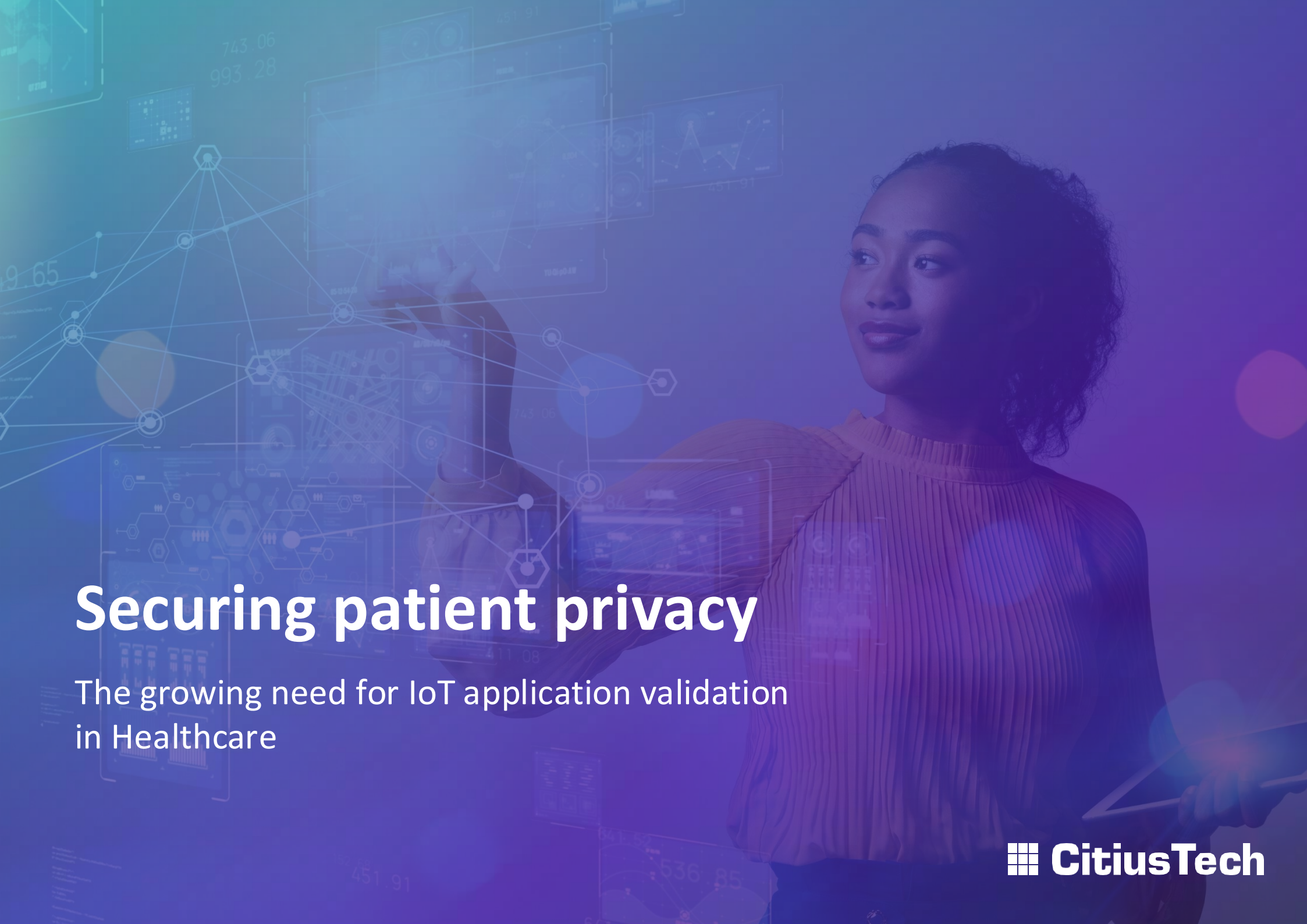


Securing patient privacy

The growing need for IoT application validation in Healthcare

CitiusTech

Table of contents

The IoT movement in Healthcare

The future of IoT in Healthcare is now — as enterprises embrace the change to improve care delivery and accessibility in real-time. IoT devices facilitate remote monitoring, keeping patients healthy and allowing physicians and providers to offer better care. Care providers are implementing IoT-enabled remote monitoring systems to track different health parameters of patients to improve in-home care through connected devices like smartwatches, intelligent patches, personal emergency response systems (PERS), smart inhalers, and glucometers.

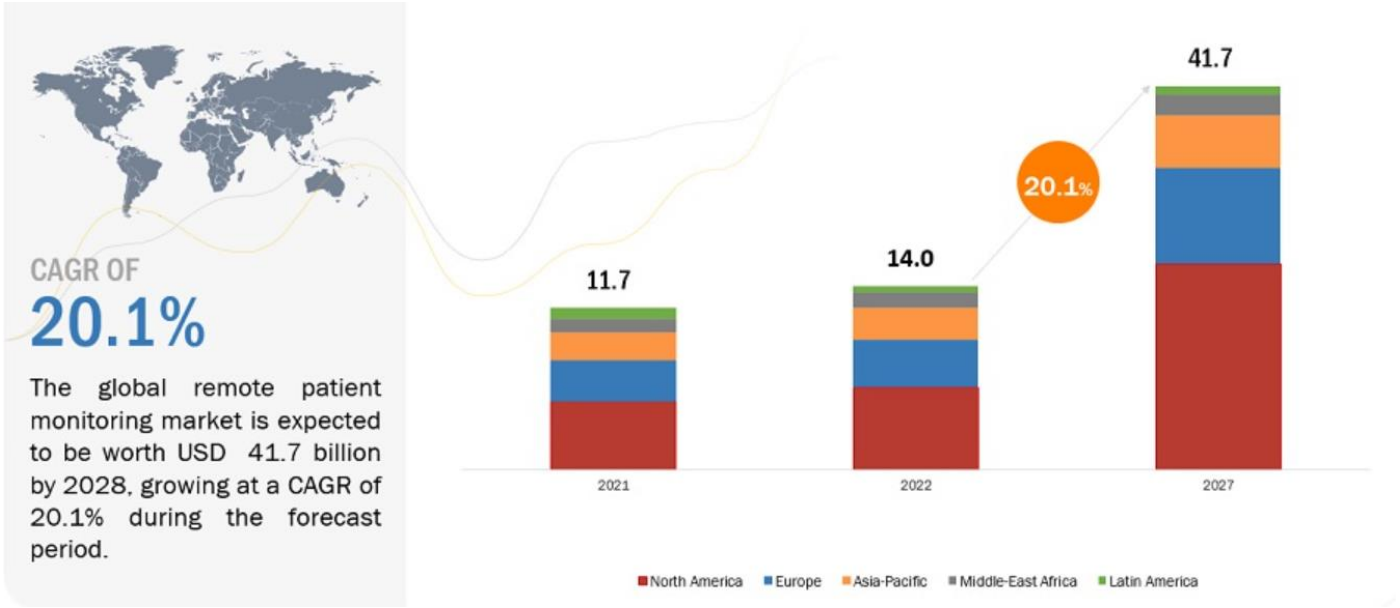


Figure 1: The rising market of Healthcare IoT (HIoT)[1]

For example, smart inhalers can connect with a mobile app via Bluetooth for easier monitoring of respiratory conditions similar to chronic obstructive pulmonary disease (COPD) or asthma. These are equipped with sensor technology to collect actionable data on patients' usage patterns, including time, date, and location. Now, patients can easily stay on track as the inhalers can automatically remind patients about upcoming doses and alert them if they forget to bring the inhaler. Tracking medication use can also help identify patterns of missed doses, allowing them and their doctor to address adherence challenges

This enhances patient satisfaction, reduces hospital stays, and significantly lowers healthcare costs. Research findings indicate that using HIoT to monitor cardiac patients remotely has helped significantly reduce readmission rates by 64% — lowering the financial burden on healthcare providers and payers.[2]

Some Healthcare facilities are also implementing IoT-enabled devices within their premises to better manage their assets and resources and keep tabs on their inventory. Some facilities even use IoT devices to collate all patient data into a centralized platform for physicians to develop improved treatment plans.

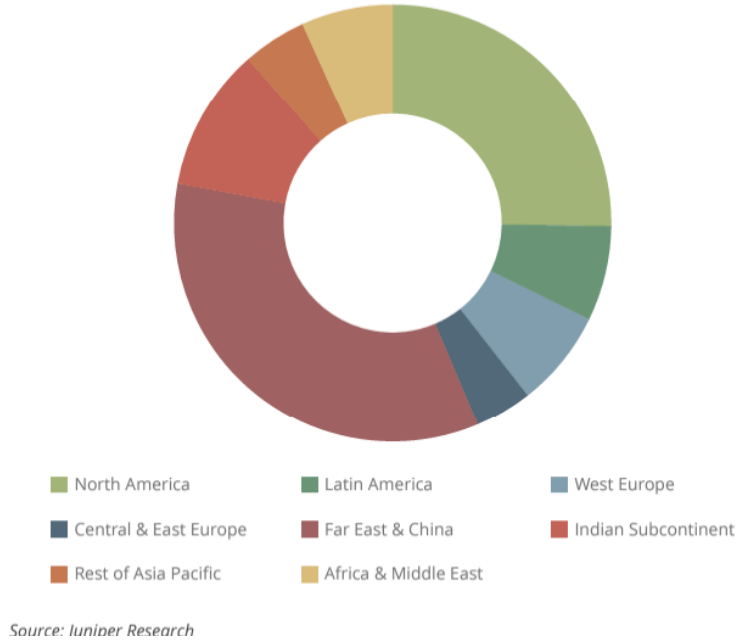


Figure 2: Total HIoT users across all the eight key global markets are expected to reach 115.5Mn by 2027[2]

Architecture of Healthcare IoT system

A typical IoT system in healthcare contains three main components: publisher, broker, and subscriber. Publishers, in this context, represent a network of connected sensors and other medical devices that may work individually or simultaneously to record the patient's vital information. This information may include blood pressure, heart rate, temperature, oxygen saturation, ECG, EEG, EMG, etc.

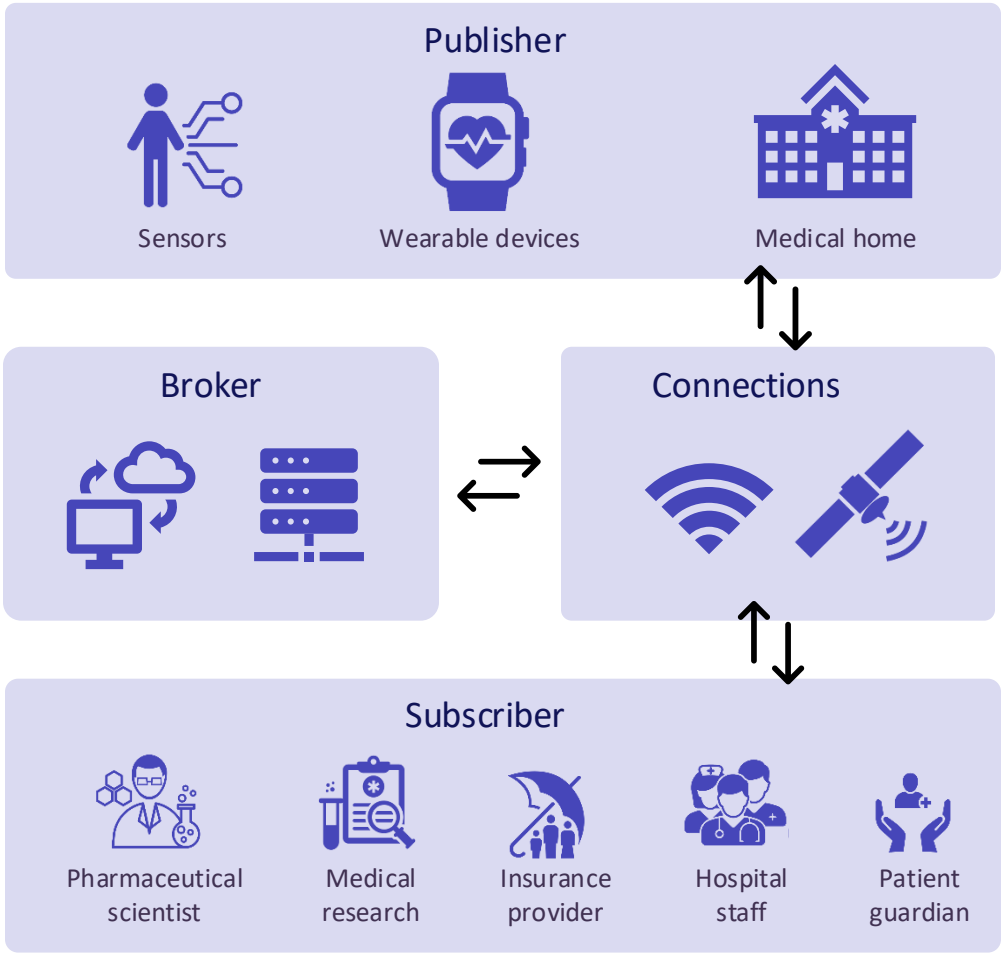


Figure 3: The architecture of healthcare IoT systems

The publisher can continuously send this information through a network to a broker.

On the other hand, brokers are responsible for processing and storing acquired data in the cloud. Finally, subscribers leverage the data collected by publishers and processed by brokers.

They use the data to continuously monitor patients' information, which can be accessed and visualized through a smartphone, computer, tablet, etc. The publisher can process these data and give feedback after observing any physiological anomaly or degradation in the patient's health condition.

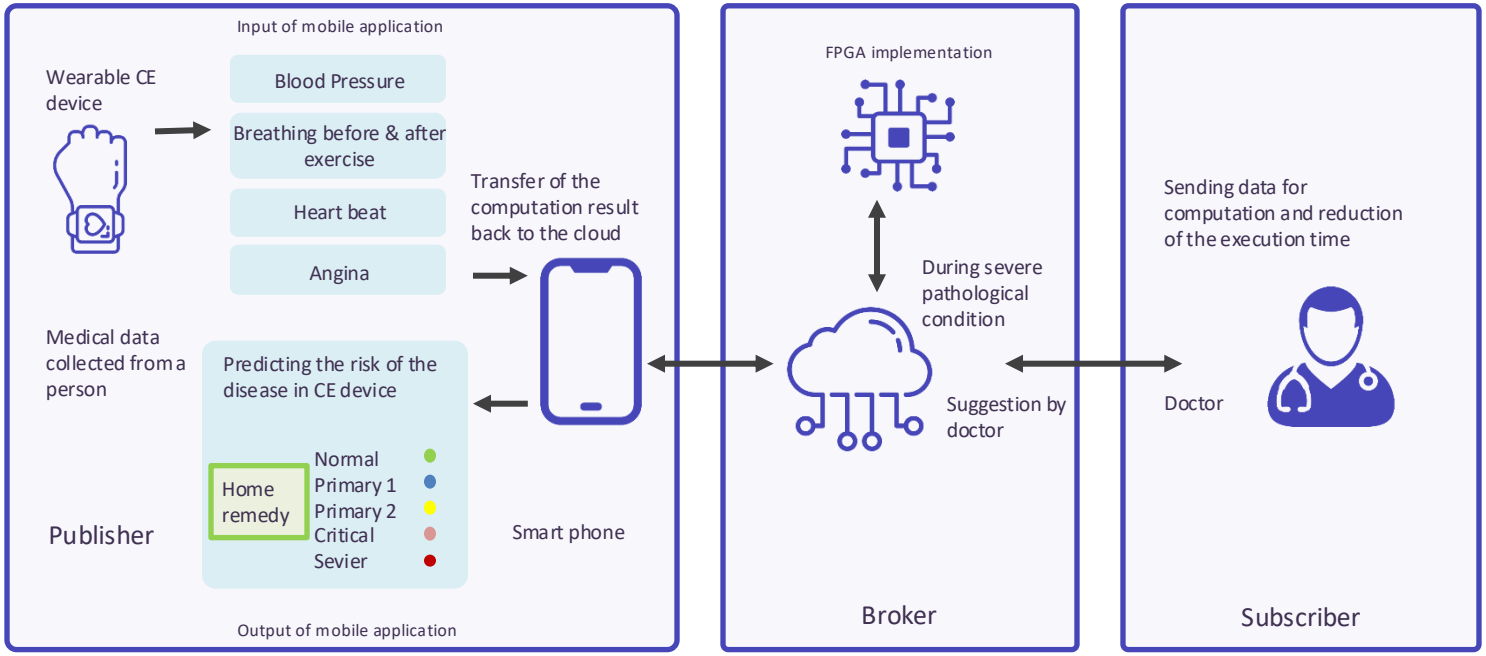


Figure 4: A typical flow of data across all the HIoT devices[3]

With great power comes great responsibility

As we continue implementing IoT across the care delivery system, we must be mindful of certain aspects of a connected world. While cyber threats already pose a significant threat to our online data, the impact of any security breach in a Healthcare setting can be far more devastating. Every touch point we create with connected devices contrives a potentially vulnerable point that cyber attackers can exploit.

That's why the onus is on the care providers to ensure that the connected IoT devices are safe from attack, and that confidential and sensitive patient data remain secure. This explains the sudden boom of the HIoT security market, which is projected to reach USD 3.56 billion by 2033 — an uptick from its USD 0.62 Billion assessment in 2023.[4]

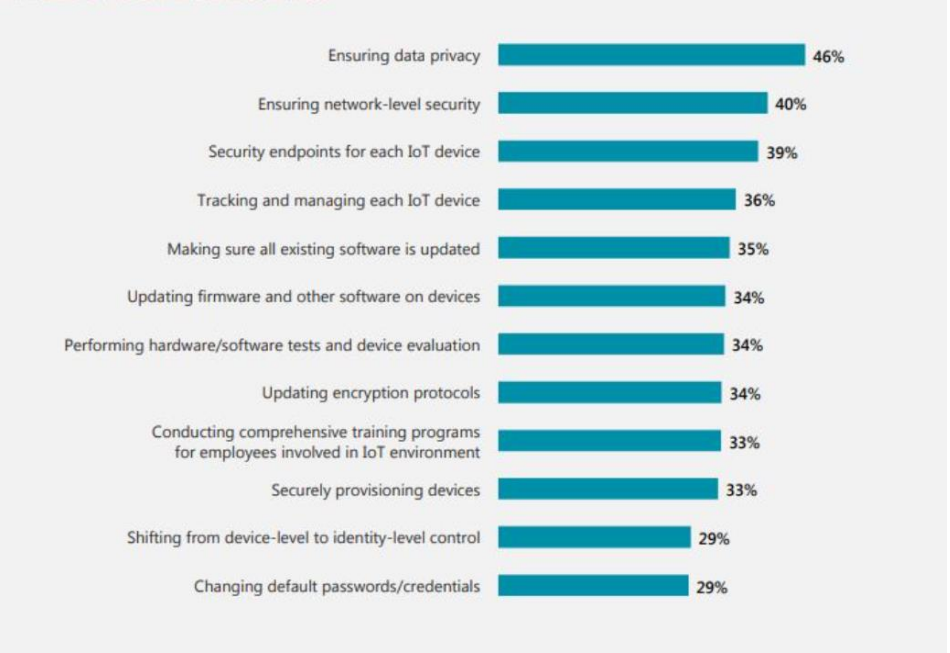


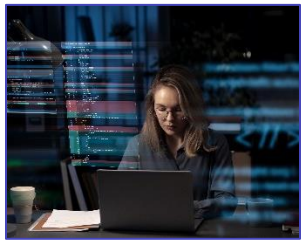
Figure 5: Top HIoT security concerns[4]

Beyond the security concerns, the performance of IoT devices also needs to be considered. Since these devices are responsible for patients' lives or deaths, the performance must always be reliable and top-notch. The margin of error, in this case, is a solid zero. Besides, the interoperability of IoT devices is another aspect that needs our attention.

The premise of connected devices is the ability of different systems to work together. IoT-enabled interoperability strengthens the foundation of a connected Healthcare system.

Validating IoT applications: The need & the methods

One way to ensure the robust functionality and security of the HIoT devices is to test and validate them before implementing them in a Healthcare setup. By investing in IoT testing services tailored for Healthcare, care providers can ensure robust functionality and security while mitigating risks of unauthorized access and data breaches. Following is a comprehensive list of tests that can validate IoT devices and qualify them for medical usage:



- **Security testing:**

Security testing ensures IoT Healthcare devices and networks are fortified against unauthorized access and cyber threats, safeguarding patient data and maintaining privacy. It can also verify if IoT devices (publishers) implement secure communication protocols and encrypt sensitive data and mechanisms to authenticate themselves with the network.

- **Interoperability testing:**

Interoperability testing can help you validate the seamless integration and communication between different IoT devices (publishers), ensuring they can seamlessly integrate and communicate with the broker using standardized protocols. You can handle data from diverse publishers and subscribers, also validate subscriber applications can receive and process data, and maintain compatibility across the Healthcare IoT network.

- **Reliability and performance testing:**

You can evaluate the reliability and performance of IoT devices under different conditions, ensuring they function correctly and respond promptly to the broker with reliability and performance testing. Reliable performance is critical in Healthcare to avoid delays in receiving vital data or commands, contributing to timely and accurate patient care. Evaluating the reliability and performance of the broker, checking its ability to handle a large volume of data, maintain low latency, and avoid bottlenecks.

Data accuracy and integrity testing:

Data accuracy and integrity testing verifies the precision and integrity of data collected by IoT devices, validates broker correctly handles incoming data for accurate diagnosis and treatment planning, and subscriber applications accurately interpret and display the received data. This is essential for informed decision-making by Healthcare professionals, preventing misdiagnoses or incorrect treatment plans.

Usability testing:

This evaluates the user-friendliness of IoT applications, ensuring that both patients and Healthcare professionals can easily navigate and use the devices. Intuitive interfaces reduce the chances of user errors, enhancing the overall safety and effectiveness of Healthcare IoT devices (publisher).

Regulatory compliance testing:

You can ensure adherence to industry regulations, promoting patient safety and legal compliance in Healthcare operations with regulatory compliance testing. This helps mitigate risks associated with device malfunctions, ensuring that Healthcare providers follow established safety protocols. You can even confirm that subscriber applications meet regulatory requirements for the secure handling and storage of health data.

The challenges of IoT application validation

Now, if we understand the importance of validating IoT applications before using them, why are we not testing these devices as aggressively?

Well, what impedes the validation of HIoT devices is the plethora of challenges that we must address.

Network connectivity

Challenge:

Unreliable networks hinder HIoT device testing due to varied security and stability.

How to overcome:

Include the use of virtual network simulators to vary the network load, connectivity, and stability.

Interoperability issue

Challenge:

Testing IoT devices presents a significant challenge due to the diverse range of publisher and subscriber configurations utilized by various manufacturers.

How to overcome:

Include the use of simulation tools and emulation environments to validate the functionality and compatibility of IoT devices under various scenarios.

Too many IoT platforms

Challenge:

Every connected device has its own hardware and relies on software to drive it. That's why it is hard to test all possible combinations of hardware and software.

How to overcome:

Gather information from end users and figure out which devices and software versions they're using to determine the most popular combinations.

Data security concerns

Challenge:

IoT devices often lack robust built-in security features. This vulnerability makes them prime targets for hackers.

How to overcome:

Pay particular attention to the password policies of IoT devices and ensure that minimum password requirements are built and enforceable on the devices.

Scalability and realistic testing

Challenge:

Testing the scalability and realistic performance of all these devices, accounting for diverse network conditions and scenarios, is a substantial challenge.

How to overcome:

Utilize cloud-based testing platforms that can simulate a vast number of IoT devices.

Best practices for HIoT application validation

Don’t let the roadblocks stop you from changing the care delivery model for the better with HIoT. From our experience, we have seen that specific validation best practices help Healthcare Providers leap over the challenges and create a solid organization-wide IoT foundation.

- ## Adopt a risk-based testing approach

In this approach, the features and functionalities of the HIoT system that carry the highest risk are tested first. This ensures that the system's most critical components are well-tested and functional.

- ## Testing early and often

Testing should start early in the development process and be performed regularly. This allows for early detection of defects and issues, making them more accessible and cheaper to fix.

- ## Implement a continuous testing process

IoT devices in Healthcare systems are dynamic and often updated. Continuous testing ensures that any system changes, updates, or additions are tested promptly, maintaining the system's overall quality.

- ## Prioritize security testing

Given the potential vulnerabilities of HIoT devices, security testing should be a high priority. This includes testing for potential breaches and PHI data leaks and ensuring compliance with Healthcare regulations.

- ## Leverage automation where applicable

Automated IoT testing tools can help perform many tests quickly and accurately without human intervention — thus reducing labor dependency.

- ## Test in real-life scenarios

Teams should test real-life conditions, including different user experiences, performance, network, and compatibility testing scenarios.

Creating a healthier and safer tomorrow

Yes! Implementing IoT in your Healthcare system will have hurdles, but it's a journey worth embarking on. As the Internet of Things advances, testing practices must evolve to support the growing complexity of smart devices. Through effective planning and execution, IoT testing is crucial in improving the quality of data gathered by Healthcare IoT device test equipment, ensuring the integrity of critical information.

What will help you in this endeavour are collaborative efforts and innovative approaches to finding solutions for overcoming the roadblocks. Only then can we create a better and healthier future together.

References:

1. Remote patient monitoring market (marketsandmarkets.com)
2. Remote patient monitoring: Three key trends (juniperresearch.com)
3. Process flow of the IoT-based smart healthcare system | Download Scientific Diagram (researchgate.net)
4. Healthcare Internet of Things (IoT) Security market surges projected to reach USD 3.56 billion by 2033 with a striking 19.1% CAGR (yahoo.com)
5. Remote patient monitoring: Key trends, regional analysis & market forecasts 2023-2027 (juniperresearch.com)
6. The role of the Internet of Things in health care: a systematic and comprehensive study (researchgate.net)
7. IoMT (Internet of Medical Things): Reducing Cost While Improving Patient Care (embs.org)
8. Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5G network (nature.com)

Authored By:

Harshada Salvi
Sr. Manager, Quality & Validation Practice, CitiusTech

Reshma Ravi
Manager, Quality & Validation Practice, CitiusTech

Rahul Sahu
Tech Lead, Quality & Validation Practice, CitiusTech

To learn more about this contact us at
sales@citiustech.com

visit our website
www.citiustech.com

CitiusTech