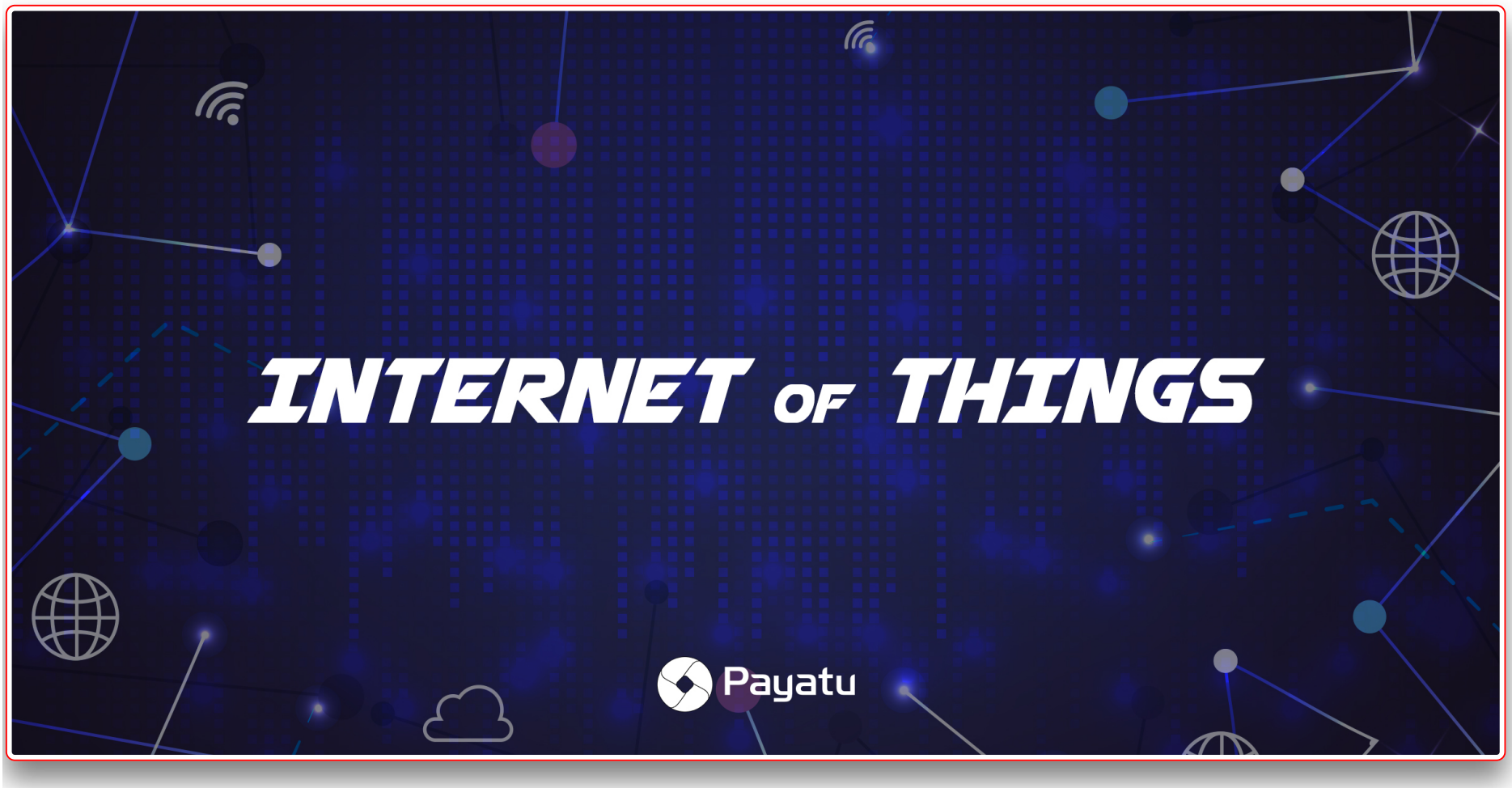
Payatu

IoT Security – Part 1 (101 – IoT Introduction And Architecture)

Admin-Payatu
10/08/2017



I have been getting a lot of queries recently from folks interested in Internet of Things security about where to start in IoT security research so, I decided to create a series of IoT Security blog posts to help researchers who want to get into IoT security, IoT penetration testing and exploitation.

The problem with every new and complex technology for security researchers is not knowing where to start and how/where to attack. This is a common problem and has a common solution i.e. breaking the technology into small components and start learning each component individually. This process makes you master each component and guides you to focus on the most interesting components according to the researcher. If you have read till here, I'm assuming you are going to stick around and read through. So, without any delay let's start :) .

Note:
1. The information in this blog series is generic and can be applied to the security research of IoT products in any domain irrespective of their usage including Home automation, Industrial Control Systems, Healthcare, Transportation etc.
2. I will use the words device, hardware and sensor interchangeably to mean the same thing unless specifically mentioned with explanation.
3. I mention IoT ecosystem to mean an IoT product or a solution due to the nature of the IoT technology that comprises of different technologies.

IoT != Hardware

This is a common misconception among folks that IoT means hardware only, which creates an imaginary roadblock and discourages most security researchers from venturing into IoT security. Yes, there is hardware involved and the skills required to analyze it can be learnt. If it helps "IoT security research is not difficult", but requires dedication and inclination to learn. As you read through this blog post you will realize that the hardware only forms 1/3 part of the IoT ecosystem. On top of that if you can compromise other components (for ex. Cloud) you can cause more damage than just hacking into the device. I had the same inhibition few years ago when I started working on IoT security, so I broke down the problem into small pieces and attacked pieces individually and learned some cool tricks along the way. If an average person like me can do it, I think anyone can.

Introduction

What is IoT?

There are many definitions of IoT on the Internet and the crux of mastering a technology is to understand the basic ideology behind it which helps in defining your own meaning and applicability of the same. Everyone can have their own definition and for me IoT is all about three important things

1. Automation: Let's face it, we are lazy and the future is all about making us more lazy and automating any task that we do manually.

2. Virtual-Physical world interface: Creating a bridge between the physical and the virtual world. In simple terms allow the virtual world to read and write from/to the physical world. When I say read I mean sensing the physical environment and converting the state into data and sending it across to the virtual data storage for further analysis such as temperature sensors, medical sensors, cameras etc. Write means to control the physical world with an action i.e. converting the data into an action on the physical world such as door locks, controlling the vehicle operations, spraying water, medical pumps etc. You get the idea.

3. Insight and Decision making: The data gathered from the devices can be analyzed in real-time to understand the environment better, act on certain events, find the root cause of any physical world problems etc.

The IoT technology thus empowers both end users as well as the vendors with real-time information and automation of the tasks at hand.

Based on the above definition, if we were to create a technology to solve this problem we would require

1. A hardware device that provides the virtual-physical interface
2. A backend data storage to store and computing power to perform statistical analysis on the data.
3. A virtual interface for the users to view the analyzed data and send commands to the physical world.

The first is solved by having economical hardware devices embedded with the respective sensors/controllers, the second is conveniently solved by the cloud and finally the third is easily solved by a mobile application and/or a web application.

Where is IoT used?

As I mentioned above IoT is all about making us fat and lazy. Humans are good at innovating and we can find out areas that can be improved event in a near perfect system for whatever reasons. The usage of IoT technology is limitless in today's world. I bet if you just look around you will probably come up with an IoT idea. There are various domains that are currently seeing a lot of innovation in IoT with the sole aim of automation and real-time data analysis from the physical world

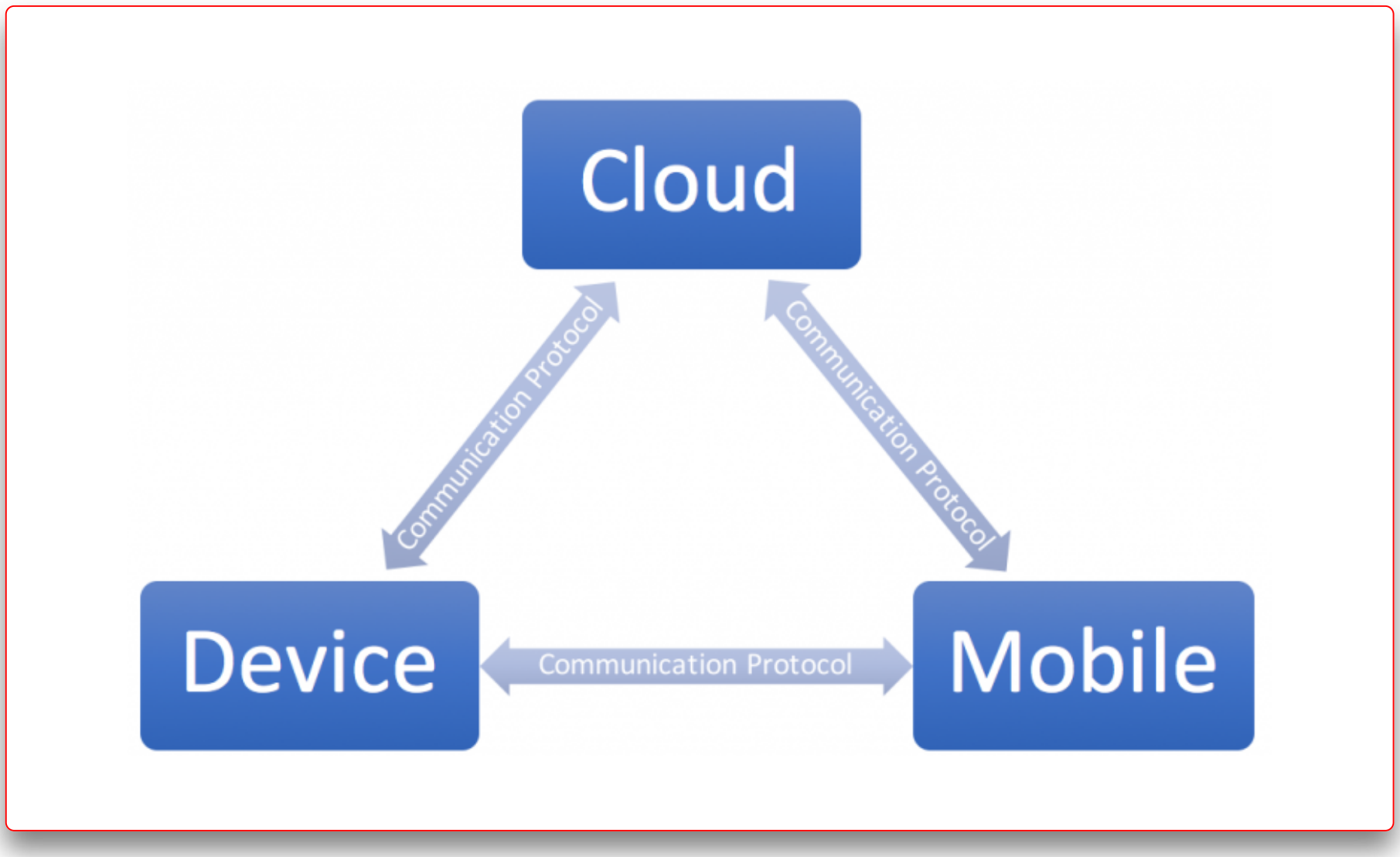
1. Home automation
2. Smart infrastructure
3. Healthcare
4. Industrial Control Systems
5. Transportation
6. Utilities
7. And more

IoT Architecture

High level view

In its simplest form IoT architecture includes three components as shown in the below diagram.

1. Mobile
2. Cloud
3. Device



The communication between the components depends on the usage and/or type of the IoT product. Following are some examples which will make it clear how and why do components talk or do not talk to each other.

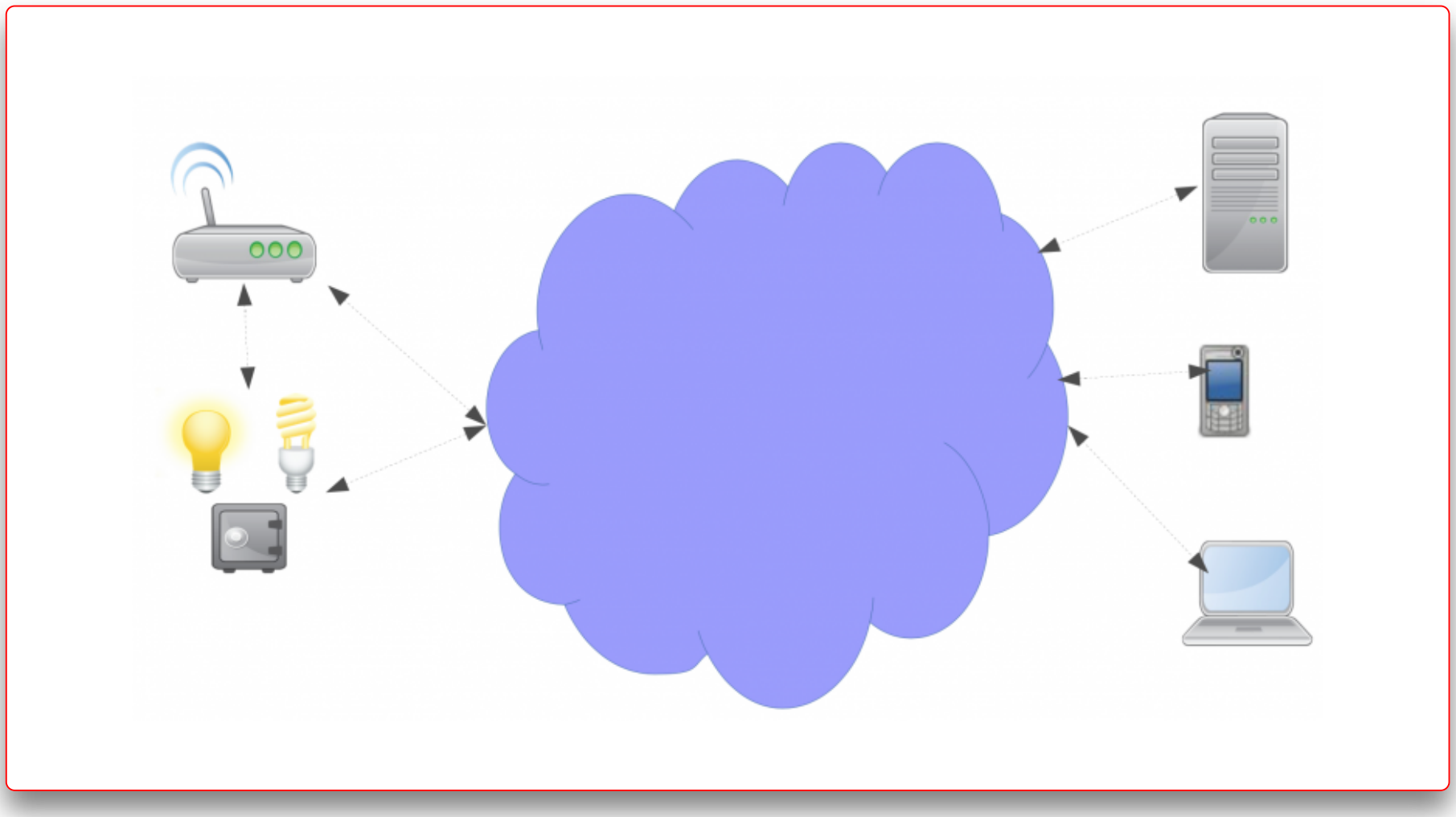
1. Device talks mobile only – Ex. BLE based devices

2. Device talks to IoT gateway only – Ex. ZigBee, Wireless HART devices etc.

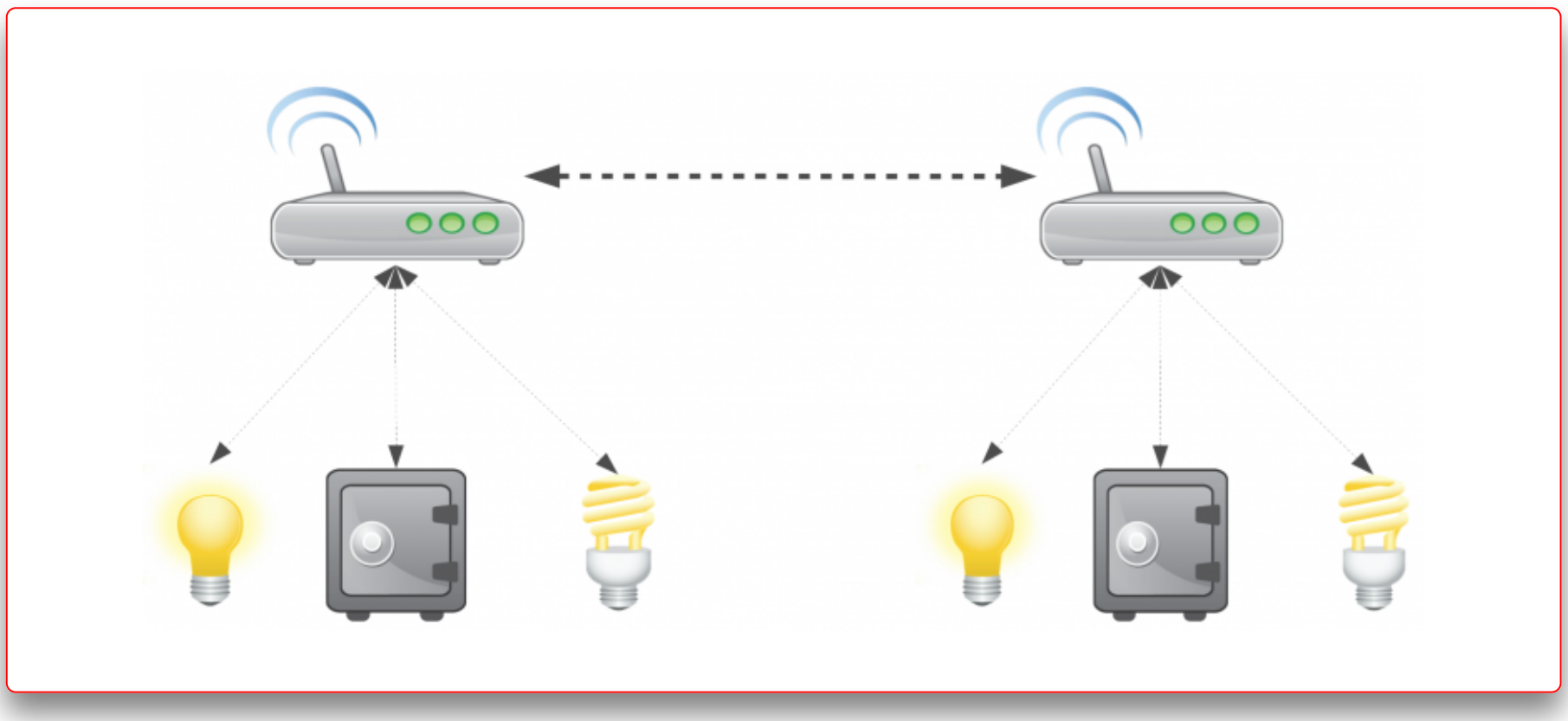
3. Mobile talks to Cloud only – In cases where the users do not have proximity access to the device and it can only be controlled via the cloud.

Functional Architecture

Expanding further the functional architecture can be defined a network of sensors communicating with the cloud and the mobile/web interface via the Internet. The sensors may have their own network over tradition TCP/IP based technology or Radio based in case where the traditional networks cannot be implemented and radio communication offers more efficiency and makes more sense. In the latter case, there needs to be a gateway (our so called IoT gateways/Hubs/Routers) that acts an interface between the radio communication and the traditional TCP/IP communication. From now on I will refer to TCP/IP as traditional network/communication.



We can also have geographically spread sensor networks that can communicate with/are connected to each other via traditional networks by the IoT Gateways as shown below.



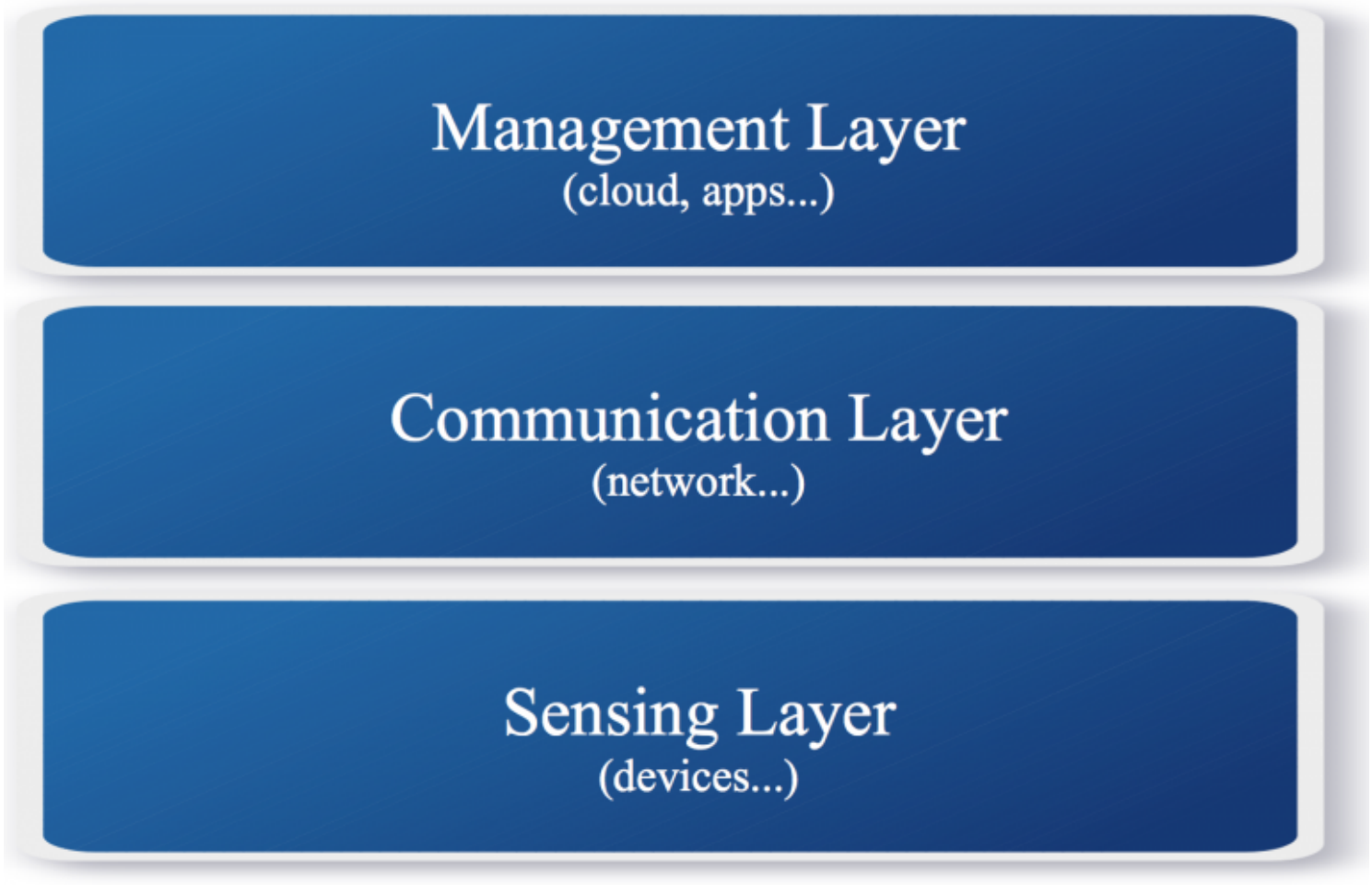
Layered model

If we look at the IoT technology from a layered perspective we can define it in 3 simple layers that form the core of IoT

1. Sensing layer – This consists of the hardware sensors and sensor networks.

2. Communication Layer – This consists of the communication mechanism that allows the sensing layer to communicate with the Management layer for example – Wifi, 3G, LTE, Ethernet etc.

3. Management Layer – This is the top most layer and is responsible for making sense out of the raw data and provide a presentable and fancy view to the users. It includes the cloud, storage, apps etc.



If you are reading this, you are really interested in IoT security :). The aim of this blog post was to give you an idea about the IoT technology. Going forward, we will start talking about IoT security. The next blog post will describe the attack surface of the IoT ecosystem. I hope you enjoyed reading this as much as I enjoyed writing it :).

Payatu Software Labs offers quality IoT penetration testing services and Practical IoT Hacking training worldwide. If you are interested in corporate training or security testing of your IoT products, kindly get in touch with us – info [_a t_] payatu DOT com

Continue to second part