can be quite a burden on companies as a large amount of data is required in order to get valuable information from the IoT devices. As more devices are added to the system, more storage is required, leading to a need for scalability. To get valuable and useful information from the large amount of data that these devices create, the data needs to be processed into something understandable for humans.

IoT and cloud computing have become tightly coupled over the years due to IoT requiring large amounts of storage and processing power.

Determining your infrastructure requirements for an IoT solution is quite difficult and making use of Cloud service providers brings the added benefit of scalability. This increased scalability can be used to add new services to your solution as it is needed, without the need for acquisition and installation of new hardware on the premises. In many situations it is more cost effective to use cloud providers as they typically only charge for the resources consumed. This means that there is no need operate data centres.

There are many situations where cloud computing may not be the best solution. A system that requires real time calculation cannot afford to wait for a network request to the cloud infrastructure and response before reacting.

An excellent example of this is a self-driving car; If an autonomous car is about to collide with an object, it cannot wait for the cloud infrastructure to analyse the data and report back with an instruction, it may be too late. This is where fog or edge computing comes in. This is when local (to the device) computing is used to make decisions based on the data collected. This does require more sophisticated hardware on the devices [37,38].

STREAM PROCESSING

By a stream, we refer to flow of data. By stream processing we imply that we are applying some sort of data processing logic on the stream to either generate information or take some action based on the data.

IoT devices are constantly generating data and some of these devices stream data through the internet for processing. These streams of data can be attached to services which analyse the live stream as soon as data reaches a cloud/internet endpoint so that we can take some action based on the data values. It offers us the ability to store, analyse, visualise and take immediate action, almost real time, as soon as a datapoint reaches the endpoint, rather than after data is saved to storage and then analysed.

Imagine an air conditioning system that is linked to foot traffic sensors at doors and hallways. It counts foot traffic and combines this with temperature sensors at windows that measure ambient temperate. Based on people moving past the foot traffic sensors the system can adjust the temperature and airflow around the building taking into consideration the location that are getting higher volumes of people instead of just assessing the temperature after it drops.

EDGE COMPUTING

Edge computing with respect to IoT devices, is computing and data storage to drive event-based decisions or actions on device without the need to transmit data to the cloud for processing. Think of it as making storage and processing resources closer to the location where needed.

We may want to enable an IoT device to make decisions near real time, and sometime there may be an overhead with having to transmit information to the cloud where the benefit would be greater to do computing on device.

An edge computing benefit is reducing latency or waiting times caused by cloud transmission. This enables the IoT device to be able to respond faster to events and take action in the field.

Imagine a drone travelling to remote location which is guided by GPS to inspect pipelines where there may not be internet connectivity. If the drone can inspect a pipe and use AI on device to identify a problem, this allows improved data collection and action on-the-go. When the device gets to its location where it can send out a communication response to engineers of a fault, it can action the notifications.

SECURITY AFTERTHOUGHT

IoT devices are typically small and have low amounts of CPU, RAM and storage. This means that aspects that are not directly linked to the device functioning are often left out.

One example of this is the lack of support for HTTPS on IoT devices. While there are ways to work around this now, it is an indication of security being an afterthought for many companies designing these IoT devices. If security is a concern for your company, you may need to research this more thoroughly.

THE FISH TANK

Any IoT device connected to your corporate network should be secured, and these measures need to be well thought out and implemented consistently. No matter the device, security should always be considered. This was not the case for a Las Vegas casino who had taken every care to have robust firewalls and security measures, but did not secure their IoT enabled fish tank. This led to a major breach of their systems with hackers accessing their clients banking and other personal details.

NETWORK

GETTING YOUR DEVICES **CONNECTED AND COMMUNICATING** IS A KEY COMPONENT OF ANY IoT IMPLEMENTATION

There are two key considerations here being the topology and the type of connection used for communication. The typical medium of communication used for IoT projects is wireless however, wired networks can still be extremely useful in certain cases. There is no single correct network solution, it all depends on the situation and where the location of the devices.

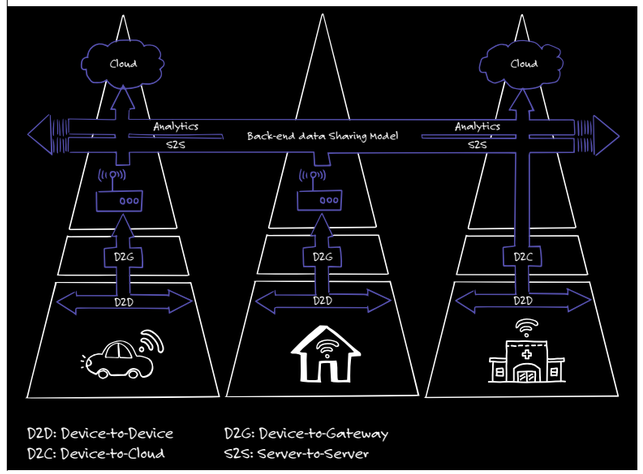
Types of communication models
The International Architecture Board defines four connectivity models for IoT networks that are commonly used for IoT projects.

Device-to-Device
This is used for small amounts of data transfer and generally use short range networks. Commonly used protocols include Bluetooth, ZigBee and Z-Wave. This is popular in home-automation projects where relatively small amounts of data is transmitted infrequently between devices.

Device-to-Cloud
This involves directly connecting an IoT device to the internet. This is generally implemented using Ethernet, WiFi or cellular networks. This is typically used to push data directly to the cloud from the device and enables granular management of the devices. This model enables users to remotely access devices and sensors and can allow for controlling the devices from anywhere or one-way data-transfers to the cloud.

Device-to-Gateway
This generalises into setups where devices to an intermediary device or hub before data is pushed to the cloud. A common example of this are smart watches that connects to a smartphone which manages the data being sent to the cloud. Having hubs or intermediate devices allows for interoperability between devices that use different standards as well as allowing for data to be aggregated or transcoded before being transmitted.

Back-end data sharing
Some IoT projects allow for device and sensor data to be accessible by 3rd parties. This is essentially an extension of device-to-cloud models, with the key addition to greater control and accessibility of the data within the cloud.



COMMUNICATION NETWORKS

The medium used to connect devices is a generally overlooked as wireless is generally the preferred choice due to the inexpensiveness and simplicity of use for IoT systems. However, wired networks provide major advantages with regards to network speeds and security as well as overall reliability.

The options for connectivity include:

Bluetooth
A wireless technology that is great for short distance communication and works within the 2.4 to 2.4835 GHz frequency range.

Cellular
Technologies such as GSM, 3G, 4G, 5G networks work well for transfer of data over long distances.

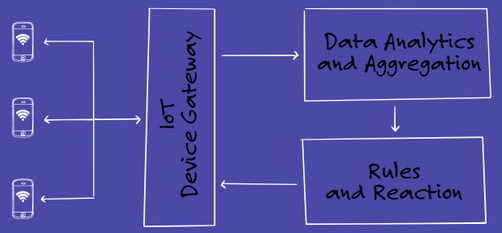
WiFi
Based on IEEE 802.11 family of standards [1] which provide various levels of capabilities regarding frequency bandwidths and speeds.

LoRaWAN (Long Range Wide Area Network)
A protocol designed to work over large distances with low power consumption and is extremely useful for large scale IoT projects. This network standard can handle millions of connected devices transmitting data up to 50 kbps.

NFC (Near Field Communication)
Based of Radio Frequency Identification (RFID) protocols, with a key difference being that NFC enables two-way communication between devices. RFID systems require 2 types of devices for communication, a reader and a tag.

Zigbee
A short-range communication protocol with a range of up to 200m which has become a preferred method of communication for many home automation devices. [39]

CHOOSING THE RIGHT APPROACH



NOW THAT WE'VE LOOKED AT THE COMPONENTS THAT MAKE UP IoT SOLUTIONS, IT'S TIME TO DIVE INTO **THE ARCHITECTURE AND IMPLEMENTATION**.

The design and implementation of an efficient IoT is a complex and challenging task. Large-scale IoT systems harness the scaling capabilities, distributed nature, dynamic attributes and raw computational power of cloud-based resources [40,41,42,43].

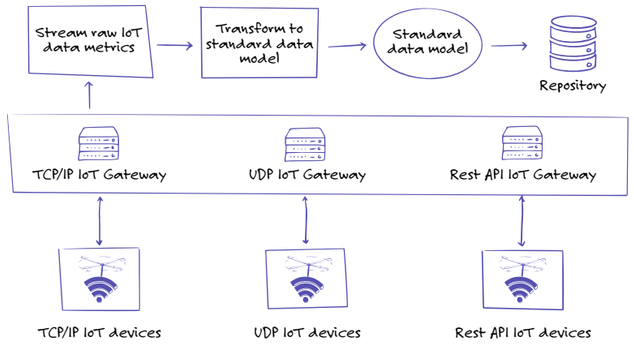
Various aspects influence the architectural design of an IoT system, such as the problem domain, expected scale, devices, metrics and technology stack. Nevertheless, the design of IoT systems generally follows an architectural pattern of distributed components.

Large-scale IoT projects can be broken down into many small devices communicating with each other. While this does not sound overly complex, every new device added to a network brings in more data to manage, another device to monitor, and another connection to maintain.

LEVEL UP YOUR CAREER?

careers@entelect.co.za

PRESS START



IOT DEVICE GATEWAY

The IoT device gateway is the layer responsible for receiving and processing the incoming data metrics of an IoT device. The gateway layer is primarily responsible for overcoming the following set of technical obstacles:

It acts as the primary API or endpoint to consume the data metrics of an IoT device.

It potentially caters to a myriad of different IoT devices where each device implements its own manufacturer-specific, version-specific or protocol-specific (such as TCP, UDP and HTTP) communication.

It transforms the raw device data into a standard data model. The data model is of the utmost importance if the IoT system supports different IoT devices and device communication protocols.

Finally, it persists the data into a repository model for further data analysis and real-time monitoring.

DATA ANALYTICS ENGINE

The data analytics engine is responsible for processing, analysing and aggregating the IoT device data collected from the IDG. The analytics engine is primarily responsible for the following data related operations:

It transforms or aggregates the IoT device data to one or more data models optimised for reporting purposes, front-end user display purposes, or evaluation against a rules engine (next section).

It can harness a multitude of cloud-based resources such as distributed queues or distributed message processors to transform and optimise incoming IoT device data.

RULES ENGINE

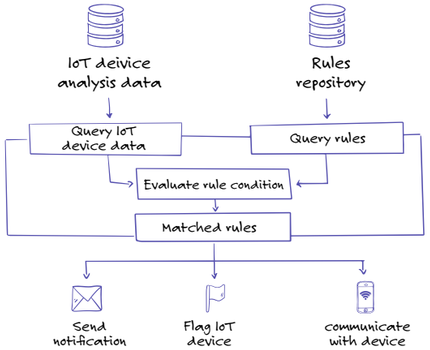
Generally, the purpose of an IoT system is to provide a system capable of reacting to incoming IoT device data. For example, IoT device manufacturers can continuously analyse IoT device data to predict or report malfunctioning IoT devices [44]. Such a reactive IoT system requires a rules engine. The rules engine realises the following set of technical objectives:

It's a platform to set up and define rules. A rule is a set of conditions, and once the conditions of a rule match the data of an IoT device, the rules engine executes the rule.

The execution of a rule generally performs one or more of the following actions:

- The notification of one or more parties via email or SMS.
- Communication with device to prompt a reboot, power-down, etc.
- The execution of additional rules.
- The execution of additional logic such as auditing or flagging a device for maintenance.

The rules engine requires the means to evaluate a rule against IoT device data using a query language or even JavaScript/TypeScript engines. Similar to the analytics engine, one can harness a multitude of cloud-based resources to implement a rules engine such as message processors and streaming analytics.



THE DESIGN COMPLEXITIES OF IOT SYSTEMS

The design of IoT systems corresponds with many design characteristics of large-scale distributed systems, such as:

Separation of concern using micro-services.

Automated scaling of cloud-based resources.

Asynchronous processing of batch data or event data.

However, the intricate design of IoT systems falls victim to the same complexities of large-scale distributed systems, such as:

The identification and debugging of bottlenecks prove complex.

The introduction of distributed components adds a layer of complexity regarding communications, error logging, deployments and security.

Lastly, the design of an IoT system exhibits the following challenges unique to an IoT system:

The processing of vast volumes of IoT device data in real-time.

The authorisation and security of IoT devices, ensuring rogue or malicious devices do not gain entry to the IoT system.

The ad-hoc registration of IoT devices in an IoT system.

The following section provides a list of steps one may potentially consider when designing an IoT system.

SYSTEMATIC DESIGN OF AN IOT SYSTEM

The design and implementation of a large-scale, real-time monitoring and efficient IoT system are intricate. The reader can try to design their own IoT system by conducting the following steps:

1. Determine what IoT devices to monitor. One can use real or simulated IoT devices.
2. Determines the metrics the IoT system monitors and how it reacts to IoT device metrics.
3. Determine the homogeneity of device protocols. If possible, use a single entry point for the IoT device gateway (IDG) and a mature, scalable and efficient IoT cloud-based resource such as Azure IoT Hub.
4. Determine the complexity of the required aggregations on the IoT device data. Incrementally design, expand and improve the data analytics engine (DAE) and rules engine (RE).
5. Identify potential bottlenecks as early as possible.
6. Scale the IoT system out into smaller, scalable, distributed components when necessary.

The design of a robust IoT system capable of large-scale and real-time monitoring of IoT device data is a technically complex task. Fortunately, the use of mature, scalable cloud services in conjunction with proven distributed system design patterns, paves the way for the implementation and use of IoT systems.

HOW DOES IT ALL FIT TOGETHER?

NOW THAT WE UNDERSTAND THE CONCEPTS AROUND IoT **WE NEED TO THINK ABOUT HOW THE SOLUTION IS GOING TO BE PUT TOGETHER** AND THE LIMITATIONS THAT WE WILL ENCOUNTER WITH OUR DESIGNS.

SENSORS

Sensors are often the core focus of an IoT device, they are what make IoT devices unique.

A larger number of sensors means the device will not only cost more to create but will also increase the size of the device. Another thing to consider is the number of pins that a microcontroller contains. Microcontrollers come prebuilt with differing numbers of pins, this means that unless you are designing your own microcontroller or have control over the number of pins the microcontroller you will be using has, you may need an IO expander. There are various types of IO expanders each with their own benefits and drawbacks.

In the case of a fitness watch, adding a lot of sensors will make the watch larger which may impact users negatively as it becomes uncomfortable to wear a large device. It may also negatively affect the longevity of your device as each sensor is vulnerable to damage from movement. For devices that users do not often see, size may not matter as much and wont limit the number of sensors the device can have.

DEVICE STORAGE

In some situations, an IoT device may not have consistent internet connection or the ability to communicate with a central server at all time. In this case it will be necessary to save data locally to the device until a connection can be established and the saved data can be uploaded. Different sensors produce different sizes of data from simple step counting to measuring atmospheric pressure over time, with more sensors on the device, more storage will be required.

In the case of a Fitness watch, physical space is limited and so storage on the device will be smaller than on other IoT solutions. This is especially difficult for Fitness watches as they are often not connected directly to WiFi networks etc and will therefore need to store data locally until a connection can be made to the outside world. Looking at IoT devices that would exist in a smart city, their local storage would not need to be large as they should be in constant contact with central servers and could therefore may not have much local storage.

CONNECTIVITY AND UPDATES

Due to the active nature of the individuals wearing these fitness watches, we cannot expect that the devices will be near to WiFi hotspots. In addition, fitness watches are generally smaller devices that do not provide enough space for a comfortable keyboard for entering credentials for a WiFi hotspot.

These fitness devices also contain information that can be considered personal, and so we cannot expect users to use public hotspots.

Adding a WiFi module also increases the size of the device which can negatively impact user experience. Some solutions around this problem have involved using the user's smartphone to offload data as well as connect to the internet.

UPDATING

Internet connectivity is essential to updating the IoT device software, these updates may include important security patches and fixes. It is also important to consider what type of users will be using the device, as many users may not want to update their device if the updating process is complicated.

DISPLAYING/ REPORTING OF DATA

Users of the device will want to see their data in a form that they can easily understand and gain information from. If the Fitness Tracker is small or it tracks a large amount of data points, displaying the data on the device's screen is not user friendly.

CHAPTER 3

TAKING A STEP BACK

CONSIDERATIONS, COMPLICATIONS AND CONCERNS

GIANT TECH ANALYST COMPANIES AND GARTNER PREDICATED THAT BY 2025 THERE WILL BE 41.6 BILLION CONNECTED IoT DEVICES IN TOTAL. WITH 5.8 BILLION OF THOSE DEVICES CONNECTED BY 2020 BELONGING TO THE ENTERPRISE AND AUTOMOTIVE SECTORS.

We've seen a great advancement of this technology and its capability to create possibilities even in industries where its application was overlooked. This technology is so broad that it touches different points which cannot be ignored. Technical challenges remain but what is even more complex are the legal and developed challenges that are emerging.

The obvious challenge, security, is discussed in detail within this publication and therefore will not be discussed as an area of concern.

VULNERABILITY

However, with that being said, another type of vulnerability that we can discuss is hardware loss or damage if any IoT device is left unattended or exposed. This includes not only troublemakers but also things like harsh external conditions If the device is in a place where it can be easily spotted it can be stolen, and someone can try to extract the data from it, but it can also be blown away, or be hit with debris. Devices today have evolved to be waterproof, yet we still don't have anything that is fireproof or earthquake proof.

Another threat to IoT devices can be seen in the smart farming use case. IoT sensors, used to track the cow's behaviour and temperature, are implanted in multiple locations under the cows. They are expected to perform without fail for at least two years after they have been activated. However, if the cow decides to rub a part of its body where the sensor is located, it may cause damage to the device.

IoT challenges traditional expectations of privacy and it's because of this that it may hold back full adoption of IoT.

IOT STANDARDS

The IoT definition put together by the European Research Cluster (IERC) reads "a dynamic global network infrastructure with self- configuring capabilities based on standard and interoperable communication protocols where physical and visual things have identities, physical attributes and virtual personalities and use intelligent interfaces and are seamlessly integrated into the information network." Notice how this definition recognizes standards and the need for the ability to exchange and make more use of information.

Big vendors such as Amazon, Microsoft, Apple and Google have grown rapidly over the past few years in the IoT market. Each promote their own IoT infrastructure, governing rules, incompatible standards, causing them to operate in silos. They can hardly share an eco-system; this is a limitation to obtaining potential benefits of IoT.

There are bodies which are managing certification programs that will ensure heterogeneous interoperability between IoT devices. The challenges with these initiatives, is that it makes IoT development a bit costlier and therefore vendors are reluctant to adhere to the standards. This area has been a contributing factor and in most cases the reason why most IoT projects fail at proof of concept stage.

A survey done by Cisco highlighted that the devices used to implement the solution are often not designed for the business case.

Companies usually find that they have adopted the wrong Connectivity Plan and with this happening there is no way to identify the reason for connectivity failures which get picked up during testing. Even further, do we as a company have the right plan for testing and deployment?

LEGACY SYSTEMS

Traditional computing differs from IoT. Their traditional computing devices' functionalities vary depending on how the users use them. IoT is different. In IoT, each device is subject to different conditions, e.g. computation and security capabilities. These things could be made by various manufactures that do not comply with common standards. For example; 6LOWPAN is interoperable with other wireless 802.15.4 devices as well as with any IP based devices using a simple bridging device. But in order to bridge between Zigbee and non-Zigbee networks, one requires an advanced application layer gateway.

According to Technopedia, **ZigBee is an open global standard for wireless technology designed to use low-power digital radio signals for personal area networks**. ZigBee operates on the IEEE 802.15.4 specification and is used to create networks that require a low data transfer rate, energy efficiency and secure networking. It is employed in a number of applications such as building automation systems, heating and cooling control and in medical devices. ZigBee is designed to be simpler and less expensive than other personal are network technologies such as Bluetooth. As a result of wireless communication technologies evolving other interoperability issues are:

- Integration issues; network-based integration, independent integration and hybrid integration.
- Other issues; thing–to–thing interaction, virtual representation of things, searching, finding and accessing things and syntactic interoperability between things.
- Alongside security, interoperability is a fundamental for realizing the vision of a global IoT eco-system.

Lack of documented best practices may bring issues like:

- IoT devices behaving badly – unintended interaction between devices. Poor design and configuration may impact network resources they connect to negatively.
- Creation of propriety eco-system.
- Using cheap or inferior hardware to construct the devices.
- Cyber security risk.

All of this being said, there is a lot of work being done by technology corporations to define standard requirements, at an enterprise level and some even proposing an architectural framework for IoT. The IoT market is still maturing, and therefore this may take a while as these efforts are costly and time consuming.

LEGAL, REGULATORY AND RIGHTS ISSUES

This area requires thoughtful consideration as IoT devices are bringing in new complications that didn't exist previously. IoT devices are complicating already existing legal matters, e.g. cross-border data flows, and policy and regulatory bodies are always behind as technology advances rapidly, and so law trails implementations.

THE S IN IOT STANDS FOR SECURITY

"DESPITE CONTINUED SECURITY PROBLEMS, THE IoT WILL SPREAD AND PEOPLE WILL BECOME INCREASINGLY DEPENDENT ON IT. THE COST OF BREACHES WILL BE VIEWED LIKE THE TOLL TAKEN BY CAR CRASHES, WHICH HAVE NOT PERSUADED VERY MANY PEOPLE NOT TO DRIVE."

— RICHARD ADLER

As the movement towards edge computing and IoT enabled devices accelerates so too does the need to securely integrate and connect these devices into larger systems.

This has not been the case in the past as evidenced by the Mirai botnet DDoS [45] attacks that utilised millions of unsecured IoT devices to disrupt services such as Spotify, Netflix, Reddit and Twitter. The architects behind this attack leveraged one key fact; most IoT devices utilise basic default password and username combinations that never get updated. This also highlights the need for robust security in your IoT solutions.

The security concerns surrounding finance and, in particular, access to finance has also been largely affected by the world of IoT. Biometric authentication is one aspect that is prevalent in many areas throughout the finance industry as well as business in general. The technological advancements have allowed biometric data to be captured in many facets of financial business. Fingerprint scanners form a staple for biometric access along with remote controlled cameras which not only record movement of employees and customers but can be used for facial recognition.

The very nature of IoT devices renders a massive network that when compromised, can be very dangerous. This is why the consideration of security with IoT devices is very important.

Digital signatures are a useful tool whereby the device software and firmware, is digitally signed to protect against tampered software being installed on the devices.

The important role that digital signatures play in the world of IoT is two-fold. Firstly, it helps protect against the risks of code tampering and malware from infecting devices and secondly it helps ensure the integrity of the devices because often firmware updates are necessary for both the introduction of new features as well as the fixing of current bugs and problems on the device. Code signing the firmware updates makes sure that the software running on said devices is legitimate.

Some simple, effective and relatively easy to implement security measures would include:

- Incorporating security as a concern in the design process, as opposed to when it is too late.
- Don't use a device with manufacturer set credentials, update these and utilise strong passwords.
- Use public key infrastructure to secure data sent over your network, the need for encryption and protection is especially pertinent when dealing with sensitive personal data.
- Have a means to uniquely identify each device this will help monitor the performance of devices and could go a long way in mitigating the effects of a security breach.
- Update your firmware regularly as outdated driver software can often be an easy point of entry.
- Allow network administrators and security products to monitor network and individual device performance.
- Utilise penetration testing to test and improve your security measures.

Implementing any of the above points could go a long way to making your networks more robust and secure as well as mitigating the extent and impact of an attack. Having security be a priority in the design and implementation phase will protect your networks, customers and give you the ability to expand your networks in a safe and secure manner. [46,47]

ETHICS

THE MORE WE ROBOTISE OUR WORLD, THE LESS WE GOVERN OURSELVES

With sensors being introduced in both public and private spaces they are sure to have a number of implications. The data collected could be driven by financial motivation to either collect more than what is needed and monetise the data [48]. Organisations in this space should look at this in the eye of "should we do this", rather than "can we do this" [48].

Our existing ethical and legal frameworks lack guidance and standards (best practices) that can hold organisations accountable in the era of the internet freedom. There is little in place that can be used to protect the user.

LET'S LOOK AT SOME IMPLICATIONS

In the words of Emily Taylor "we have come to tolerate an incredibly exploitative deal in return for free services" [49]. All those freemium apps we use on our phones, tablets etc. are "free" for a reason; but what is the consumer giving up using those apps? The organisation that owns the app owns the data generated by the app and uses it for its own benefit. Their only obligation to you is to provide that "free service". This is the price we pay to lose the ability to control how our images, videos or data are is used/ interpreted on the internet [49].

Big Brother is watching – when individuals know that every movement, they make is being monitored; it gets in the way of them behaving like they would under "normal circumstances" - It is an intrusion of privacy.

There is another concept which ties up with this one, around increased surveillance. There won't be a need for government to set up infrastructures to collect this data, instead they can ask for access to it from institutions who are already collecting data about people [50]. This can also be viewed as repurposing of data; how do we manage instances where data is used outside of context it was collected/ intended for? [51]. There are laws appearing that address this, including The European Union's GDPR, but there are still many regulatory gaps.

Implications around freedom of association – in an instance where a candidate makes an application in order to be part of a club, currently one would fill in a form with the required details, in future the organisation could just ask for an ID number and then extract data about you and that would dictate whether they will accept you as a member or not. Imagine going for an interview and someone has already pulled out a report about you. You cannot alter this data. As much as you generated it, you have no access to it [51].

Who owns the data? Organisation possess the data that is generated by consumers. Consumers have no say or control over how this data is used, how long it's kept, whether it can be shared. Organisations rarely give consumers the option to withdraw their data. It is a complication. What measures are in place to protect the identity of the users. Security on IoT devices is generally so flawed that, if tampered with, they might expose sensitive information [52]. Even when the privacy has been breached on these devices; will there be signs of this kind of activity? Which brings in accountability issues – since these devices are programmed by humans who is held responsible if their failure threatens someone's safety? An example of this is autonomous vehicles. How do we manage the governance of the internet and its networked component? A loss of networks could be determined and impact critical function in our daily lives e.g. medical organisations [53].

End of life – There is a need to take care of these IoT devices we purchase and use, e.g. everyday labour of maintenance but also responsibility for what becomes out of them. Many IoT start-up companies fail within first 2 years. Sometimes they do not go under but may be bought or merged into other companies, meaning their products reach the "end of life". Their devices and applications are still widely used. But now who will take responsibility of the "becomings" of their products is very costly. People move countries, jobs, sectors. Sometimes as a developer you want to move on from previous ventures/projects, emotionally detach themselves and no longer want to be associated with that particular project. This is unfair for end-users because now it means that their devices are at risk, e.g. breached, attacked, or stop being supported altogether. After spending their hard-earned money. IoT ethical challenges go beyond data ethics. The concern about the end of life is not only about what happens to the data but that the 'life' of the product raises important ethical questions about what and who the developers acre about – investors, end-users, environments [54].

An example of this would be the Revolv's smart home hub. The startup was acquired by Google in 2014. The hub included a range of different IoT devices, e.g. connected lights via smartphone app. This came with a $300 price tag. Once the company was sold to Google there was an announcement made that the cloud service privately offered to them would be shut down. This meant that Revolv would stop working entirely. The price tag is one thing: what about wearables in the health sector? What if a heart chip stop working when the company producing it changes hands or no longer supports the chips sold? [54]

Where do we draw the line between the ethical and unethical use of data?

CONCLUSION

"AS THE INTERNET OF THINGS ADVANCES, THE VERY NOTION OF A CLEAR DIVIDING LINE BETWEEN REALITY AND VIRTUAL REALITY BECOMES BLURRED, SOMETIMES IN CREATIVE WAYS."

— GEOFF MULGAN

The promise of IoT is a large one – a connected world, data about almost everything used for predictions, monitoring leading to lower costs, better health, smarter homes, energy-efficient cities, safer factories and more. These promises may be achievable but the IoT revolution is not without its downsides in the form of security concerns, privacy concerns, ethical concerns and more. It's the responsibility of those of us designing and implementing such solutions to ensure that we don't sacrifice privacy, security or similar.

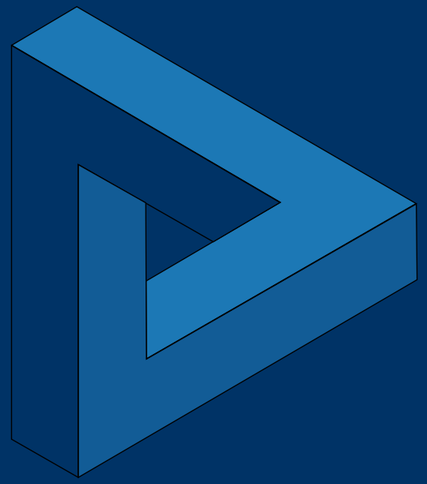
WHO MADE THIS

A LIST OF CONTRIBUTORS

Arohan Naidoo
Duane McKibbin
Gail Shaw
Gerard Gouws
Greg Schroder
James McGuire
Jason Evans
Jolene van Heerden
Kurt Lourens
Mark Jones
Matthew van der Velden
Mohammed Ismail
Privolin Naidoo
Refilwe Molekwa
Rishal Hurbans
Sophie Laher
Vincent Chegwidden
Warren Bonn

REFERENCES

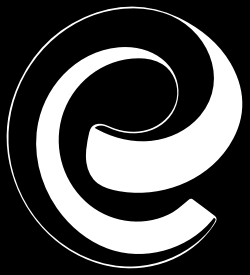
1. https://www.bbvaopenmind.com/en/technology/digital-world/the-internet-of-everything-ioe/
2. https://www.linkedin.com/pulse/internet-things-iot-characteristics-kavyashree-g-c
3. https://www.theguardian.com/technology/2017/nov/18/germany-bans-childrens-smart-watches-over-surveillance-concerns,
4. https://www.theguardian.com/technology/2019/feb/05/eu-recalls-childrens-smartwatch-over-data-fears
5. https://www.vox.com/recode/2019/12/27/21039517/amazon-ring-hacking-lawsuit
6. https://threatpost.com/alexa-google-home-eavesdropping-hack-not-yet-fixed/151164/
7. https://www.vice.com/en_us/article/9395be/the-hacker-in-my-ring-camera-a-tale-of-trolls-and-a-podcast,
8. https://player.fm/series/reset-2555404/maybe-dont-put-a-ring-on-it
9. B. Buntz, "The Top 20 Industrial IoT Applications," IoT World Today, Sep. 2017. https://www.iotworldtoday.com/2017/09/20/top-20-industrial-iot-applications/ (accessed May 24, 2020).
10. C. Gupta, A. Farahat, T. Hiruta, K. Ristovski, and U. Dayal, "Collaborative Creation with Customers for Predictive Maintenance Solutions on Hitachi IoT Platform," Hitach Rev., vol. 65, no. 9, pp. 403–409, 2016.
11. W. Knight, "Inside Amazon's Warehouse, Human-Robot Symbiosis," MIT Technology Review, Jul. 2015. https://www.technologyreview.com/2015/07/07/248370/inside-amazons-warehouse-human-robot-symbiosis/ (accessed May 24, 2020).
12. K. Field, "IIC Testbeds Take IoT Use Cases Out of the Lab and into the Real World," IoT World Today, May 2016. https://www.iotworldtoday.com/2016/05/02/iic-testbeds-take-iot-use-cases-out-lab-and-real-world/ (accessed May 24, 2020).
13. Thyssenkrupp Elevators, "MAX: The game-changing predictive maintenance service for elevators.," Thyssenkrupp Elevators, Germany, Brochure, 2016.
14. A. Khan, M. Pohl, S. Bosse, S. W. Hart, and K. Turowski, "A Holistic View of the IoT Process from Sensors to the Business Value," presented at the Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, 392-399, 2017, pp. 392–399, doi: 10.5220/0006362503920399.
15. https://www.wareable.com/fitness-trackers/how-your-fitness-tracker-works-1449
16. https://www.wareable.com/health-and-wellbeing/vo2-max-guide-understand-and-increase-789
17. https://www.ncbi.nlm.nih.gov/pubmed/3525187
18. https://www.slant.co/topics/7363/~fitness-trackers-with-an-altimeter
19. https://www.nationalgeographic.org/encyclopedia/geographic-information-system-gis/
20. https://www.wareable.com/health-and-wellbeing/vo2-max-guide-understand-and-increase-789)
21. https://www.cnet.com/news/apple-watch-ecg-app-what-cardiologists-want-you-to-know/
22. https://www.mn.uio.no/fysikk/english/research/projects/bioimpedance/whatis/
23. https://www.discovery.co.za/vitality/vitality-active-device-benefit
24. https://www.statista.com/statistics/610433/wearable-healthcare-device-revenue-worldwide/
25. https://www.androidcentral.com/best-smart-scales-for-tracking-weight-loss
26. https://www.espressif.com/en/products/socs/esp32/overview
27. https://learn.sparkfun.com/tutorials/iot-weight-logging-scale/all
28. https://techcrunch.com/2017/09/30/motivs-fitness-ring-is-simple-but-surprisingly-capable/
29. https://www.wareable.com/fitness-trackers/oura-ring-study-illness-early-warning-7943
30. https://www.techradar.com/news/are-fitness-trackers-the-future-of-healthcare
31. https://www.wired.com/story/mojo-vision-smart-contact-lens/
32. https://www.washingtonpost.com/business/technology/googles-smart-contact-lens-what-it-does-and-how-it-works/2014/01/17/96b938ec-7f80-11e3-93c1-0e888170b723_story.html
33. https://en.wikipedia.org/wiki/Artificial_pancreas
34. https://www.hanselman.com/blog/TheExtremelyPromisingStateOfDiabetesTechnologyIn2018.aspx
35. https://openaps.org/
36. https://www.researchgate.net/publication/330327990_Intelligent_Monitoring_and_Inspection_of_Power_Line_Components_Powered_by_UAVs_and_Deep_Learning
37. https://blog.resellerclub.com/what-is-the-role-of-cloud-computing-in-iot/
38. https://www.businessinsider.com/iot-cloud-computing
39. Explaining WiFi standard. https://www.netspotapp.com/explaining-wifi-standards.html
40. C. Sarkar, A. U. Nambi, V. Prasad, and A. Rahim, "A Scalable Distributed Architecture TowardsUnifying IoT Applications," presented at the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, Mar. 2014, pp. 508–513.
41. G. Fortino, W. Russo, C. Savaglio, W. Shen, and M. Zhou, "Agent Oriented Cooperative Smart Objects: from IoT System Design to Implementation," EEE Trans. Syst. Man Cybern. Syst., vol. 48, no. 11, pp. 1939–1956, Nov. 2018.
42. A. Yassine, S. Singh, M. S. Hossain, and G. Muhammed, "IoT Big Data Analytics for Smart Homes with Fog and Cloud Computing."
43. Stefan Nastic, S. Sehic, D.-H. Le, H.-L. Truong, and S. Dustdar, "Provisioning Software-defined IoT Cloud Systems," presented at the 2014 International Conference on Future Internet of Things and Cloud (FiCloud 2014), Barcelona, Spain, Aug. 2014, pp. 288–295.
44. A. Adnan et al., "Real-Time Probabilistic Data Fusion for Large-Scale IoT Applications," IEEE Access, vol. 6, pp. 10015–10027, Feb. 2018.
45. https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/,
46. https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security,
47. Digicert executive interview: https://soundcloud.com/helpnetsecurity/why-we-need-to-secure-iot-connections-sooner-than-later
48. https://www.internetsociety.org/policybriefs/responsible-data-handling/
49. https://www.treehugger.com/solar-technology/solar-smart-greenhouses-produce-both-clean-electricity-food-crops.html
50. http://www.digitaljournal.com/business/caterpillar-is-an-iiot-hipster-they-ve-been-on-it-since-the-90s/article/530822
51. https://www.youtube.com/watch?v=EW65AZ9WetQ
52. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf
53. https://royalsociety.org/science-events-and-lectures/2017/10/tof-internet-of-things/
54. https://medium.com/@VIRT_EU/ethics-beyond-data-how-does-iot-challenge-our-perspective-on-data-ethics-df6952745adc



NEED HELP GOING DIGITAL?

START THE CONVERSATION

solutions@entelect.co.za



entelect.co.za