Hospital Network IoT Implementation

(Smart IoT deployment)

Table of Contents

Hospital Network IoT Overview 2

IoT Implementation and Architecture 3

- IoT Architecture Overview 3
- Elements of the IoT architecture 5

IoT Security Components 6

- Network IoT Security 6
- Cloud IoT Security 8

Author: George Price – Group 1

Hospital Network IoT Overview

Smart networks often heavily rely on several IoT devices which are intelligently deployed and managed, acting as sensors and tools to gather and communicate critical system information that facilitates the organisation's operational needs. Modern hospital networks are perhaps one of the best examples of an organisation's heavy reliance on IoT devices. For this reason, the hospital network design accommodates adequate and secure IoT architecture.

For context, here is a quick table of IoT devices that would be used in the actual operational use of the smart hospital network and information systems (Table 1).

IoT Type	Examples	Physical Nature
Patient monitoring devices	blood pressure monitors, glucose monitors, heart rate monitors, sleep monitors, connected inhalers, and smart thermometers.	• Bluetooth, WIFI, 5G, cabled connectivity. • On hospital premises. • At home use. • Patient outcall, emergency vehicles.
Medical machines and devices	MRI machines, CT scanners, Ultrasound machines, X-ray machines, Mechanical Ventilators, Research Equipment, etc.	• Bluetooth, WIFI, and cabled connectivity. • On hospital premises.
Medical staff devices	tablets, laptops, workstations, and hand-held devices used to access electronic patient records and treatment data.	• Bluetooth, WIFI, and cabled connectivity. • On hospital premises.
Patient devices	unsecured tablets, laptops, and mobile phones.	• WIFI connectivity. • On hospital premises.
Environmental sensors	room temperature sensors, air quality sensors, and bed sensors.	• Bluetooth, WIFI, and cabled connectivity. • On hospital premises.
Security sensors	security cameras, fire sensors, alarms, biometric sensors, etc.	• Bluetooth, WIFI, 5G, cabled connectivity. • On hospital premises. • On emergency vehicles.

Table 1. Types of IoT devices commonly used at a hospital.

IoT Implementation and Architecture

Hospitals handle and store an enormous amount of sensitive information daily, from patient records, emergency procedures, operational activities, communications, IoT medical device handling, to security-related information streams.

This raw volume of data is overwhelming for people to handle securely and effectively. So, the use of AI-assisted solution has become popular with healthcare organisations. Analytics are also a very effective tool in processing, understanding, interpreting, and communicating significant patterns and insights drawn from data, especially with the assistance of Artificial Intelligence (AI) and Machine Learning (ML). Combined, these cutting-edge technologies will go a long way in making this hospital's network truly 'smart'.

AWS IoT Core is well equipped with prebuilt tools to handle a large array of devices for complex organisations. Amazon has a range of products that specifically service the needs of healthcare organisations, such as medical IoT device handling, Comprehend Medical AI, HealthLake ML, Research Tools, smart Patient Dashboards, and so on. For more details, please refer to these documents:

- Hospital AI Recommendations (Group1-Hospital-AI-Recommendations.docx).
- AI & Analytics Research (Group1-Research-AWS-Analytics-and-AI.docx).

IoT Architecture Overview

The illustration below (Figure 1) is the IoT architecture design for this smart hospital network, heavily incorporating the use of IoT integration into the AWS Cloud. From left to right, the three panels (sections) are explained:

External IoT Devices (left panel, Figure 1): Hospital personnel and contractors utilise a large array of IoT devices away from the main building, from ambulance crews, outcall patient care, to third-party partners; requiring uninterrupted connectivity to hospital systems. AWS IoT Greengrass Core (Amazon Web Services, 2019) is a flexible management system for large volumes of IoT devices on the edge, or remotely located, securely and efficiently handling IoT communications (with asymmetrical encryption, and encrypted protocol use). Greengrass can also handle external patient care IoTs, managing wearable devices such as Pacemakers, glucose monitors, etc.

AWS Cloud, IoT Management (middle panel, Figure 1): In the Amazon Cloud, the AWS IoT Core (Amazon Web Services, 2019) is structured to handle all aspects of IoT management, and this is where both the external and on-premises devices securely communicate via the MQTT broker. Each IoT must be registered with AWS IoT Core as a Thing, where X.509 certificates and encryption keys are generated for each device. In the cloud, all the registered IoTs data communications are stored and further processed using Analytics, Machine Learning, and AI tools.

On Premises IoT Devices (right panel, Figure 1): All IoT devices on premises of the hospital will connect through local network IoT servers, to be registered, managed, secured and communicated through. The hospital network provides wireless and wired IoT connectivity. However not all IoT devices are processed intelligently through the AWS cloud. There are some IoTs that only need local monitoring (such as door sensors), and there are devices that won't be permitted to communicate with AWS IoT Core, such as patient BYOD devices, and staff use workstations.

Devices that have a reason to be integrated into the AWS Cloud, can be set up to do so, while also registered and handled locally. This allows 24/7 availability and functionality for critical medical devices and services, in the event of internet or cloud service failures.

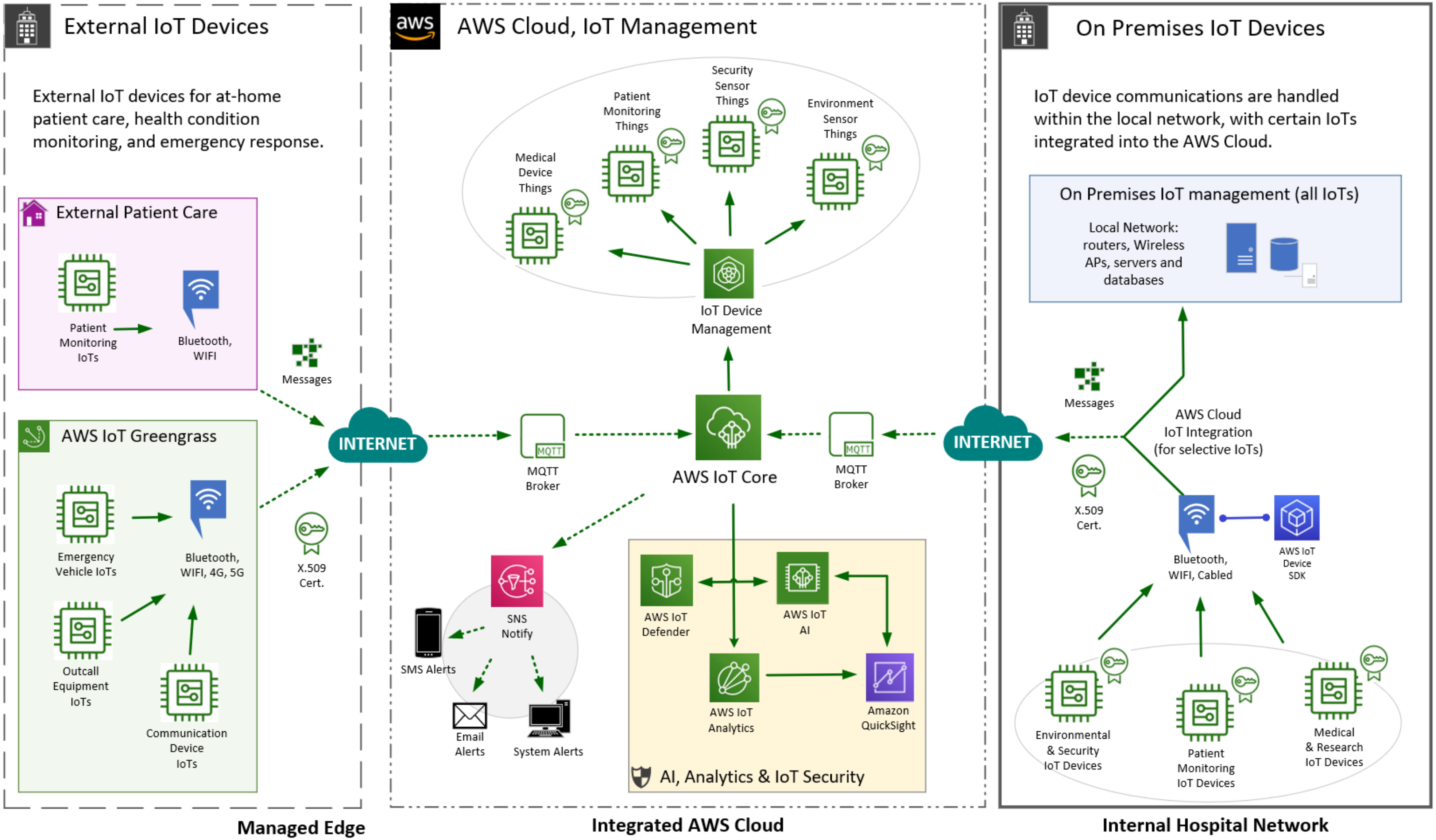
External IoT Devices
External IoT devices for at-home patient care, health condition monitoring, and emergency response.
External Patient Care
Patient Monitoring IoTs
Bluetooth, WIFI
Messages
AWS IoT Greengrass
Emergency Vehicle IoTs
Bluetooth, WIFI, 4G, 5G
Outcall Equipment IoTs
Communication Device IoTs
X.509 Cert.
INTERNET
aws
AWS Cloud, IoT Management
Medical Device Things
Patient Monitoring Things
Security Sensor Things
Environment Sensor Things
IoT Device Management
MQTT
MQTT Broker
AWS IoT Core
MQTT
MQTT Broker
SNS Notify
SMS Alerts
Email Alerts
System Alerts
AWS IoT Defender
AWS IoT AI
AWS IoT Analytics
Amazon QuickSight
AI, Analytics & IoT Security
INTERNET
On Premises IoT Devices
IoT device communications are handled within the local network, with certain IoTs integrated into the AWS Cloud.
On Premises IoT management (all IoTs)
Local Network: routers, Wireless APs, servers and databases
Messages
AWS Cloud IoT Integration (for selective IoTs)
X.509 Cert.
Bluetooth, WIFI, Cabled
AWS IoT Device SDK
Environmental & Security IoT Devices
Patient Monitoring IoT Devices
Medical & Research IoT Devices
Managed Edge
Integrated AWS Cloud
Internal Hospital Network

Figure 1. IoT Architecture for the smart hospital network, displayed in three panels, from left to right.

Author: George Price – Group 1

AWS IoT Analytics. Analytics are implemented in the IoT network (refer to the middle panel in Figure 1), providing smart data handling of medical devices and other IoT sensors. Amazon SageMaker and QuickSight tools are used to set up the ingesting, storing, processing, and outputting of the IoT data. The analytics data flow is shown in Figure 2, illustrating the key components in use.

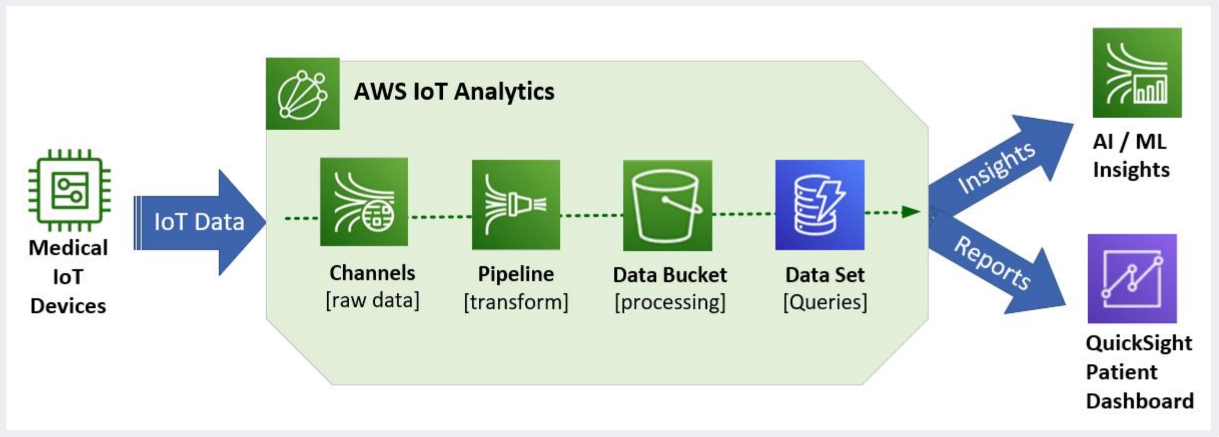

Figure 2. How the data flows from the IoT device to a graphical output, or AI/ML assisted smart data processing.

AWS System Notification System (SNS). Notifications are configured for IoT devices, such as a high heart rate from the Pacemaker-IoT that will trigger an SMS text or email, or a system alert to the appropriate medical staff. SNS leverages the monitoring and auditing tools provided by AWS, and the AI/ML smart processing of IoT data, allowing alerts and alarms to be triggered when certain conditions are reached. This allows for greater security controls, more accurate device health and correct-use monitoring, quicker emergency response to critical patient monitoring devices, as well as identification/quarantining of compromised devices.

Elements of the IoT architecture

The elements that make up the hospital's IoT deployment and management are:

I. **IoT Devices.** The hospital requires the integration and use of many IoT devices and sensors. Some are simple sensors like temperature detectors, smoke alarms and security cameras. Other devices are medical and patient care IoTs such as patient monitoring devices, medical machines, diagnosis equipment, and laboratory IoTs. More complex IoTs also share the network, such as laptops, tablets, PDAs, and handheld patient care devices.

II. **Gateways.** A secure deployment of access points acts as the entry and exit gateway of the hospital network, through wireless connectivity to the IoTs. The wireless IoTs connect using WPA3-Enterprise 802.1X for authentication and encryption. Access is also controlled based on IP address and MAC address filtering.

III. **Switches and routers.** Additional distribution network hardware and cables are required to deploy gateways in prime coverage positions, and provide the required security elements of network segregation, firewalls, and access control.

IV. **IoT Servers.** Once IoT traffic enters the network, their communications are passed to the servers and services that manage the device registration and handling within the network.

V. **IoT Applications.** Many IoT devices are integrated parts of services and treatment procedures carried out within the hospital. For example, Medical IoT devices facilitate the diagnosis, treatment, monitoring, and post-care of patients. Different applications and enterprise healthcare solutions are installed on the hospital system, or provided through the cloud, which then handle the ingested IoT data. From there the data is used accordingly.

VI. **IoT Data lake/warehouse.** IoT data that requires storing for processing later, or intelligent analysis, is stored in databases on the hospital network and/or cloud. This can be structured or unstructured data generated by the IoT devices, including behaviour metrics and other loggable statistics.

VII. **Analytics, AI, ML.** AI-powered Machine Learning (ML) technology is leveraged to produce superior analysis of IoT data. Amazon cloud services, and the locally deployed AI server, can be used to intelligently process massive amounts of IoT data, to gain deeper insights, predictive and behavioural observations, speed up research, and assist in for more accurate patient diagnosis and treatment planning, and much more.

IoT Security Components

Because hospitals are increasingly a target for cyber-attacks, coupled with the growing concern into the vulnerabilities and risks in IoT, preventative and reactive security measures are strongly incorporated.

The protection of IoT devices will be provided by both the hospital network security, and AWS IoT security components (for devices integrated into the cloud). Physical security will also be considered, along with user policies, and auditing mechanisms.

All IoT device handling and communications are secured using:

- AWS IoT Defender
- Live IoT message and state Monitoring
- Triggers, Alerts, SNS notifications
- Behavioural Analytics, device auditing.

Encryption/cryptographic technology used for IoT device communication:

- AWS IoT facilitates the creating and registering of X.509 certificates, to securely authenticate all the medical IoT devices integrated into the AWS cloud. A private and public key pair is also generated for each registered IoT, allowing asymmetric cryptography. RSA and SHA algorithms are supported, up to 512bit keys. Full certificate support is available, including expiration and reissuing management, and Certificate Authority handling.
- The Transport Layer Security (TLS) 1.2 protocol is used along with the X.509 certificates, to secure the communications of the IoT devices.

Network IoT Security

The local hospital network and cybersecurity measures are the first line of defence and protection for all the IoT devices that reside on and communicate through them.

Strong cyber defence and protection measures are put in place for the hospital's IoT devices, and conversely the wireless portion of the network. The following implemented measures provide a solid foundation, allowing devices to connect more securely and safely, with greatly reduced vulnerabilities and risks.

Segregation of wireless network, critical IoTs

IoT devices that transmit confidential or sensitive data are connected to separate wireless networks, that operate under stricter access rules and conditions of use. This ranges from medical IoT devices, patient monitoring devices, to devices required by hospital personnel to carry out their diagnosis and treatment of patients. Unsecure devices that connect to the public wireless network (guest WIFI), will only be allowed to do so in selective locations, through wireless infrastructure that structurally separate from the highly sensitive IoT network.

Centralised access logs

The most efficient measure to prevent unauthorised access to the IoT network is by preventing such devices from connecting in the first place. An IoT server will manage a centralised access log of all the wireless networks, all the hardware and ICT devices attached, and all the authorised IoT devices that are connected. The log contains records of logins, device IDs, time and locations, bandwidth use, and duration of use. This assists cybersecurity personnel, and monitoring tools, in identifying unauthorised access, anomalous behaviour, and attack patterns.

IoT server registration, gateway enforcement

The hospital network hosts the gateway access points that handle the wireless connectivity of IoT devices. All IoTs operate through defined IP ranges, and MAC (Media Access Control) addresses that are used to identify them on the network. The gateway will grant devices access only if they strictly match the IP and MAC address that the devices are registered with. The IoT server located on the hospital network handles the registering and managing of all IoT devices allowable on the network (the guest network is handled separately).

Encryption and cryptographic authentication

Strong encryption protocols are implemented, using HTTPS, TLS, and SFTP where required. DNS security extensions also protect against malicious domains, and DNS poisoning. The local wireless IoTs connect using WPA3-Enterprise 802.1X network access control for authentication, and for data sensitive IoT devices X.509 cryptographic keys are used, which is also required for connectivity into the cloud service AWS IoT Core.

All IoT devices capable of processing and storing data, will use data encryption services for the data-at-rest, and encrypted passwords at login.

Medical IoT access to the confidential wireless network requires certificate authorisation, and identity confirmation of the IoT by the authentication service. A Certificate Authority, or the AWS IoT Core, issues and manages certificates.

Super strong passwords, MFA

Default settings and passwords are strictly forbidden, all hospital IoT devices no matter how insignificant, will be securely configured. Devices that have login access are governed by the strict rules defined in the password policy (see Group1-Password-Policy-and-Guidance.docx).

Where used, the WIFI access passwords are changed to complex phrases (for example the guest password) and done so frequently.

Personnel devices, such as laptops, tablets, work mobiles, and other computational powered IoTs, are protected with another layer of security, by enabling Multi-Factor Authentication (MFA). For devices that are less powerful, other options are available such as 2FA by Google Authenticator.

Enforce strict network communications policies

By default, simple IoT devices such as temperature sensors are often set up in a permissive state, allowing very relaxed and even unrestrictive access permissions. The policies for all IoT devices must be strictly enforced, only granting permission to authorised sources. Additionally, all IoT devices will be made unreachable on standard TCP/IP ports, Telnet and FTP protocols. This reduces sniffing and network discovery of the IoT devices.

Firmware vulnerabilities and updates

The hospital relies on several third-party manufacturers and vendors for its medical devices and other IoTs used to operate with. The cybersecurity department must evaluate the security merits of all IoT devices and understand the vulnerabilities they introduce into the network. Preventive measures are undertaken to mitigate where needed, and important firmware and software updates for the IoT devices are carried out, logged, and monitored.

Cloud IoT Security

AWS IoT Defender

For the hospital's IoT devices that are integrated into the cloud, they will be secured locally by the existing network security, and additionally with Amazon's cloud-based IoT security suite—AWS IoT Device Defender.

IoT Defender provides advanced tools that audit IoT configurations, handle device authentication, detect anomalies, and handle alarms/alerts. This further secures the hospital's IoT local devices, fleet devices that are off premises, and patient wearable medical devices.

According to Amazon, Defender can secure cloud IoT devices by (Amazon Web Services, n.d.):

- Auditing the security posture of IoT resources across the hospital's device fleet to easily identify gaps and vulnerabilities.
- Using machine learning (ML) models to define the hospital's device behaviours and monitor traffic from a malicious IP or a spike in connection attempts.
- Providing security alerts when an audit fails, or behaviour anomalies are detected. This allows the hospital's cybersecurity personnel to quickly take actions and minimize operational risk.
- Easily mitigate security issues through built-in actions such as updating a device certificate, quarantining a group of devices, or replacing default policies.

Here is a simplified illustration of how IoT Defender works to protect the hospital's devices (Figure 3):

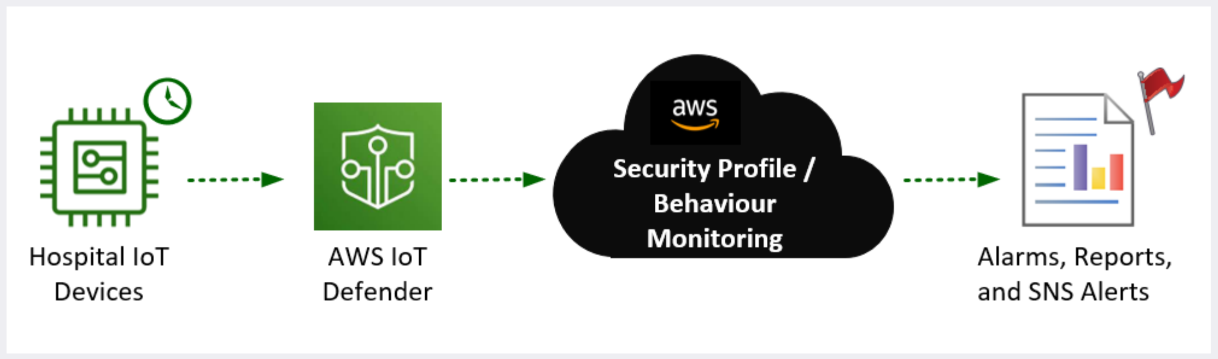
Hospital IoT Devices
AWS IoT Defender
aws
Security Profile / Behaviour Monitoring
Alarms, Reports, and SNS Alerts

Figure 3. Defender utilises behaviour metrics and rules to create security profiles for monitoring IoT communications.

AWS Darktrace AI cybersecurity

The problem with conventional IoT security, such as intrusion detection systems, is that they are unable to deal with the volume and nature of emerging threats. Typically, IDS use rule-based monitoring and pattern detection models that are often static and cannot evolve to guard against novel threats the way self-learning AI does. Also, traditional IoT security does not consider attacks on all other components of the system or network that are also a threat vector, whereas AI-based cybersecurity has superior processing power and a centralised overview of the whole system, allowing for a more complete IoT cyber defence.

The hospital network and IoT devices are far better protected with AI-assisted cyber defences, and as AWS cloud services are already integrated into the hospital's IoT network, it is beneficial and efficient to use Amazon's integrated Darktrace AI Cybersecurity (darktrace.com, n.d.) suite of tools (Figure 4):

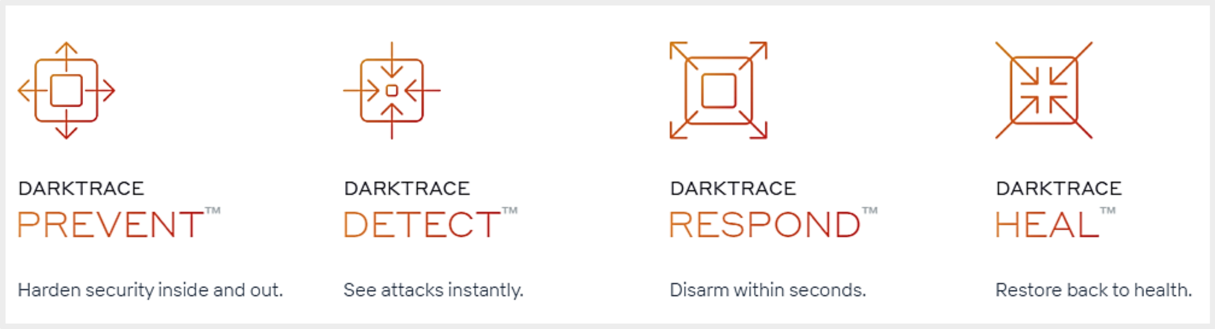

Figure 4. Darktrace AI-powered cybersecurity suite for Amazon cloud services and interconnected end points. Image Source: https://darktrace.com/solutions/aws

Darktrace AI leverages cutting-edge AI technology to prevent, detect and respond to cyber threat events. Darktrace's cutting-edge self-learning AI can learn the hospital's unique IoT cloud environment and users' behaviour, to autonomously create highly customised security models that will spot any subtle deviations or anomalies in IoT communications, data packets, and other device metrics. Threats to the IoT devices are autonomously neutralised, and affected IoTs can be quarantined where required, or self-healed and redeployed if possible.

REFERENCES

Amazon Web Services, Inc. (2019). AWS IoT Core Overview - Amazon Web Services. [online] Available at: https://aws.amazon.com/iot-core/.

Amazon Web Services, Inc. (2019). AWS IoT Greengrass - Amazon Web Services. [online] Available at: https://aws.amazon.com/greengrass/.

Amazon Web Services, Inc. (n.d.). IoT Security | IoT Device Security Management | AWS IoT Device Defender. [online] Available at: https://aws.amazon.com/iot-device-defender/.