CYBERSECURITY AND THE CHALLENGES OF CLOUD CONNECTIVITY

Here, Gabrielle Whitworth-Smith, Engineering Consultant, and Thomas Watts, Engineering Consultant, both of Team Consulting, look at the benefits and risks associated with cloud connectivity and the accompanying cybersecurity challenges.

For the past few years, cloud connectivity has been creeping into every aspect of our lives, from doorbells to smart meters that track our energy usage. In the medical device and healthcare industry, cloud connectivity has the potential to unlock a wealth of benefits, both for the user and the manufacturer. Before you can begin, however, you first need to consider what you are trying to achieve and which technology best suits your needs. Building in cloud connectivity can also open up a host of cybersecurity challenges that need to be navigated, so it is important to be fully prepared for what this will involve when starting out on your development.

WHAT PROBLEMS CAN CLOUD CONNECTIVITY HELP SOLVE?

From allowing patients to share data about their condition and treatment direct with their clinicians, to offering manufacturers valuable insights into how their devices are being used, there are many reasons to consider building cloud connectivity into your system. While cloud connectivity can seem appealing, it is important to know exactly which problems you are seeking to solve with this technology before committing to building it into your development. Here are some of the common problems cloud connectivity can solve:

> "Monitoring aspects of device use with real patients can provide data to allow early identification of any malfunctioning devices or unforeseen use cases."

Post-Market Surveillance

With medical device regulation requiring more rigorous post-market surveillance, manufacturers need to proactively collect and review experience gained from their devices on the market. Cloud connectivity offers a means to collect this data in real time. Monitoring aspects of device use with real patients can provide data to allow early identification of any malfunctioning devices or unforeseen use cases.

Patient Adherence

Cloud connectivity can also be used to encourage adherence by tracking elements of patient interactions and providing more targeted feedback. For example, data can be gathered on a patient's administration approach and fed back to help improve their technique and efficacy. Tracking medication dosage and delivery time can also help patients manage their conditions through the use of reminders and alerts, while use data can also keep patients' clinicians informed.

Data Processing

You may wish to have some of your processing and analysis take place directly on your app, which can allow you to display information in real time to the patient. One of the benefits of cloud connectivity, however, is that potentially complex analysis and power-hungry data analytics can be sent to the cloud, allowing the hardware in the device to be kept simple and low cost. In addition, algorithms can continue to be developed and improved if calculations are performed offline.

How Can I Make My Device Connected?

Fundamentally, a cloud connected system collects, stores and shares data to servers accessed over the internet. When considering adding cloud connectivity to a device, it is important to determine how the data are going to be transferred to the cloud (Figure 1).

Gabrielle Whitworth-Smith
Engineering Consultant
T: +44 1799 532 700
E: gabrielle.whitworth-smith@team-consulting.com

Thomas Watts
Engineering Consultant
T: +44 1799 532 700
E: thomas.watts@team-consulting.com

Team Consulting
Abbey Barns
Duxford Road
Ickleton
Cambridge
CB10 1SX
United Kingdom

www.team-consulting.com

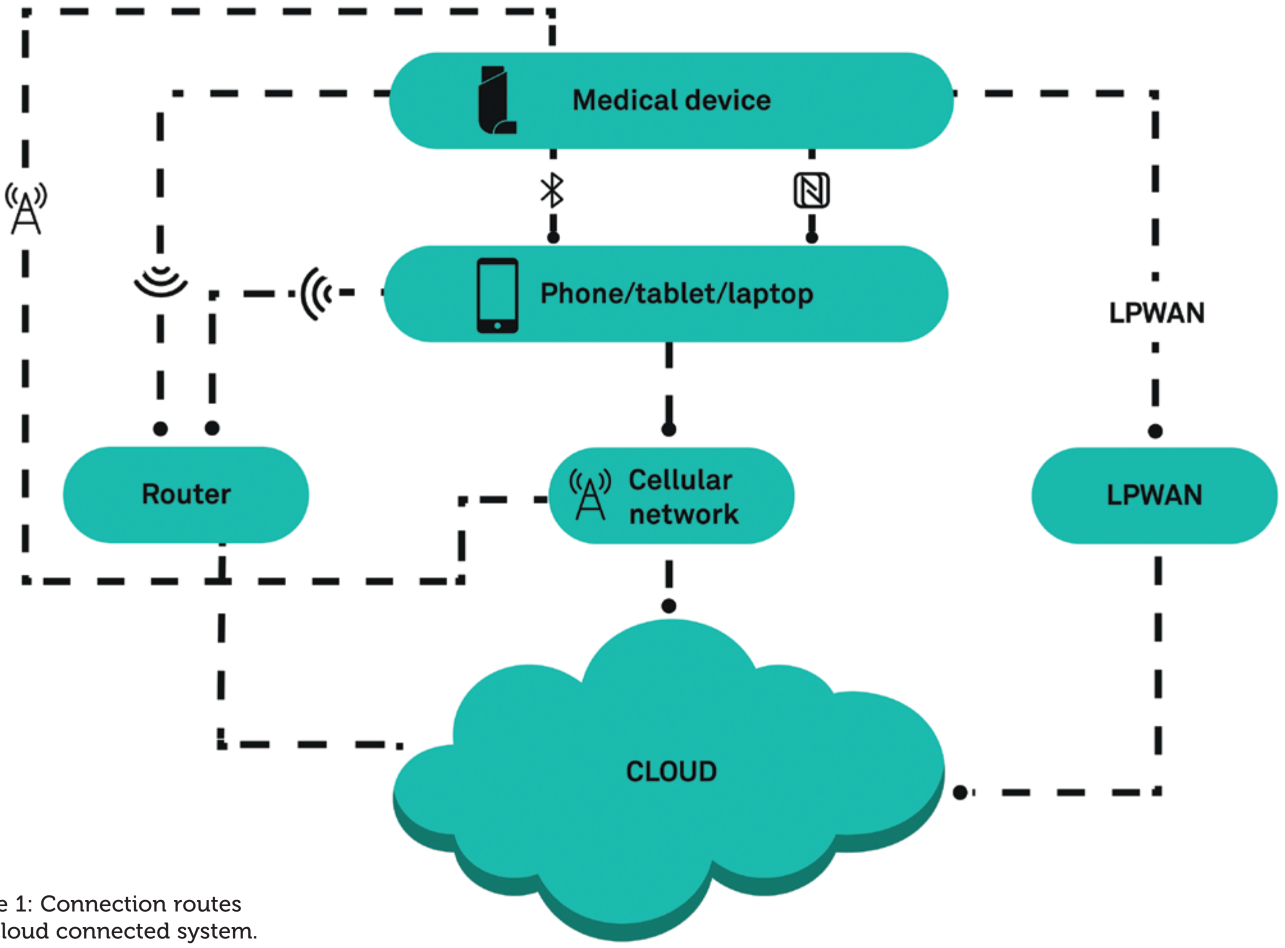


Figure 1: Connection routes of a cloud connected system.

> "A smartphone approach to cloud connectivity presents an opportunity to build a custom smartphone app to help facilitate this, offering engaging ways to present the data back to the user, as well as a variety of other benefits."

Smartphones are a popular choice for facilitating this transfer. Using Bluetooth, Bluetooth low energy (BLE) or near-field communication (NFC), data can be sent from medical device to a user's phone. From the phone, data can be transferred to the cloud servers using its active network connection. It is worth noting that if the user's phone is connected via cellular networks this will add costs for the user.

Another mechanism to implement cloud connectivity is to build Wi-Fi, cellular or low-power wide area network (LPWAN) connectivity into the medical device directly, and access the cloud through a router, a cellular network or base station.

Once the data has been collected, you then need to consider how it will be analysed and displayed using a dashboard. A smartphone approach to cloud connectivity presents an opportunity to build a custom smartphone app to help facilitate this, offering engaging ways to present the data back to the user, as well as a variety of other benefits. It is also worth investigating how data could be shared and integrated with existing healthcare systems, such as electronic patient records, if this would be beneficial.

Which Connectivity Approach Should I Use?

When choosing an approach to relay data to the cloud, it is important to consider system requirements regarding power, range, speed and cost.

	Bluetooth / BLE
Features	• Low power (BLE) • Medium range • Medium data transfer rate • Well adopted among many modern devices • Existing support for making Bluetooth devices secure.
When to use it	**You want to provide a rich user interface** Bluetooth connectivity typically involves using a smartphone as a gateway, which creates the opportunity to develop a rich user interface via an app. **You have a low-power device** BLE has low power requirements for wireless communications, enabling connectivity to be added without needing significantly larger batteries.
Challenges	**Gateway device required** Bluetooth often requires a smartphone or similar device to act as a gateway to the cloud, although there are now routers with Bluetooth radios as well as Wi-Fi that allow BLE devices to connect directly. **Cybersecurity and user engagement** Pairing and bonding a device via Bluetooth will involve extra security steps, while exchanging encryption keys to protect data during transfer. This additional security may also require user to facilitate the bonding process.

NFC	
Features	• Low power • Short range • Low data transfer rate • Cheap.
When to use it	**Minimal data to transfer** NFC offers a low-cost and low-energy approach to extract data from a device. In some cases, the sensor could be powered passively, removing the need for an onboard battery.
Challenges	**Data packet size** This approach is only useful when a small amount of data is being transferred. A purely NFC solution does not provide continuous sensor monitoring **Data download and user interaction** You will need to consider how to make using the NFC feature a natural part of the user steps **Gateway device required** NFC requires a smartphone or reader device to act as a gateway to reach the cloud.

WiFi	
Features	• High power • Medium range (further than Bluetooth) • High data transfer rate • Widely available.
When to use it	**Static devices** Useful for devices which remain in one location **You need to transfer large volumes of data** With high-speed data transfer, Wi-Fi offers an effective connection to transfer larger volumes of data.
Challenges	**Range of use** The device needs to remain in range of the router to transfer the data to the cloud. **Access credentials** How to share access credentials on initial set-up of "headless" devices can be challenging.

Cellular	
Features	• Long range • High speed • Global coverage • Easy to scale, using existing network.
When to use it	**Operating in remote locations** You are able to get access to the cloud in places where Wi-Fi might not be available. **Non-static devices** Useful for devices which move around and don't remain in one location.
Challenges	**Power hungry** High data rate cellular, such as 5G, can consume significant amounts of power. However, LPWAN can provide a lower power alternative at the cost of lower data rates. **Additional costs** Cellular access incurs an additional cost from paying the mobile network provider for access, and the hardware solution component cost is also more expensive.

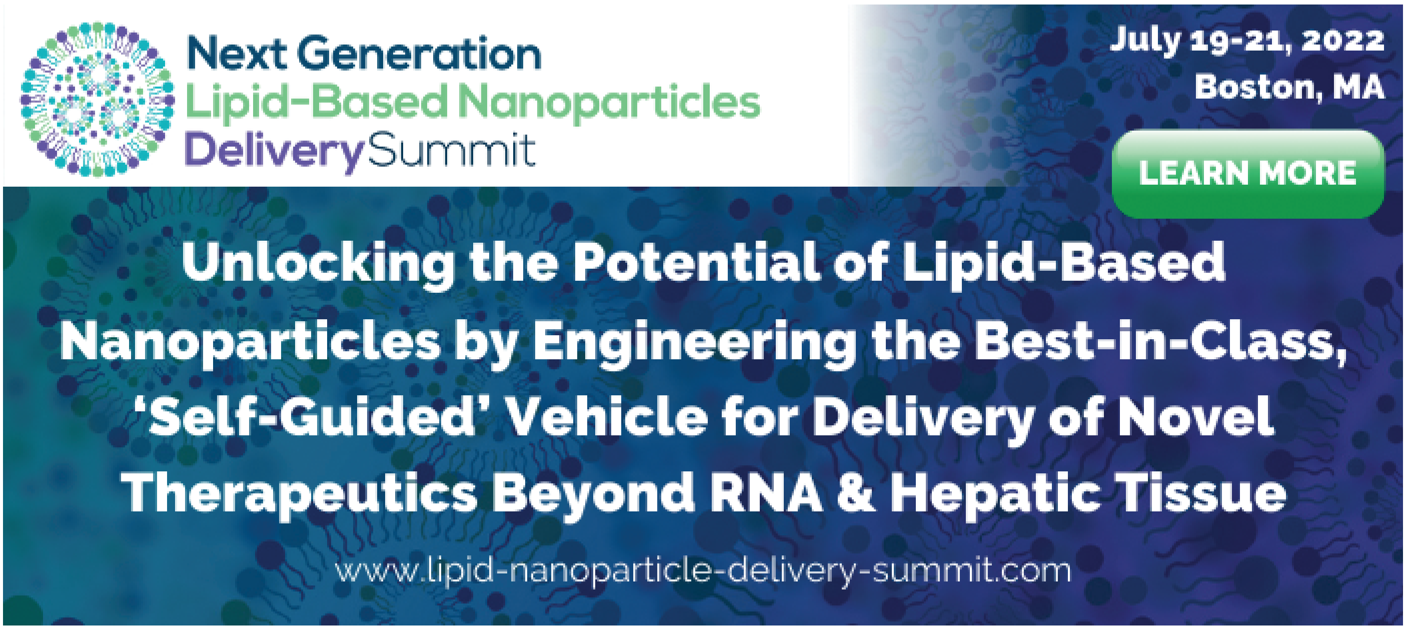
Cloud Services

When considering a cloud-based system, you need to decide whether to use an existing provider or if you want to create your own private cloud. Typically, existing cloud providers will have great tools to help with analysis and can enable fast set up, however, they will come with a regular fee.

Some of the main cloud service providers currently available are:

1. Google Cloud Platform
2. Amazon Web Services (AWS)
3. IBM Cloud Services
4. Microsoft Azure.

There are, of course, some benefits to creating your own private cloud. This approach will have a lower cost in the long run compared with the existing providers, which become more expensive as you



> "The level of cybersecurity protection within your system will be driven by the severity of harm that could be caused if a breach were to occur."

scale up. In contrast, creating your own will require a higher upfront cost but a lower cost as you scale up. When designing your system, it is typically best to design and architect it in such a way as to make it easy to transfer over to a private cloud either way. It is best not to be too reliant on one provider of specific cloud service tools as this will make migration between platforms more challenging, and it exposes your platform to risks associated with suppliers removing services and tools.

WHAT ARE THE CHALLENGES OF MAKING YOUR DEVICE CONNECTED?

Costs

Along with the many benefits that cloud connectivity can offer, there are, of course, also significant challenges. Adding cloud connectivity to a device will incur higher development and device costs due to the additional hardware and software required. Incorporating any electronics into a device will also result in a higher carbon footprint, increasing the environmental impact of the development. There will also be continuous maintenance costs for cloud hosting services and to support post-launch application updates, for example, maintaining compatibility with mobile operating system upgrades. It is important to weigh up the benefits that connectivity will bring against these increased costs.

Cybersecurity

Patient Safety

When determining the cybersecurity protections necessary for your system, the potential risks of a malicious or unauthorised user accessing different elements of your system should be considered. For example, could they intercept the data being transferred from the device to the user's phone? What harm could be caused if they manipulate the data undetected? Serious injury? Death? The level of cybersecurity protection within your system will be driven by the severity of harm that could be caused if a breach were to occur. It is equally important to consider what would occur if the system were susceptible to a denial-of-service attack and what harm could result to the patient if they were not able to access the system.

Data Privacy

In addition to patient safety, data privacy is also paramount to avoid large fines and protect your organisation's reputation. Compliance with data privacy regulations is key when handling healthcare data. For example, in the US Health Insurance Portability and Accountability Act, compliance must be demonstrated that an organisation has protected the privacy, security and integrity of protected health information.

Approach

Because of the potential risks of cybersecurity attacks, cybersecurity management for connected devices is of high importance, and the regulatory authorities are putting a lot of emphasis on this. The Association for the Advancement of Medical Instrumentation has published a guidance document for cybersecurity management of medical devices called "TIR57 Principles for medical device security – Risk management", which describes how to perform cybersecurity risk management within the requirements of the ISO 14971 standard. As part of the cybersecurity risk management, a threat model and threat analysis are performed to establish possible routes of attack, vulnerable assets to protect and the mitigations to put in place. Typical mitigations include end-to-end encryption of data, device authentication and keeping regular data back-ups. Penetration tests are carried out to investigate the existing protection and help identify any security issues. The important thing to remember is that cybersecurity should be considered early on in device development and not as an afterthought.

CONCLUSION

There are clearly many benefits and challenges that come with integrating cloud connectivity into a device. System requirements should be considered from an early stage, and make sure you choose the appropriate connectivity approach to best suit your needs. But most importantly, you need to ensure you have a clear plan for how you are going to use your connected solution. Do not expose your device to the challenges that accompany cloud connectivity without first understanding what benefit it will bring to both the device developer and the patient.

ABOUT THE COMPANY

Team Consulting is a leading medical device design and development consultancy focusing on the pharmaceutical and healthcare industries. Team is an expert in drug delivery device development and works with companies both large and small across Europe, the US and beyond. Combining its expertise and experience in industrial design, engineering and human factors, Team develops medical devices from early concept through to commercial launch. Team is accredited to ISO 9001:2000 and 13485:2003.

ABOUT THE AUTHORS

Gabrielle Whitworth-Smith is an engineering consultant at Team Consulting. In her role, Ms Whitworth-Smith applies her background in biomedical engineering to a wide variety of ongoing and potential projects. She has a first-class MEng Honours degree in Biomedical/Medical Engineering from Imperial College London (UK).

Thomas Watts is an electronics and software engineer at Team Consulting, where he specialises in embedded software development for medical devices. Before joining Team, Mr Watts worked for a company focusing on neonatal ventilator systems. He has an MEng in Biomedical Engineering from Imperial College London (UK).