10 IoT Best Practices for Home Appliance Manufacturers

Ayla Networks

As home appliance manufacturers consider adding smart appliances to their product lines, they need to ask themselves an important question: "Do we have the specialized technical expertise in house to successfully connect, scale and secure versions of our appliances for the Internet of Things (IoT)?"

This best practices guide outlines some of the considerations important for appliance manufacturers as they design, build and eventually sell IoT connected appliances. IoT is complex, and creating connected home appliances requires more than simply embedding a wireless chip or adding a sensor. Home appliance manufacturers need to consider everything from network security to application software design. Furthermore, they need to know how to budget, scale, distribute and future-proof their products.

As a home appliance manufacturer, you will want to ensure that as you move to the IoT, you are able to dedicate your time, attention and resources to your core business. Implemented poorly, IoT connected products can drain your resources, budgets and even your brand reputation. Done well, however, connected versions of your appliances can enhance your revenues and help differentiate your products in crowded marketplaces.

Table of Contents

IoT Best Practice #1: Clearly define your use case 4

IoT Best Practice #2: Prioritize security and scalability from the beginning 4

IoT Best Practice #3: Design for end-to-end configurability.....................6

IoT Best Practice #4: Use open standards-based IoT solutions...............6

IoT Best Practice #5: Make your connected products easy to install and use....................................7

IoT Best Practice #6: Design for secure over-the-air (OTA) system updates....................................8

IoT Best Practice #7: Include role-based access control (RBAC) and other advanced management controls...9

IoT Best Practice #8: Start thinking about your appliances from a "service" perspective instead of a "product" perspective 9

IoT Best Practice #9: Product hardware still matters. Stick with proven hardware solutions 10

IoT Best Practice #10: Work with a leading IoT platform.......................11

IoT Best Practice #1:
Clearly define your use case

The IoT gives manufacturers unprecedented visibility into how their appliances are actually performing and how customers are using them. Before embarking on the IoT journey, however, it is extremely important to clearly identify compelling reasons for creating a connected appliance from your customers' perspective. Because the IoT introduces new capabilities not possible with traditional, discrete products, your use cases for connected appliances might be very different from what you've done in the past.

Remember, too, that the real value of the IoT lies in the data that connected devices generate. When identifying use cases for your connected appliances, consider how you might use the data to differentiate your products, enhance their features and generate additional revenue streams.

IoT Best Practice #2:
Prioritize security and scalability from the beginning

Security is only as powerful as the weakest link in the IoT ecosystem. IoT security must be bulletproof at the device, cloud and mobile app levels, as well as everything in between. Plan for end-to-end security from the very beginning.

Also from the beginning, know how you will achieve enterprise scalability with your connected products. That might mean producing 2,000 or 100,000 connected appliances a month, or turning on millions of connected appliances in a short period of time. Make sure that as you scale, your security scales, too.

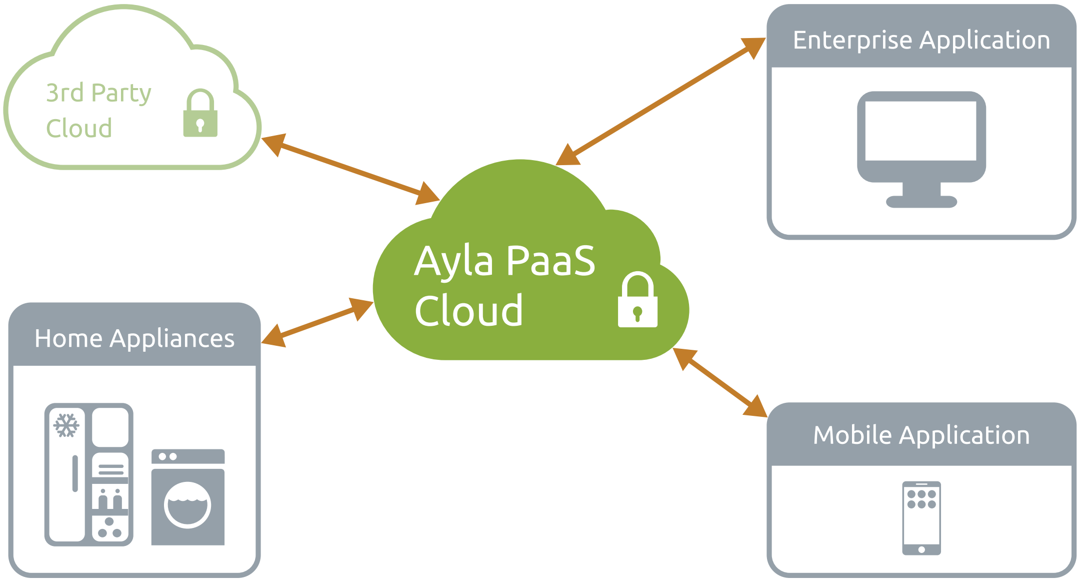

Figure 1: End-to-end, bullet proof security

Because security is invisible, it's tempting to see it as an area to cut costs. Viewing security as an afterthought, however, is a disastrous mistake. If you don't build in end-to-end security from the beginning, you'll have to go back to recreate and validate that every link in the security chain is secure.

For example, say your company invested $5 million to launch its first IoT refrigerator, but neglected to include end-to-end security. It could cost an additional $5 million to start over and add security at every point of your connected refrigerator product. Plus, you might have to spend more on hardened security than you would have spent originally—not to mention causing a significant time-to-market delay.

Don't risk embarrassing, high-profile security breaches of your connected products or the customer data they generate. Resist the temptation to compromise on security.

IoT Best Practice #3:
Design for end-to-end configurability

Like scalability and security, configurability needs to be included in every aspect of your connected appliances, from the beginning. Although configurability is complex, it's essential to IoT.

The data generated by your IoT appliances represents a powerful tool for gaining knowledge and insights not previously available. In the past, you had to rely on surveys or questionnaires to understand how your products performed and how customers used them. Now, you can get these insights from the products themselves. You can use that knowledge to build better appliances, add new value-added services, and establish new and stronger relationships with your customers.

IoT Best Practice #4:
Use open standards-based IoT solutions

Your connected products will need to reach customers worldwide and support cloud-to-cloud connectivity with various IoT platform, manufacturer and retailer clouds. Your connected appliances will also need to integrate with related products and services from other providers. The best way to achieve this interoperability is through using open, native libraries and other standards-based solutions.

For example, if you manufacture a connected refrigerator, you might want to manage its use with other appliances, such as ovens and dishwashers, and also with other home automation systems such as connected water filtration, HVAC, door locks and lighting.

Choose a cloud architecture that is schema-less and agnostic to any particular data types. That way, smart home appliance products can interoperate with existing clouds and connectivity methods (Apple HomeKit, Nest Weave, Google Home, Amazon Echo, Wink Connected Home, etc.) as well as new cloud and connectivity approaches that emerge in the future.

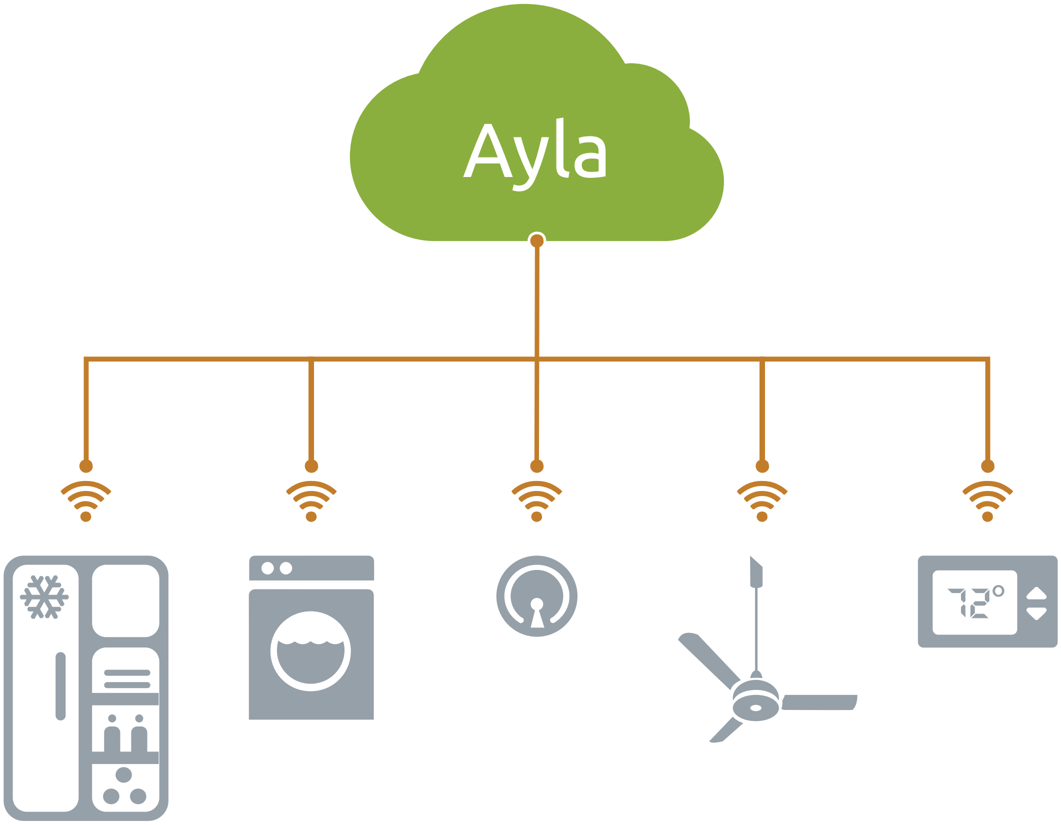

Figure 2: Schema-less cloud architecture

IoT Best Practice #5: Make your connected products easy to install and use

All IoT products require some level of control, whether that means frequent input from an end user via a mobile app or occasional use of a web application by service professionals. With the complexity of the IoT and the high expectations of end users, manufacturers have the added challenge of making those mobile or web apps extremely easy to use.

Here are some of the considerations that will need to guide the design of your mobile or web app:

- Who will install and set up the connected appliance, and what information will they need to have?
- How will you provide that installation information?
- Will the setup be done using a display on the product, a mobile app, web application—or some combination?
- What kind of PIN, password or other identification is necessary for installation?
- Will networking setup happen at the same time as product installation, or will it be a separate process?
- How will end users register their products?

Testing is critical throughout the IoT design process, but it's especially important that you test and retest to make sure that your mobile or web app delivers a superb user experience—for all the operating systems and browsers that you will support.

IoT Best Practice #6: Design for secure over-the-air (OTA) system updates

One of the biggest differences between connected appliances and traditional appliances is that connected appliances are able to change and improve over time—even after installation in an end user's home.

Through over-the-air (OTA) updates, you can update the firmware on your connected washing machine or refrigerator, or add features based on analyzing real-world customer usage of that appliance. Your OTA system will need to have enterprise-level security to ensure data integrity and prevent hacking. The security itself can also be updated via OTA communication as needed.

IoT Best Practice #7: Include role-based access control (RBAC) and other advanced management controls

Role-based access control (RBAC) is a method for granting either temporary or permanent access to a particular appliance by individuals based on their “roles” or their relationships to the products.

For example, service technicians could be granted access to a refrigerator during hours of a scheduled maintenance visit. Adults, children and guests in a household could all be given different degrees of ability to control various appliances in the home.

Owners of vacation properties could provide vacationers with temporary access to a unit’s heating and air conditioning controls, as well as to its door locks, washer/dryer, dishwasher, lighting and other connected features. Likewise, owners of apartment buildings, office complexes or hotels could provide various levels of connected appliance access based on whether the individual is a facility manager, corporate energy manager, employee, building contractor, tenant or guest.

In addition to RBAC, other advanced controls to design into your connected products include custom scheduling, triggers and alerts, and notifications—to the end user/owner, dealers or other service professionals, and to you as the manufacturer.

IoT Best Practice #8: Start thinking about your appliances from a “service” perspective instead of a “product” perspective

The IoT changes everything. To grow your business in the new IoT world, appliance manufacturers must shift their mindsets to capitalize on the new opportunities available with the IoT. Start by rethinking how you define the boundaries between a “product” and a “service.”

Some of the things you can do with connected appliances that your traditional products could not achieve include the following.

- Use rules engines, which allow your connected appliances to evaluate various rules rather than following pre-set procedures. This approach makes the appliances more responsive to the needs of the people using them.
- Establish geo-fences, which are virtual barriers or boundaries for geographic areas. Using GPS systems, radio-frequency identification (RFID) or mobile beacon data, geo-fences can be predefined as a zone of control, such as by a connected thermostat. Geo-fences can also be generated dynamically, such as defining a physical area in which a particular connected appliance can be controlled by smartphones.
- Implement digital dashboards on web or mobile apps to visualize data for activities such as diagnostics, predictive analytics and energy usage. Using these dashboards, you can offer fast or preventive maintenance, troubleshooting and solving problems without sending a service technician. You can also easily monitor—or allow end users to monitor—how much energy or water the appliances are using.
- Tune your connected products to achieve or demonstrate compliance with Energy Star or similar programs.
- Extend the capabilities of your IoT connected offerings beyond what traditional products could achieve by integrating with third-party services such as energy demand response, weather feeds, pollen counts or air quality reports. Using data from these third-party services, you can design your connected IoT offerings to automatically adjust their operations to optimize performance, energy efficiency or other parameters.

IoT Best Practice #9:
Product hardware still matters. Stick with proven hardware solutions

Hardware options such as electrical connectivity or networking protocols are not the place to express your competitive differentiation. For instance, if you're sourcing a Wi-Fi chip, select a proven supplier rather than shopping for a low-priced alternative.

A Wi-Fi chip from a low-cost supplier may work for simple connectivity in a prototype or proof-of-concept (POC) project, but it won't have a full networking stack or enterprise-grade security. Using inferior-quality components for production could cripple your IoT efforts if customers try to use products that lack sufficient wireless range, performance, compatibility or—most seriously—security.

IoT Best Practice #10:
Work with a leading IoT platform

You could actually eliminate the first nine best practices outlined here by starting with Best Practice #10. That's because the right IoT platform incorporates all these best practices and more.

Turning your traditional home appliances into successful IoT connected appliances means making dozens of small and large technical decisions and applying a broad range of technology expertise. For almost every appliance manufacturer, it makes more sense to buy this expertise from an established IoT platform vendor than to try to assemble all the IoT expertise needed—and then to make sure you stay up-to-date on fast-changing security practices, networking protocols, user experience design and other IoT necessities.

As an appliance manufacturer, the important question to ask is: Do you want to master all the skills, technical expertise and nuances demanded by the IoT, or do you want to focus on harnessing the value of the IoT to build and sell the best possible connected appliances?

Instead of learning all the IoT best practices yourselves, use the ones listed here as a starting point for evaluating an IoT platform. You'll not only save your sanity but you'll also get to market faster and more affordably with a better connected offering.

To find out more about how using the Ayla IoT platform can shorten and simplify the leap to the IoT, download our white paper Manufacturers' Biggest IoT Decision: Build or Buy an IoT Platform?

Request a Demo
of Ayla IoT Platform