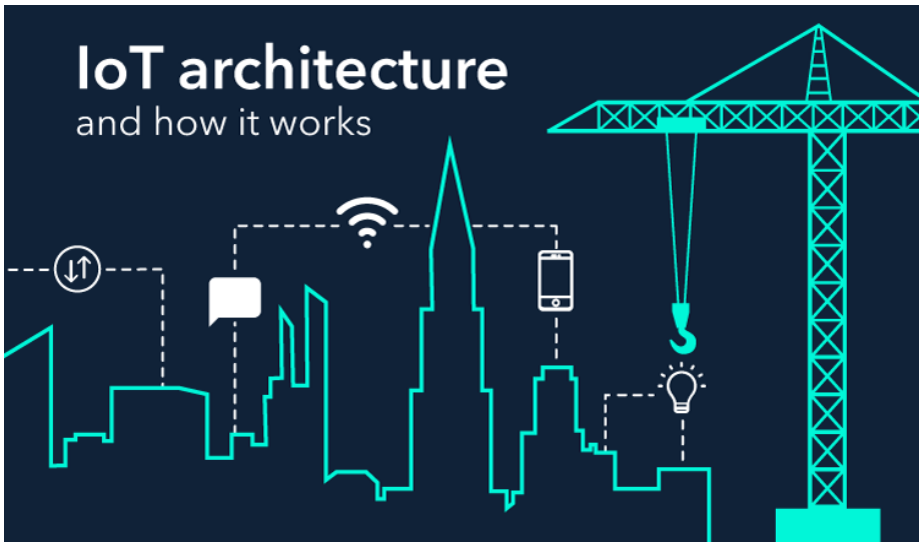
Unit-I: Fundamentals of IoT 10 hours
Architectural Overview,
Design principles and needed capabilities,
IoT Applications,
Sensing,
Actuation,
Basics of Networking,
M2M and IoT Technology Fundamentals- Devices and gateways,
Data management,
Business processes in IoT,
Everything as a Service(XaaS),
Role of Cloud in IoT,
Security aspects in IoT
Unit-II: Elements of IoT 10 hours
Hardware Components- Computing (Arduino, Raspberry Pi),
Communication,
Sensing,
Actuation,
I/O interfaces;
Software Components- Programming API's (using Python/Node.js/Arduino) for Communication;
Protocols-MQTT, ZigBee, Bluetooth, CoAP, UDP, TCP.

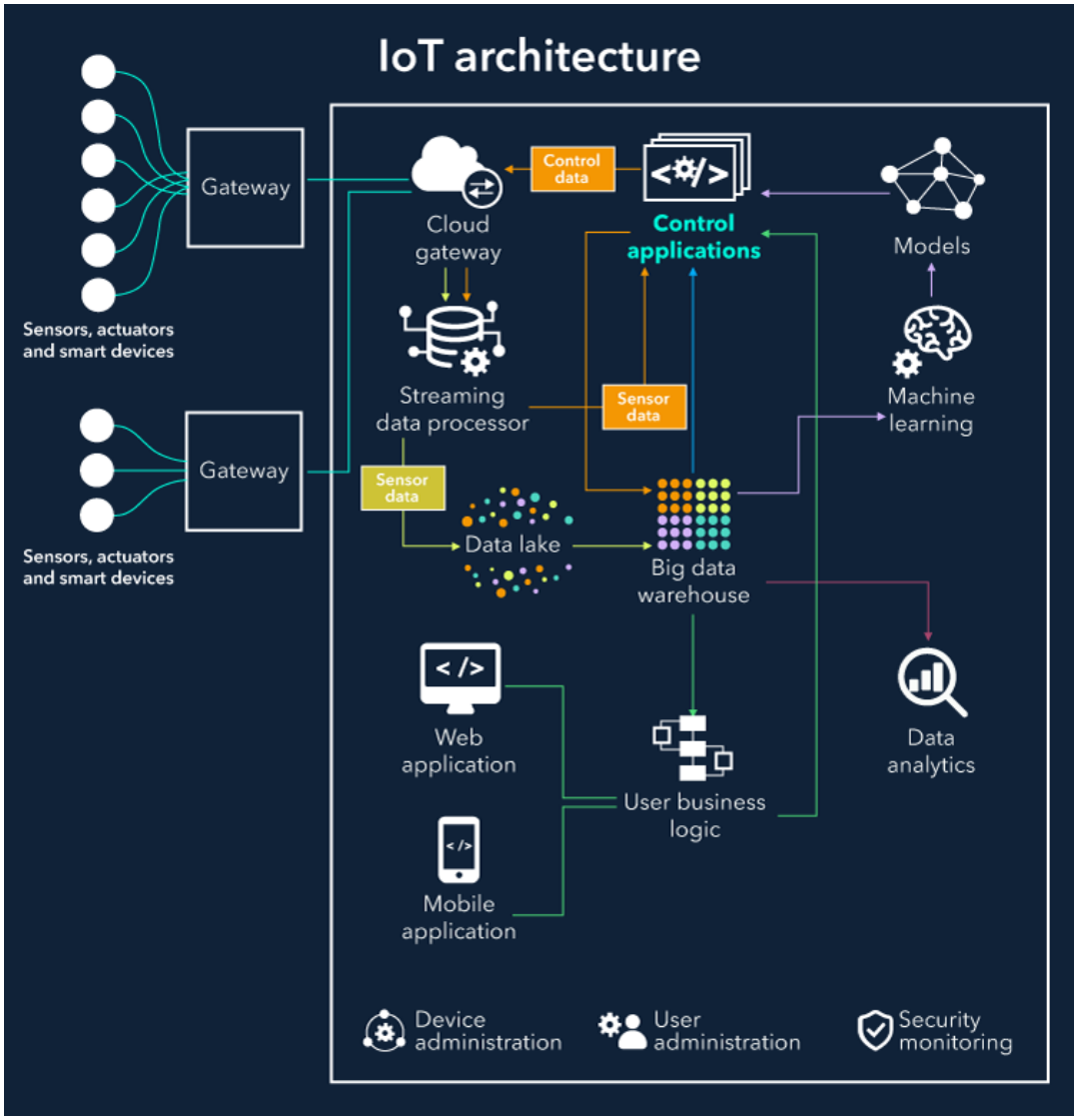
Can you imagine a huge variety of smart devices under the centralized control from one “brain”? To a certain extent, it’s possible with the evolvement of the Internet of Things - the network of physical objects with sensors and actuators, software and network connectivity that enable these objects to gather and transmit data and fulfill users’ tasks.

The effectiveness and applicability of such a system directly correlate with the quality of its building blocks and the way they interact, and there are various approaches to IoT architecture. In this article, our IoT developers will share their hands-on experience and present their original concept of a scalable and flexible IoT architecture.




# Basic elements of IoT architecture

Our approach to IoT architecture is reflected in the IoT architecture diagram which shows the building blocks of an IoT system and how they are connected to collect, store and process data.




**Things.** A “thing” is an object equipped with **sensors** that gather data which will be transferred over a network and **actuators** that allow things to act (for example, to switch on or off the light, to open or close a door, to increase or decrease engine rotation speed and more). This concept includes fridges, street lamps, buildings, vehicles, production machinery, rehabilitation equipment and everything else imaginable. Sensors are not in all cases physically attached to the things: sensors may need to monitor, for example, what happens in the closest environment to a thing.

**Gateways.** Data goes from things to the cloud and vice versa through the gateways. A gateway provides connectivity between things and the cloud part of the IoT solution, enables data preprocessing and filtering before moving it to the cloud (to reduce the volume of data for detailed processing and storing)

and transmits control commands going from the cloud to things. Things then execute commands using their actuators.

**Cloud gateway** facilitates data compression and secure data transmission between field gateways and cloud IoT servers. It also ensures compatibility with various protocols and communicates with field gateways using different protocols depending on what protocol is supported by gateways.

**Streaming data processor** ensures effective transition of input data to a data lake and control applications. No data can be occasionally lost or corrupted.

**Data lake.** A data lake is used for storing the data generated by connected devices in its natural format. Big data comes in "batches" or in “streams”. When the data is needed for meaningful insights it’s extracted from a data lake and loaded to a big data warehouse.

**Big data warehouse.** Filtered and preprocessed data needed for meaningful insights is extracted from a data lake to a big data warehouse. A big data warehouse contains only cleaned, structured and matched data (compared to a data lake which contains all sorts of data generated by sensors). Also, data warehouse stores context information about things and sensors (for example, where sensors are installed) and the commands control applications send to things.

**Data analytics.** Data analysts can use data from the big data warehouse to find trends and gain actionable insights. When analyzed (and in many cases – visualized in schemes, diagrams, infographics) big data show, for example, the performance of devices, help identify inefficiencies and work out the ways to improve an IoT system (make it more reliable, more customer-oriented). Also, the correlations and patterns found manually can further contribute to creating algorithms for control applications.

**Machine learning and the models ML generates.** With machine learning, there is an opportunity to create more precise and more efficient models for control applications. Models are regularly updated (for example, once in a week or once in a month) based on the historical data accumulated in a big data warehouse. When the applicability and efficiency of new models are tested and approved by data analysts, new models are used by control applications.

**Control applications** send automatic commands and alerts to actuators, for example:

- Windows of a smart home can receive an automatic command to open or close depending on the forecasts taken from the weather service.
- When sensors show that the soil is dry, watering systems get an automatic command to water plants.
- Sensors help monitor the state of industrial equipment, and in case of a pre-failure situation, an IoT system generates and sends automatic notifications to field engineers.

The commands sent by control apps to actuators can be also additionally stored in a big data warehouse. This may help investigate problematic cases (for example, a control app sends commands, but they are not performed by actuators – then connectivity, gateways and actuators need to be checked). On the other side, storing commands from control apps may contribute to security, as an IoT system can identify that some commands are too strange or come in too big amounts which may evidence security breaches (as well as other problems which need investigation and corrective measures).

Control applications can be either rule-based or machine-learning based. In the first case, control apps work according to the rules stated by specialists. In the second case, control apps are using models which are regularly updated (once in a week, once in a month depending on the specifics of an IoT system) with the historical data stored in a big data warehouse.

Although control apps ensure better automation of an IoT system, there should be always an option for users to influence the behavior of such applications (for example, in cases of emergency or when it turns out that an IoT system is badly tuned to perform certain actions).

**User applications** are a software component of an IoT system which enables the connection of users to an IoT system and gives the options to monitor and control their smart things (while they are connected to a network of similar things, for example, homes or cars and controlled by a central system). With a mobile or web app, users can monitor the state of their things, send commands to control applications, set the options of automatic behavior (automatic notifications and actions when certain data comes from sensors).

# Device management

To ensure sufficient functioning of IoT devices, it’s far not enough to install them and let things go their way. There are some procedures required to

manage the performance of connected devices (facilitate the interaction between devices, ensure secure data transmission and more):

- **Device identification** to establish the identity of the device to be sure that it's a genuine device with trusted software transmitting reliable data.
- **Configuration and control** to tune devices according to the purposes of an IoT system. Some parameters need to be written once a device is installed (for example, unique device ID). Other settings might need updates (for example, the time between sending messages with data).
- **Monitoring and diagnostics** to ensure smooth and secure performance of every device in a network and reduce the risk of breakdowns.
- **Software updates and maintenance** to add functionality, fix bugs, address security vulnerabilities.

# User management

Alongside with device management, it's important to provide control over the users having access to an IoT system.

User management involves identifying users, their roles, access levels and ownership in a system. It includes such options as adding and removing users, managing user settings, controlling access of various users to certain information, as well as the permission to perform certain operations within a system, controlling and recording user activities and more.

# Security monitoring

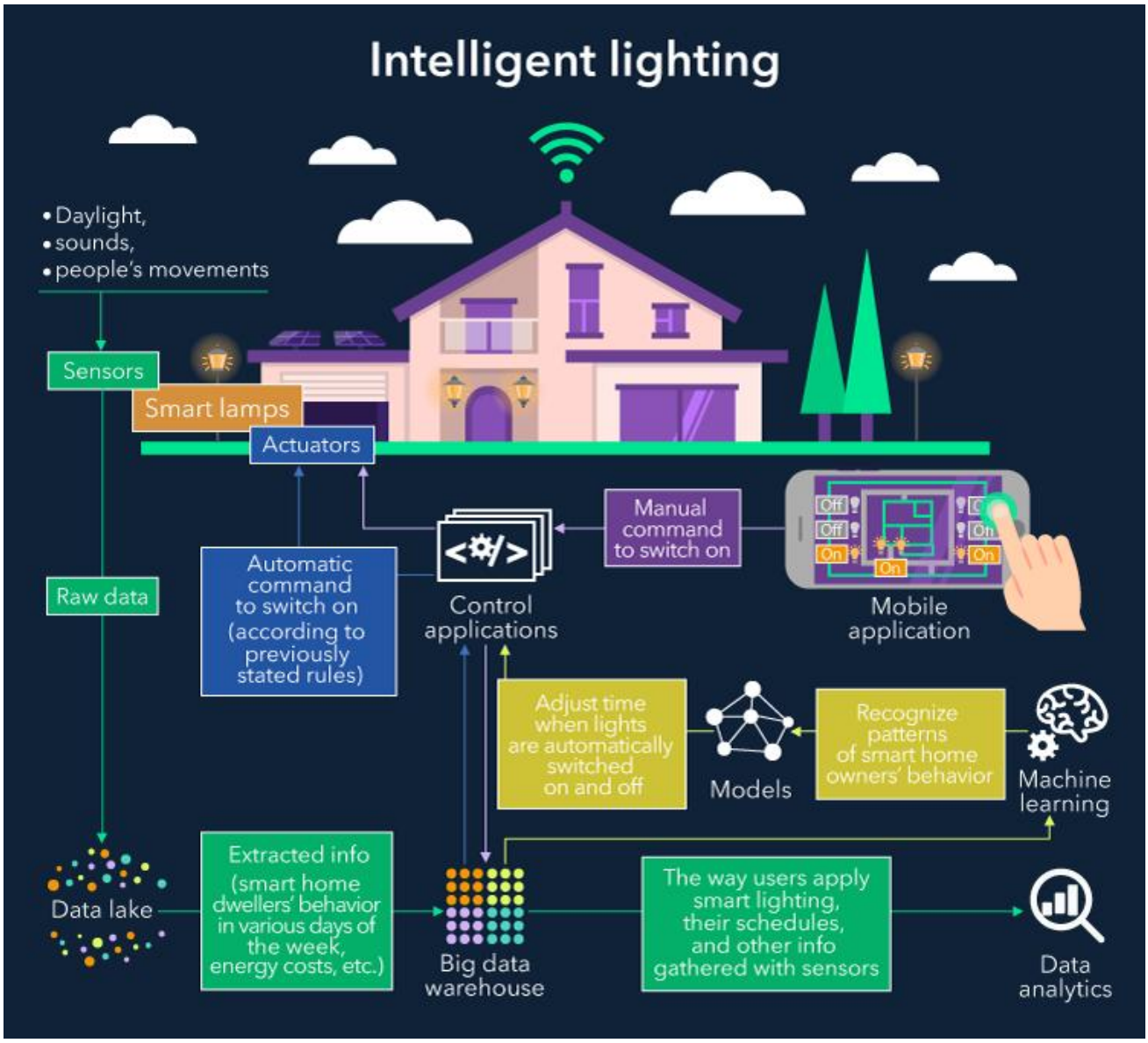
Security is one of the top concerns in the internet of things. Connected things produce huge volumes of data, which need to be securely transmitted and protected from cyber-criminals. Another side is that the things connected to the Internet can be entry points for villains. What is more, cyber-criminals can get the access to the "brain" of the whole IoT system and take control of it.

To prevent such problems, it makes sense to log and analyze the commands sent by control applications to things, monitor the actions of users and store all these data in the cloud. With such an approach, it's possible to address security breaches at the earlies stages and take measures to reduce their influence on an IoT system (for example, block certain commands coming from control applications).

Also, it’s possible to identify the patterns of suspicious behavior, store these samples and compare them with the logs generated by an IoT systems to prevent potential penetrations and minimize their impact on an IoT system.

# IoT architecture example – Intelligent lighting

Let’s see how our IoT architecture elements work together by the example of smart yard lighting as a part of a smart home – a bright illustration of how an IoT solution simultaneously contributes to user convenience and energy efficiency. There are various ways a smart lighting system can function, and we’ll cover basic options.




# Basic components

Sensors take data from the environment (for example, daylight, sounds, people's movements). Lamps are equipped with the actuators to switch the light on and off. A ***data lake*** stores raw data coming from sensors. A ***big data warehouse*** contains the extracted info smart home dwellers' behavior in various days of the week, energy costs and more.

# Manual monitoring and manual control

Users control smart lighting system with a ***mobile app*** featuring the map of the yard. With the app users can see which lights are on and off and send commands to the control applications that further transmit them to lamp actuators. Such an app can also show which lamps are about to be out of order.

**Data analytics**

Analyzing the way users apply smart lighting, their schedules (either provided by users or identified by the smart system) and other info gathered with sensors, data analysts can make and update the algorithms for control applications.

Data analytics also helps in assessing the effectiveness of the IoT system and revealing problems in the way the system works. For example, if a user switches off the light right after a system automatically switches it on and vice versa, there might be gaps in the algorithms, and it's necessary to address them as soon as possible.

# Automatic control's options and pitfalls

The sensors monitoring natural light send the data about the light to the cloud. When the daylight is not enough (according to previously stated threshold), the control apps send automatic commands to the actuators to switch on the lamps. The rest of the time the lamps are switched off.

However, a lighting system can be "baffled" by the street illumination, lamps from neighboring yards and any other sources. Extraneous light captured by sensors can make the smart system conclude that it's enough light, and lighting should be switched off. Thus, it makes sense to give the smart system a better understanding of the factors that influence lighting and accumulate these data in the cloud.

When sensors monitor motions and sounds, it's not enough just to switch on the light when movements or sounds are identified in the yard or switch all the lamps off in the silence. Movements and sounds can be produced, for example, by pets, and cloud applications should distinguish between human voices and movements and those of pets. The same is about the noises coming from the street and neighboring houses and other sounds. To address this issue, it's possible to store the examples of various sounds in the cloud and compare them with the sounds coming from the sensors.

# Machine learning

Intelligent lighting can apply models generated by machine learning, for example, to recognize the patterns of smart home owners' behavior (leaving home at 8 am, coming back at 7 pm) and accordingly adjust the time when lights are switched on and off (for example, switch the lamps on 5 minutes before they will be needed).

Analyzing users' behavior in long-time perspective, a smart system can develop advanced behavior. For example, when sensors don't identify typical movements and voices of home inhabitants, a smart system can "suppose" that smart home dwellers are on a holiday and adjust the behavior: for example, occasionally switch on the lights to give the impression that the house is not empty (for security reasons), but do not keep the lights on all the time to reduce energy consumption.

# User management options

To ensure efficient **user management**, the smart lighting system can be designed for several users with role distribution: for example, owner, inhabitants, guests. In this case, the user with the title "*owner*" will have full control over the system (including changing the patterns of smart light behavior and monitoring the status of the yard lamps) and priorities in giving commands (when several users give contradicting commands, an owner's command will be the one control apps execute), while other users will have access to a limited number of the system's functions. *"Inhabitants"* will be enabled to switch on and off the lamps with no opportunity to change settings. *"Guests"* will be able to switch on and off the light in some parts of the house and have no access to controlling the lights, for example, near the garage.

Apart from role distribution, it's essential to consider ownership (as soon as one system can control over 100 thousand of households, and it's important that a dweller of a smart home manages the lighting in his yard, and not the one of a neighbor).

# Instead of a conclusion

In simple terms, our IoT architecture contains the following components:

- **Things** equipped with **sensors** to gather data and **actuators** to perform commands received from the cloud.
- **Gateways** for data filtering, preprocessing and moving it to the cloud and vice versa, – receiving commands from the cloud.
- **Cloud gateways** to ensure data transition between field gateways and central IoT servers.
- **Streaming data processors** to distribute the data coming from sensors among relevant IoT solution's components.
- **Data lake** for storing all the data of defined and undefined value.
- **Big data warehouse** for collecting valuable data.
- **Control applications** to send commands to actuators.
- **Machine learning** to generate the models which are then used by control applications.
- **User applications** to enable users to monitor control their connected things.
- **Data analytics** for manual data processing.

Our IoT architecture also contains device and user management components to provide stable and secure functioning of things and control user access issues.

Developing an IoT architecture of a particular solution, it's also important to focus on consistency (giving enough attention to every element of IoT architecture and making them work together), flexibility (opportunity to add new functions and new logic) and integration with enterprise systems (teaming up new IoT solutions with previously implemented corporate IT solutions such as ERP, MES, WMS, delivery management systems and more).

# How to evaluate an IoT data platform

In the exploding world of IoT, it can be challenging to navigate through all of the buzzwords, acronyms, and platform options to understand the major impact IoT devices will have in the future. We get asked all of the time, “What capabilities should we be looking for in an IoT data platform as we comb through all of the options out there?” Here are the four capabilities you should look for in an IoT data platform, to build anything from smart home automation systems to large scale industrial IoT.

## 1. Connectivity

It starts with how a device or sensor connects to the internet and a cloud platform. There are many options to choose from WiFi through a hub or gateway, 2G, or 3G cellular networks. Once you have connectivity in place, now you can get the device or sensor talking to your cloud IoT platform. Ensure you find a service provider that can send data through clean API’s that are easy to implement and install. This will ensure you can get quickly setup and start capturing your data within minutes.

## 2. Control

The next capability necessary when evaluating an IoT data platform is control of the device. There are a number of different scenarios for control including controlling a device through an application, device-to-device communication, or control from the cloud (based on an event, rule or some other pre-determined condition). For example, if you have a water leak detector, it can automatically send a command to the device which could be an appliance or part of the core infrastructure to turn off the water valve. Here, using two-way communication, a signal can be sent from the detector to the device via the cloud to shut off the water. Lastly, you can program the device from an app (or website) to shut off at a certain time or schedule based on a pre-programmed rule.

### 3. Device Management

Device management is also a major consideration. To keep devices and sensors up to date and functional, a strong device management solution is a core component of an IoT cloud platform.
There are a few main capabilities a device management platform provides, including the ability for manufacturers to send software or firmware updates OTA (over-the-air), factory provisioning, as well as an out-of-box experience (OOBE).OOBE is part of a core experience that is often left to the last minute or completely glossed over. It's the first experience that an end user, be it a consumer, installer or technician has when interacting with a device for the first time. A great OOBE experience significantly increases the probability of an end user successfully installing and configuring a device. Furthermore, it reduces the likelihood of a support call or the end user returning the product altogether.

### 4. Actionable Data

The last capability you should consider in aIoT data platform is how you can query the data in a manner that is clear and meaningful. It's one thing to get all your data in place, but the value of the data is only realized when it's turned into information that can help solve a problem. We want organizations to focus on their core competency, like making great appliances or services that

deliver value to their customers, rather than focusing on cloud infrastructure that makes it possible. At Buddy, our job is to provide an end-to-end turn-key solution to connect the world's IoT devices and provide real-time business insights for decision making. That can take the form of simple dashboard or deep analytics through integration with partners and services.

Keep it simple when you're evaluating IoT data platform options. If a platform is connected, allows two-way communication to the device, device management and a visual IoT data graph, these are the main areas you should focus on during your process.

The Internet of Things is one of the most important and promising technological topics today. Some market researchers estimate that there are more than 20 billion connected devices and counting. Around us, there are smartphones, wearables, and other devices, all of which use sensors. Nowadays, sensors play an important role in our everyday life and in IoT. Sensors monitor our health status (e.g. a heartbeat), air quality, home security, and are widely used in the Industrial Internet of Things (IIoT) to monitor production processes. For these reasons, it is important to know how they work and how we can use them to acquire information.

## How to improve business processes with Internet of Things (IoT)?



Internet of Things (IoT) is a trending topic these days, but you might be wondering how companies should take advantage on new technological improvements, and avoid to get lost trying to implement IoT for every single step within the business processes.

We have been developing IoT projects for some time now and have built some solutions and prototypes for our customers, we have done some analysis on how to improve business processes with tech-wise operations using IoT. But have found sometimes immerse on huge opportunities that takes more time or resources to develop, so cost-benefit might bend the balance on not getting the expected result at the first time.

IoT uses are to automate process, gather valuable information, extend business functions, trigger rules, source predictive analytics and big data, among other useful objectives.

Here are some recommendations on implementing IoT business processes in your companies:

1. To define business process to improve and identify the problem you want to solve. Make sure to bring a solution to few problems at once, don't try to solve every single problem within your company. Lean principles and Design Thinking methodology can help to identify main problems to avoid losing valuable time.
2. Use an end-to-end approach. Even though you are trying to solve a single issue, map end-to-end process to make sure you are not missing anything on your analysis. Processes may involve several operational areas; they touch more than one ecosystem (Machinery, Devices, Customers, Vendors, ERP, CRM, etc.); they are driven by a bunch of people; and for sure they don't stop where you believe they do. Actually IoT could be used for many purposes, just find the right one for the process improvement.
3. Make AGILE design and start with POC (proof of concept) prototyping. Do not try to build a solution 100% ready at the first iteration, it's better to start with a prototype to be perfectible within 2 or 3 design iterations maximum, then go for construction with volume, security, profiles and the rest of "best practices" for architecture considerations. Make quick wins instead of trying to win the war at the very first step, that will not happen at the beginning of the innovation process. You will need to find perfect balance between short strings, design iterations, solution deepness and project length, that in itself is a great challenge you will face on these projects.
4. Get on board the right people, better if you keep it low but with the best knowledge. Always a very trite phrase, but you need to make sure the right team is placed to build an IoT solution, so consider business processes, technical needs, architecture compliance and that's it. The Leader must provide direction to the team to obtain goals on short strings and drive the boat to its final destiny, finally sponsorship must be involved at all IoT project stages.
5. Be persistent but acknowledgeable to failure. This is not a regular, long and high-cost IT project, persistency is a quality everybody should embrace, but as lessons are learned and challenges are raised, the team may change directions to look forward into final goals, do not be discouraged if this happens. Short strings will allow you to make changes to adjust to achieve results without bigger impacts.
6. Disruption could be there, but don't go crazy about it. IoT does not mean disruption at all costs, most of the companies that hear about innovation with IoT think on disruptive paths, the thing is you can get lost looking for disruption that does not exist. You better be prepared to identify it when happens, but don't waste valuable time to make disruptive changes or improvements if is not part of your final destination. Companies looking for disruption should be analyzing different ways to get there, but they should not just pigeonhole it with the IoT path.
7. Do not connect things to internet without a purpose. Connecting things to internet without a purpose is a waste of time and money, think on real needs and how to solve them by not connecting whatever is on your way. This is a really difficult task while technology is at reach and costs have been dropping. The way to define this is set by operational, analytical and business purposes rather than technological accessibility, design thinking should be oriented by business process not by tech drivers.
8. Make solutions simple, scalable and modular so they are able to support growth into volume and additional functions. When design iterations happen and functionality needs are defined, you will need to create a solid basis to increase functions, data processing, users access, security, etc. This should not be contradictory with the AGILE approach since you are creating a modular and scalable solution, furthermore be savvy when designing and building to avoid slowing down iterations and development with a rigid structure on the solution.

9. One of the most important for IoT projects is to define a business plan involved with the IoT project but don't expect to fulfill it with the exact amounts and numbers, also huge investments need to be avoided. Better keep the budget down to strings and not big projects that can discourage the sponsors who are providing the funds for improvements, please consider right KPI's and fine measures to validate those improvements.
10. Try to choose right technology and do not hesitate to change it when needed, IoT could be delivered with all kind of new tools out in the market, on defining the right one from the beginning will challenge your skills. Even though your decision was incorrect by the learning process, if changes are needed, you should make them and learn from it.

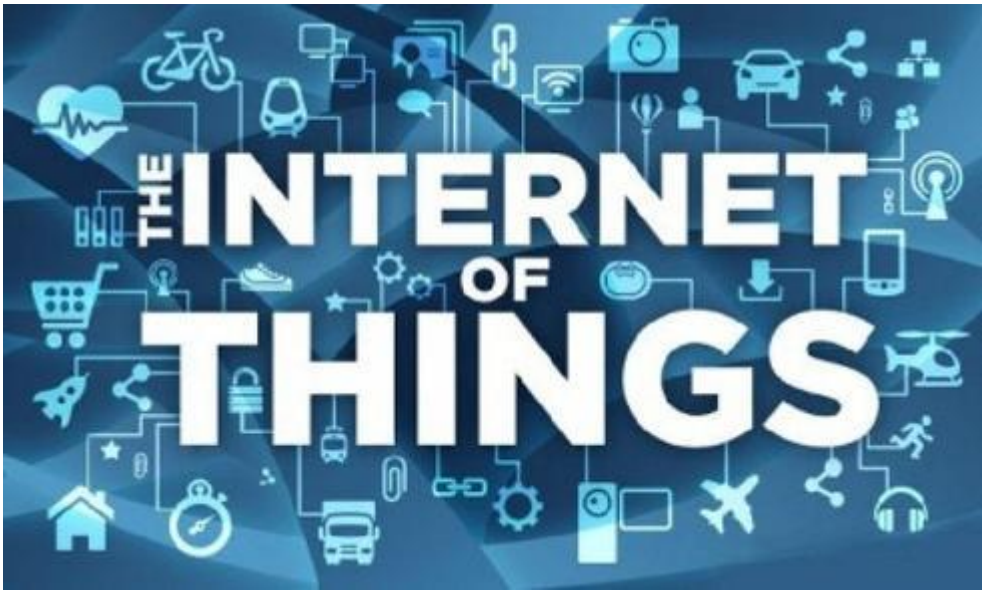
SAP is offering a set of Internet of Things (IoT) connections within SAP Cloud Platform (previously named HCP) and SAP Leonardo. It is hard to imagine that every company will define the same things to connect to, so that might not be packaged, but what is really interesting is that you could have IoT connectivity within same Architecture (SAP). IoT solutions can include SOA, BPM integration with cloud or on-premise capabilities that allows to connect with different protocols and devices, also rules modeling, on-memory database processing power with HANA, several computing language programming, and analytical capabilities to go through large information volumes. So when mapping end-to-end processes to improve with IoT, think on connecting different devices to several systems, where you can pull triggers, define alerts, set rules, analyze data, automate steps and make operations simpler according with business needs.

There are huge opportunities to make Things better with the proliferation of IoT homes, cars (telematics), cities, healthcare, and manufacturing.

Here are three key ways businesses can transform their operations with IoT technologies:

**1. Elevate the focus from technology to processes**

The real digital transformation of IoT will happen through digital processes. Cisco (which characterizes IoT as Internet of Everything), believes people, data, and processes are essential components. A key requirement for the success of IoT is the end-to-end digitization of processes. What do I mean by processes? A process has (a) inputs; (b) execution of tasks; and (c) business outcome upon completion of the tasks.




Traditionally, process automation was coordinated around humans, business partners, or enterprise applications. That landscape is changing with the rise of Things. Take, for example, a complex and dynamic digital process: the coordination of the arrival and departure of an airplane in a busy airport. The business outcome is the timely departure. The participants include airport staff (baggage, refueling, catering) as well as Things that can be queried for sensor data or asked to carry out tasks. Autonomous or semi-autonomous Things are becoming active participants in *business* processes.

So IT in increasingly digital enterprises needs to provide not only the technology infrastructure for Things, but also a business process automation platform for making Things part of *business* outcomes. Thing tasks can be as simple as responding with a sensor value (e.g. what is the cabin temperature?) or as complex as how to circumnavigate a fast-moving storm.

**2. Handling crisis events and digitizing change**

How do these processes with Things get manifested? The airport example above illustrates a "happy path" coordinating humans and Things. However, one of the most pervasive use cases for Things is sensing (through IoT sensors) a crisis event and then activating a digitized end-to-end process to respond to it. This happens when there is a vehicle accident, boiler explosion, security alarm, or elevated blood pressure. The Thing autonomously senses and then either directly, or through a brokering layer, activates an *exception* process. This typically includes monitoring back-office and field workers to respond and resolve the problem.

**3. Thing data analytics**

Often, it's not merely an individual event that starts a process. Big data will eventually become "Thing Data." Through our connected homes, connected cities, and industries (such as power plants), Things are generating enormous amounts of data. Visualization of the data and analytics can be applied to streams of sensor data that are then handled via automated processes involving humans and Things. In a connected city that may have hundreds of thousands of sensors on city infrastructures, this could be applied for transportation, pollution sensing, or power grids.

For example, in a connected city application, multiple sensors could be monitoring pollution levels in the air or water. Then, if the critical levels are reached from this analysis of "thing data" over a period of time, exception handling processes would kick in. The difference from what I describe in the No. 2 point is that the exception here is detected and analyzed from multiple sources and typically over a period of time versus a single event. Both are important use cases in dealing with a situation through a digitized automated process.

While some dismiss it as hype, the pervasiveness of the Internet of Things is unquestionable.  Estimates show there will be 25 billion to 1 trillion connected Things by 2020. These all must be coordinated with people and applications

within the enterprise through business processes. After all, isolated things have little value.

n extensive number of modern digital services, products and tools are ordered over the Internet and delivered to users on demand, rather than provided via local channels within enterprises or specialized organizations. To describe this phenomenon, a special term was invented: **Everything-as-a-Service (XaaS)**.

What is Everything-as-a-Service? Read our article for an explanation.

# What Is XaaS?

Everything-as-a-Service is a term for services and applications that users can access on the Internet upon request.

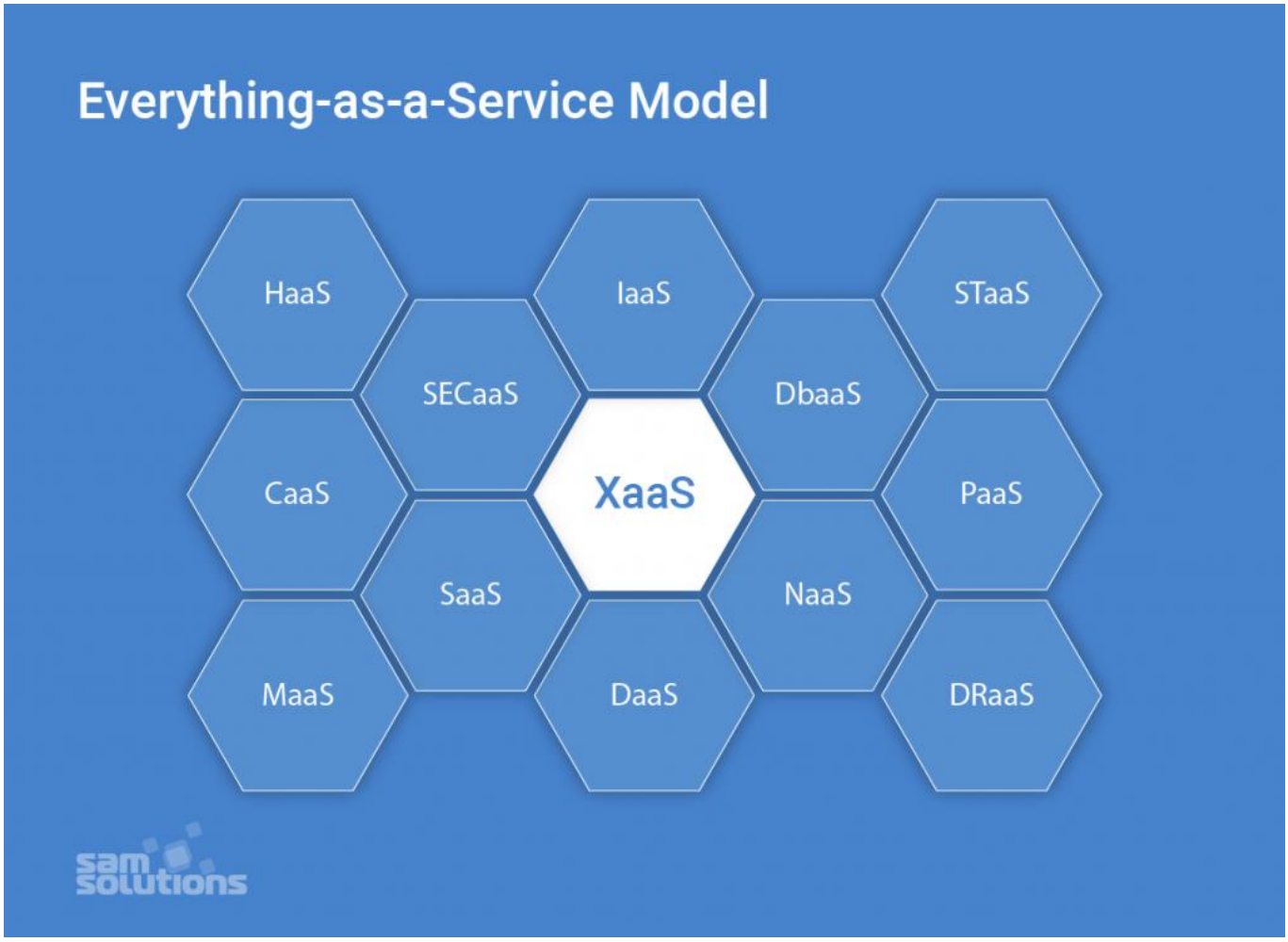
The Everything-as-a-Service definition may seem unclear at first sight, but actually, it is not difficult to understand. It all started with the cloud computing terms: SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service) and IaaS (Infrastructure-as-a-Service), meaning that ready-made software, a platform for its development, or a comprehensive computing infrastructure could be provided via networks. Gradually, other offerings appeared and now, the designation as-a-Service is associated with various digital components, e.g. data, security, communication, etc.

**Read also:** IaaS vs. PaaS vs. SaaS: What's the Difference?

What's more, Anything-as-a-Service (another name for XaaS) is not confined to digital products. You can get practically everything, from food to medical consultations, without leaving your home or office, by utilizing certain online services. Hence the "Everything" is in the name.

# Everything-as-a-Service Model Examples

Now that we've covered the XaaS definition, it's time to demonstrate some practical -aaS cases (apart from SaaS, PaaS and IaaS) that are gaining popularity.




**Hardware-as-a-Service (HaaS)**

Managed service providers (MSP) own some hardware and install it on customers' sites on demand. Customers utilize the hardware in accordance with service level agreements. This pay-as-you-go model is similar to leasing and can be compared to IaaS when computing resources are located at MSP's site and provided to users as virtual equivalents of physical hardware.

The Haas model is especially cost-effective for small or mid-sized businesses.

**Communication-as-a-Service (CaaS)**

This model includes different communication solutions such as VoIP (voice over IP or Internet telephony), IM (instant messaging), video conference applications that are hosted in the vendor's cloud. A company can selectively deploy communication apps that best suit their current needs for a certain period and pay for this usage period only.

Such an approach is cost-effective and reduces expenses for short-time communication needs.

**Desktop-as-a-Service (DaaS)**

Desktops are delivered as virtual services along with the apps needed for use. Thus, a client can work on a personal computer, using the computing capacities of third-party servers (which can be much more powerful than those of a PC).

A DaaS provider is typically responsible for storing, securing and backing up user data, as well as delivering upgrades for all the supported desktop apps.

**Security-as-a-Service (SECaaS)**

This is the model of outsourced security management. A provider integrates their security services into your company's infrastructure and, as a rule, delivers them over the Internet. Such services may include anti-virus software, encryption, authentication, intrusion detection solutions and more.

**Healthcare-as-a-Service (HaaS)**

With electronic medical records (EMR) and hospital information systems (HIS), the healthcare industry is transforming into Healthcare-as-a-Service. Medical treatment is becoming more data-driven and patient-centric. Thanks to the IoT, wearables and other emerging technologies, the following services are available:

- Online consultations with doctors
- Health monitoring 24/7
- Medicine delivery at your doorstep
- Lab samples collection even at home and delivery of results as soon as they are ready
- Access to your medical records 24/7

HaaS creates opportunities for almost all categories of citizens to get qualified medical help.

**Read also: Digital Health: the New Concept to Improve Medical Care**

**Transportation-as-a-Service (TaaS)**

Important trends of modern society are mobility and freedom of transportation at different distances. There are numerous apps popping up connected with transport, so a part of this industry is transforming into an -aaS model. The most vivid examples are:

- **Carsharing** (you can rent a car at any place via a special app and drive anywhere you need, paying for the time you use a car, or for the distance you cover)
- **Uber taxi services** (you order a taxi via an app, which calculates the cost of the rout in advance). Uber is planning to test flying taxis and self-driving planes in the near future.

TaaS model is not only convenient but also ecologically friendly.

# Benefits of XaaS

The market of services provided via cloud computing and the Internet is expanding at a rapid pace due to a range of advantages they provide both for organizations and end-users. The biggest benefits are:

- **Scalability** (outsourcing provides access to unlimited computing capacities, storage space, RAM, etc; a company can quickly and seamlessly scale its processes up and down depending on requirements and doesn't have to worry about additional deployments or downtimes)
- **Cost- and time-effectiveness** (a company doesn't purchase its personal equipment and doesn't need to deploy it, saving much time and money; a pay-as-you-go model is also beneficial)
- **Focus on core competencies** (there's no need to set up apps and programs or conduct training for employees; consequently, they can concentrate on their direct duties and achieve better performance)
- **The high quality of services** (since professionals support and maintain your infrastructure and systems, they provide the latest updates and all the emerging technologies, guaranteeing the quality of services)
- **Better customer experience** (the above-mentioned pros lead to customer satisfaction and increase customer loyalty)

However, -aaS services are not without flaws. The biggest drawbacks are mostly related to end users and concern the security of personal data and risks of massive data loss.

Many consumers are afraid to fully depend on cloud providers and lose control over their business. Service providers, on their part, are doing their best to address such concerns and allow organizations to migrate more workloads into the cloud.

# Bottom Line

What is XaaS in short? This is a conceptual model consisting of all possible services and products that can be provided over networks. At the moment, there is no full implementation of this model. Pushing for XaaS is an ideal benchmark and one of the main strategies for leading global cloud companies such as Microsoft and Google.

The future of Everything-as-a-Service seems to be bright due to emerging technologies and the proliferation of the eCommerce market.

SaM Solutions is pleased to offer you our ready-to-use PaaS — CloudBOX (Build-Operate-eXtend). It can be easily customized to your business needs and provide a range of benefits. Contact us to learn more about this very offering or other services we provide.

The Internet of Things (IoT) has gradually transformed the way daily tasks are completed. Take smart homing for instance. People can start their cooling devices remotely through their mobile phones. This earlier used to be possible via an SMS, but today the internet has made it easier. Apart from providing smarter solutions for homes and housing communities, IoT has also been used as a tool in business environments across various industries. However, with the amount of big data that is generated by IoT, a lot of strain is put on the internet infrastructure. This has made businesses and organizations look for an option that would reduce this load.

Enter cloud computing- an on-demand delivery of computing power, database storage, applications and IT resources. It enables organizations to consume a compute resource, like a virtual machine (VM) instead of building a computing infrastructure on premise.

Today, cloud computing has more or less penetrated mainstream IT and its infrastructure. Many tech biggies such as Amazon, Alibaba, Google and Oracle are building machine learning tools with the help of cloud technology to offer a wide range of solutions to businesses worldwide. This article aims to inform you of the role of cloud computing in IoT and why IoT and cloud computing are inseparable.

How IoT and cloud complement each other

Cloud computing, as well as IoT, work towards increasing the efficiency of everyday tasks and both have a complementary relationship. On one hand, IoT generates lots of data while on the other hand, cloud computing paves way for this data to travel. There are many cloud providers who take advantage of this to provide a pay-as-you-use model where customers pay for the specific resources used. Also, cloud hosting as a service adds value to IoT startups by providing economies of scale to reduce their overall cost structure.

In addition to this, cloud computing also enables better collaboration for developers, which is the order of the day in the IoT space. By facilitating developers to store as well as access data remotely, the cloud allows developers to implement projects without delay. Also, by storing data in the cloud, IoT companies can access a huge amount of Big Data. So, in a bid to lay down the relationship between IoT and cloud, here is a table that will let you know how they fit into each other like a glove.

| Parameter | Internet of things | Cloud computing |
|---|---|---|
| Big Data | Acts as a source for big data | Acts as a way or a means to manage big data |
| Reachability | Very limited | Far spread, wide |
| Storage | Limited or almost none | Large, virtually never ending |
| Role of Internet | Acts as a point of convergence | Acts as a means for delivering services |
| Computing capabilities | Limited | Virtually unlimited |
| Components | Runs on hardware components | Runs on virtual machines which imitate hardware components |

Why is Cloud essential to the success of IoT?

Just like cloud computing is built on the tenets of speed and scale, IoT applications are built on the principle of mobility and widespread networking. Hence, it is essential that both cloud and IoT form cloud-based IoT applications in a bid to make the most out of their combination. This alliance has led to the success of IoT. In addition to this, here are a few more pointers as to why the cloud is important from the point of view of IoT's success.

Provides remote processing power

Cloud as a technology empowers IoT to move beyond regular appliances such as air conditioners, refrigerators etc. This is because the cloud has such a vast storage that it takes away dependencies on on-premise infrastructure. With the rise of miniaturization and transition of 4G to higher internet speeds, the cloud will allow developers to offload fast computing processes.

Provides security and privacy

IoT's role in harnessing mobility is immense. However, its prowess would be incomplete without security. Cloud has made IoT more secure with preventive, detective and corrective controls. It has

enabled users with strong security measures by providing effective authentication and encryption protocols. In addition to this, managing and securing the identity of users has been possible for IoT products with the help of biometrics. All of this is possible because of cloud's security.

Removes entry barrier for hosting providers

Today, many innovations in the field of IoT are looking at plug-and-play hosting services. Which is why the cloud is a perfect fit for IoT. Hosting providers do not have to depend on massive equipment or even any kind of hardware that will not support the agility IoT devices require. With the cloud, most hosting providers can allow their clients a ready-to-roll model, removing entry barriers for them.

Facilitates inter-device communication

Cloud acts as a bridge in the form of a mediator or communication facilitator when it comes to IoT. Many powerful APIs like Cloudflare, CloudCache and Dropstr are enabled by cloud communications, allowing easy linking to smartphones. This eases devices to talk to each other and not just us, which essentially is the tenet of IoT cloud.

It would be fair to say that cloud can accelerate the growth of IoT. However, deploying cloud technology also has certain challenges and shortcomings. Not because the cloud is flawed as a technology but the combination of IoT cloud can burden users with some obstacles. If you ever go ahead with an IoT cloud solution, it is better if you know the kind of challenges you may face in advance.

What are the challenges posed by cloud and IoT together?

Handling a large amount of data

Handling a large amount of data can be overwhelming especially when there are millions of devices in the picture. This is because the overall performance of applications is at stake. Hence, following the NoSQL movement could be beneficial, but it is not tried and tested for the long run. Which is why there exists no sound or fool-proof method for the cloud to manage big data.

Networking and communication protocols

Cloud and IoT involve machine-to-machine communications among many different types of devices having various protocols. Managing this kind of a variation could be tough since a majority of application areas do not involve mobility. As of now WiFi and Bluetooth are used as a stop-gap solution to facilitate mobility to a certain extent.

Sensor networks

Sensor networks have amplified the benefits of IoT. These networks have allowed users to measure, infer and understand delicate indicators from the environment. However, timely processing of a large amount of this sensor data has been a major challenge. Though cloud provides a new opportunity in aggregating sensor data it also hinders the progress because of security and privacy issues.

Conclusion

The integration of cloud computing and IoT is indicative of the next big leap in the world of internet. New applications brimming from this combination known as IoT Cloud are opening newer avenues for

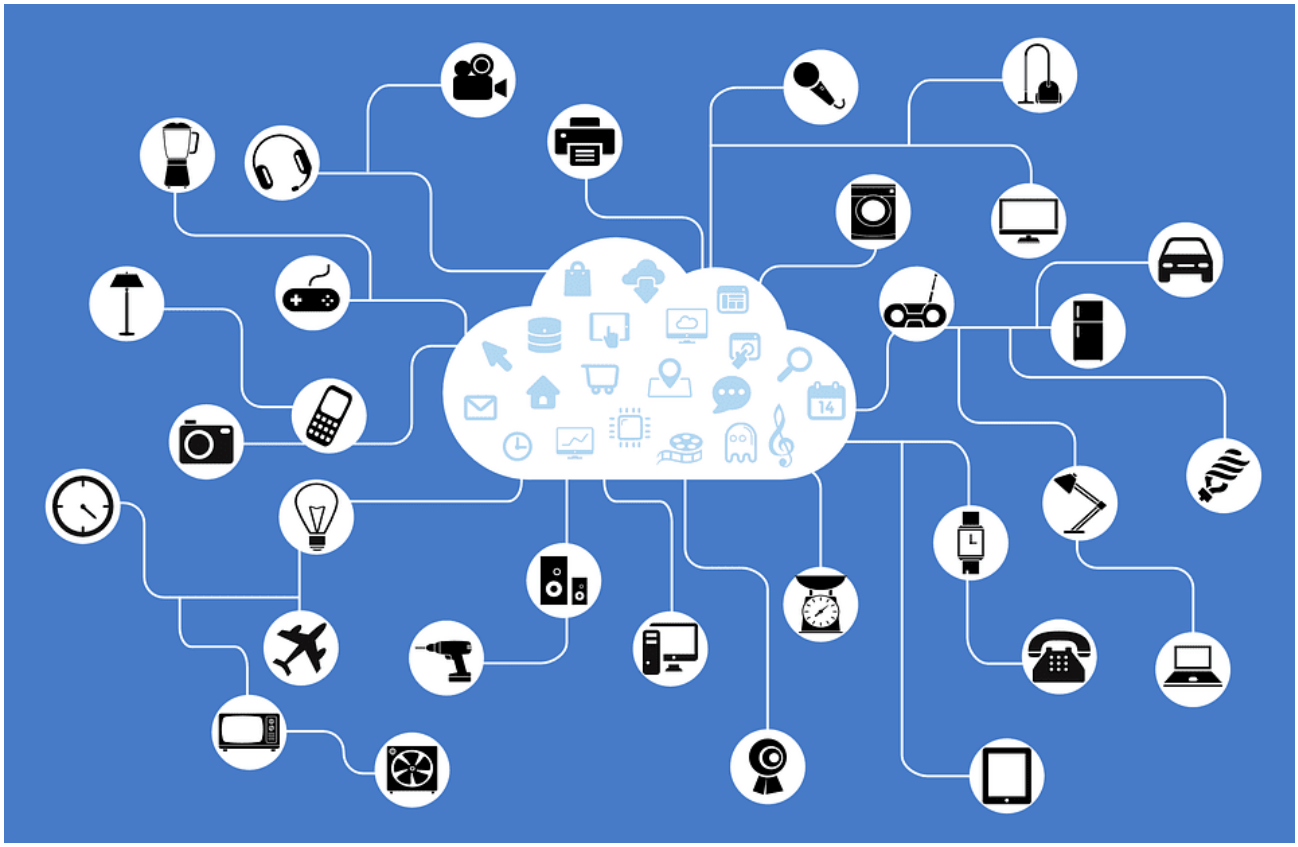
business as well as research. Let us hope that this combination unveils a new paradigm for the future of multi-networking and an open service platform for users.

We hope that you know what role cloud as a technology can play in unlocking IoT's true potential. If you have any doubts about- What is the role of cloud computing in IoT? please feel free to leave your feedback in the comments section below.

On October 2016, a hacker found a vulnerability on a specific model of security cameras. Nearly 300,000 Internet of Things (IoT) video recorders started to attack multiple social network websites and brought down Twitter and other high-profile platforms, for almost two hours.

This attack is just an example of what can happen to IoT devices with poor security.

It is not only video cameras, but anything with an internet connection, from a refrigerator, smart locks, thermostats, lightbulbs, vehicles, and even smart toys. Using them always poses IoT security challenges and risks to overcome.



# IoT Security Challenges

Now, it is not only us with our computers, but there are also “things” that interact with the Internet without our intervention. These “things” are continually communicating with the Internet, a fridge sending an update of the food inside or our vehicle transmitting messages to the mechanic to inform its oil levels.

IoT is wonderful in many ways. But unfortunately, technology has not matured yet, and it is not entirely safe. The entire IoTenvironment, from manufacturers to users, still have many security challenges of IoT to overcome, such as:

- Manufacturing standards
- Update management
- Physical hardening
- Users knowledge and awareness

# Top IoT Security Risks

Returning to what happened in 2016, the lack of compliance on the part of IoT manufacturers led to weak and unprotected passwords in some IoT video cameras, which, in turn, led to one of the most damaging botnet attacks, the Mirai malware. There are many IoT security threats, but we will be highlighting the most important.

The following **security issues with IoT can be classified as a cause or effect.**

# 1) Lack Of Compliance On The Part Of IoT Manufacturers

New IoT devices come out almost daily, all with undiscovered vulnerabilities. **The primary source of most IoT security issues is that manufacturers do not spend enough time and resources on security.**

For example, most fitness trackers with Bluetooth remain visible after the first pairing, a smart refrigerator can expose Gmail login credentials, and a smart fingerprint padlock can be accessed with a Bluetooth key that has the same MAC address as the padlock device.

This is precisely one of the biggest security issues with IoT. While there is a lack of universal IoT security standards, manufacturers will continue creating devices with poor security. Manufacturers that started to add Internet connection to their devices do not always have the “security” concept as the crucial element in their product design process.

The following are some security risks in IoT devices from manufacturers:

1. Weak, guessable, or hard-coded passwords

2. Hardware issues
3. Lack of a secure update mechanism
4. Old and unpatched embedded operating systems and software
5. Insecure data transfer and storage


*A smart thermostat*

# 2) Lack Of User Knowledge & Awareness.

Over the years, Internet users have learnt how to avoid spam or phishing emails, perform virus scans on their PCs, and secure their WiFi networks with strong passwords.

But IoT is a new technology, and people still do not know much about it. While most of the risks of IoT security issues are still on the manufacturing side, users and businesses processes can create bigger threats. One of the biggest IoT security risks and challenges is the user's ignorance and lack of awareness of the IoT functionality. As a result, everybody is put at risk.

Tricking a human is, most of the time, the easiest way to gain access to a network. A type of IoT security risk that is often overlooked is **social engineering attacks**. Instead of targeting devices, a hacker targets a human, using the IoT.

Social engineering was used in the 2010 Stuxnet attack against a nuclear facility in Iran. The attack was directed to industrial programmable logic controllers (PLCs), which also fall into an IoT device category. The attack corrupted 1,000 centrifuges and made the plant explode. It is believed that the internal network was isolated from the public network to avoid attacks, but all it took was a worker to plug a USB flash drive into one of the internal computers.

# 3) IoT Security Problems In Device Update Management

Another source of IoT security risks is insecure software or firmware. Although a manufacturer can sell a device with the latest software update, it is almost inevitable that new vulnerabilities will come out.

Updates are critical for maintaining security on IoT devices. They should be updated right after new vulnerabilities are discovered. Still, as compared with smartphones or computers that get automatic updates, some IoT devices continue being used without the necessary updates.

Another risk is that during an update, a device will send its backup out to the cloud and will suffer a short downtime. If the connection is unencrypted and the update files are unprotected, a hacker could steal sensitive information.

# 4) Lack Of Physical Hardening

The lack of physical hardening can also cause IoT security issues. Although some IoT devices should be able to operate autonomously without any intervention from a user, they need to be physically secured from outer threats. Sometimes, these devices can be located in remote locations for long stretches of time, and they could be physically tampered with, for example using a USB flash drive with Malware.

Ensuring the physical security of an IoT device begins from the manufacturer. But building secure sensors and transmitters in the already low-cost devices is a challenging task for manufacturers nonetheless.

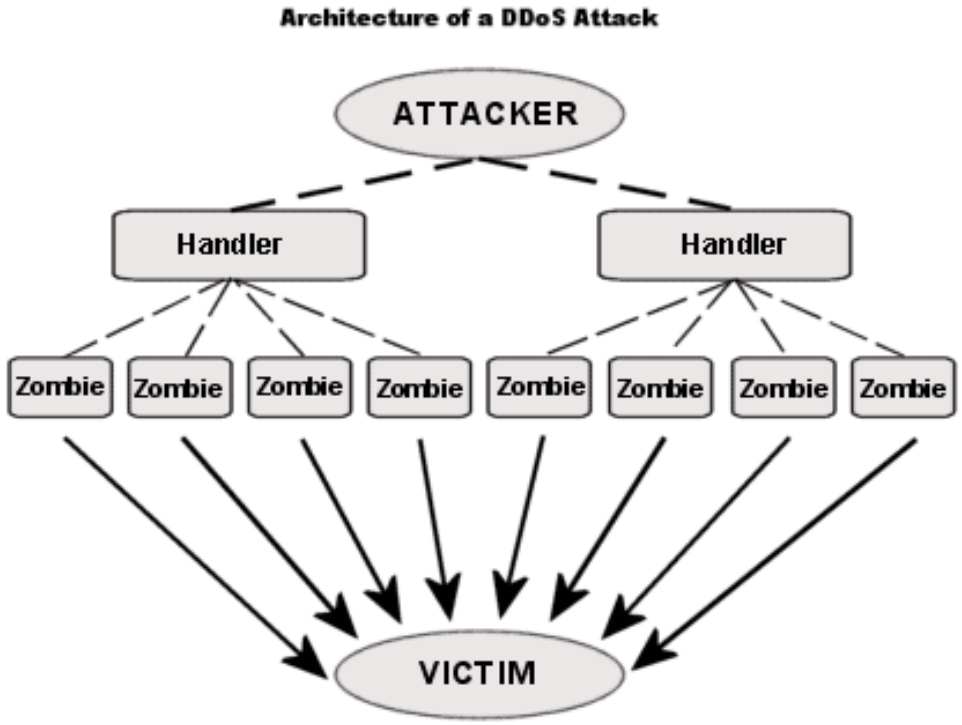
Users are also responsible for keeping IoT devices physically secured. A smart motion sensor or a video camera that sits outside a house could be tampered with if not properly protected.

# 5) Botnet Attacks

A single IoT device infected with malware does not pose any real threat; it is a collection of them that can bring down anything. To perform a botnet attack, a hacker creates an army of bots by infecting them with malware and directs them to send thousands of requests per second to bring down the target.

Much of the uproar about IoT security began after the Mirai bot attack in 2016. Multiple DDoS (Distributed Denial of Service) attacks using hundreds of thousands of IP cameras, NAS, and home routers were infected and directed to bring down the DNS that provided services to platforms like GitHub, Twitter, Reddit, Netflix, and Airbnb.

**The problem is that IoT devices are highly vulnerable to Malware attacks.** They do not have the regular software security updates that a computer has. So they are quickly turned into infected zombies and used as weapons to send incredibly vast amounts of traffic.




What is more, a botnet can pose a security threat for electrical grids, manufacturing plants, transportation systems, and water treatment facilities, which can threaten big groups of people. For example, a hacker could trigger a cooling and heating system at the same time, creating spikes on the power grid; in case of a big-scale attack, hackers can create a nation-wide power outtage.

# 6) Industrial Espionage & Eavesdropping

If hackers take over surveillance in at location by infecting IoT devices, spying might not be the only option They can also perform such attacks to demand ransom money.

Thus, **invading privacy is another prominent IoT security issue**. Spying and intruding through IoT devices is a real problem, as a lot different sensitive data may be compromised and used against its owner.

On a basic level, a hacker might want to take over a camera and use it for spying. Still, one should not forget that many IoT devices record user information, whether it is health equipment, smart toys, wearables, etc. On an industrial level, a company's big data that can be collected by hackers to expose sensitive business information.

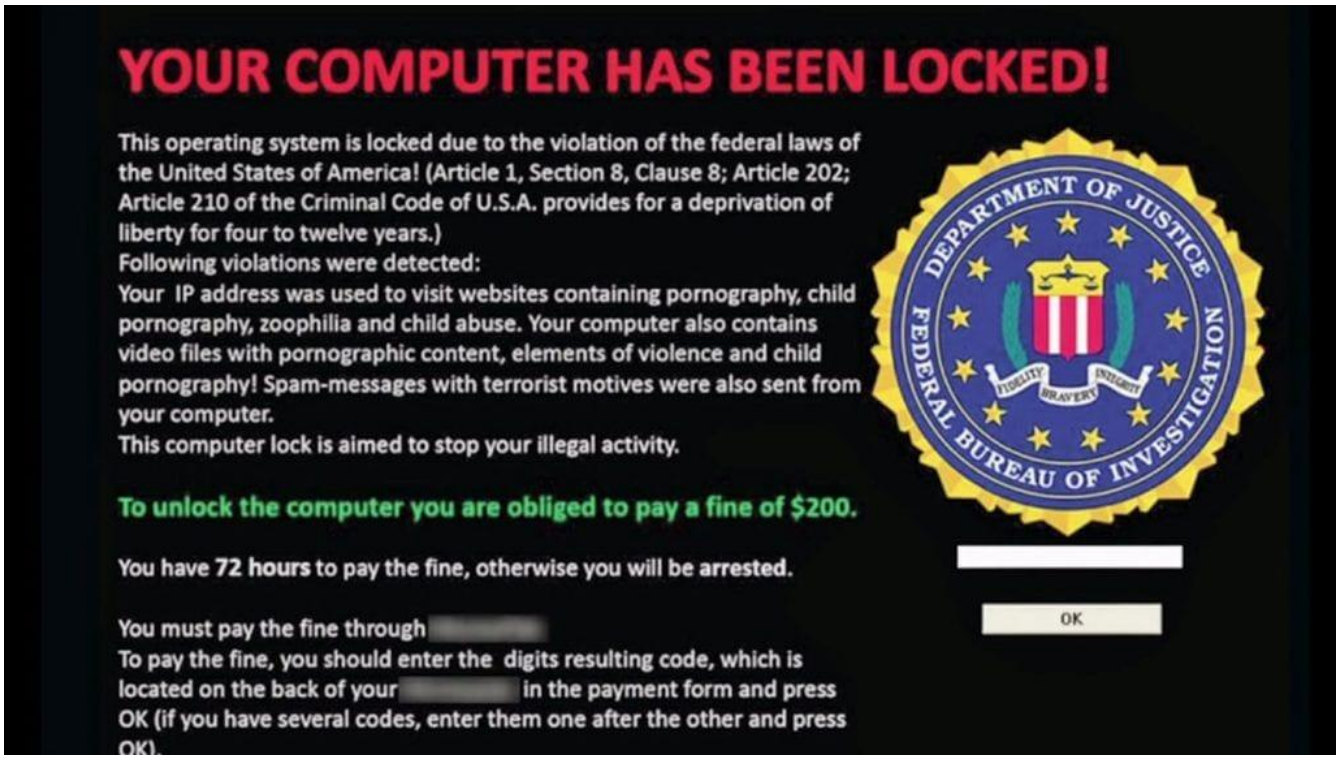
Some countries are starting to ban specific IoT devices with security problems. For example, the interactive IoT doll with a Bluetooth pin, which gave access to the toy's microphone and speaker to

anyone within the 25-30 meter radius. The doll was labeled as an **espionage device** and was banned in Germany.

# 7) Highjacking Your IoT Devices.

Ransomware has been named as one of the nastiest malware types ever existed. Ransomware does not destroy your sensitive files — it blocks access to them by way of encryption. Then, the hacker who infected the device will demand a ransom fee for the decryption key unlocking the files.

Here is how a ransomware notice looks like:




Ransomware is evolving, and IoT devices with poor security can become targets as well.

Just before the Trump inauguration speech, about 70% of the Washington DC surveillance cameras were infected with ransomware, leaving the police without the ability to record for several days.

The cases of IoT devices being infected with ransomware are rare, but the concept is quickly becoming a trend in the black hat hacker world. Still, wearables, healthcare gadgets, smart homes, and other smart devices and ecosystems might be at risk in the future.

Here, the are good news, and there are bad news. While this malware might not have valuable data to lock down because most IoT information is stored in the cloud, it canock down the entire device's functionality. Imagine that your vehicle will not start unless you pay a ransom fee — or your house is locked down, with the thermostat set to the maximum.

# 8) Data Integrity Risks OfIoT Security In Healthcare

With IoT, data is always on the move. It is being transmitted, stored, and processed. Most IoT devices extract and collect information from the external environment. It can

be a smart thermostat, HVAC, TVs, medical devices. But sometimes these devices send the collected data to the cloud without any encryption.

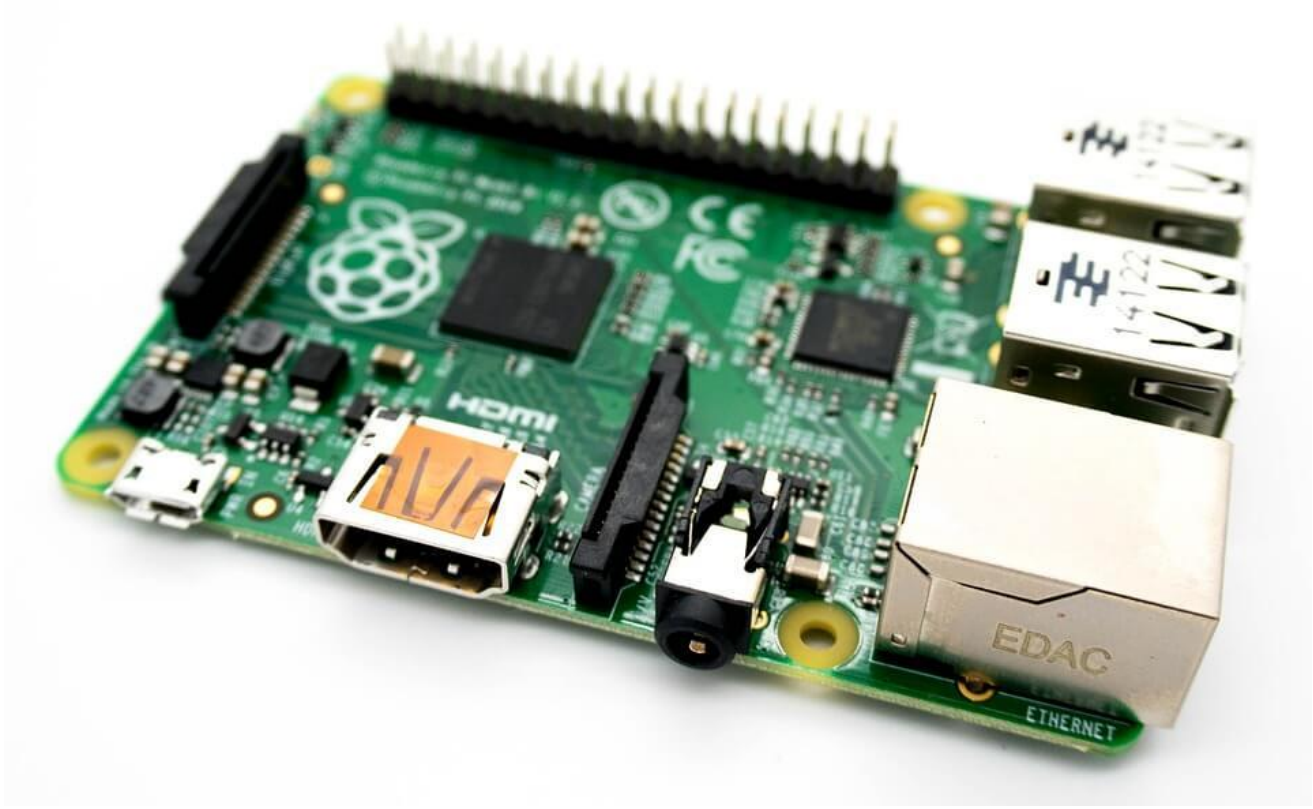
As a result, a hacker can gain access to a medical IoT device, gaining control over it and being able to alter the data it collects. A controlled medical IoT device can be used to send false signals, which in turn can make health practitioners take actions that may damage the health of their patients.

For example, a hacked medical IoT device can report a fully charged battery to the maintenance station while in reality the battery is about to die. Worse, there are risks of IoT security in healthcare devices like pacemakers or the ones making the insulin shots. The vulnerabilities found on St. Jude Medical's implantable cardiac gave access to hackers, enabling them to alter the pacing or shocks, or even worse, deplete the battery.

# 9) Rogue IoT Devices

We might already know about the rapid growth of the number of IoT devices, which is predicted to reach 18 billion by 2022, according to Ericsson. The problem with this number of devices arises not only in the BYOD (Bring-Your-On-Devices) approach in enterprises, but also in home networks. One of the most significant IoT security risks and challenges is being able to manage all our devices and close the perimeter.

**But rogue devices or counterfeit malicious IoT devices are beginning to be installed in secured networks without authorization.** A rogue device replaces an original one or integrates as a member of a group to collect or alter sensitive information. These devices break the network perimeter.




*Raspberry Pi board*

Example of rouge IoT devices can take the form of the Raspberry Pi, or WiFi Pineapple. These can be turned into a rogue AP (Access Point), thermostat, video camera, or MITM (Man in the Middle) and intercept incoming data communications unbeknownst to users. Other variations of rogue devices may also emerge in the future.

Interestingly, the upcoming horror movie “Child’s Play” was inspired by the concept and can serve as a curious example. In the movie, controlling other devices in a smart home system, Chucky is a rouge IoT device that has become a high-level threat to people’s lives.

# 10) CryptominingWithIoT Bots.

Mining cryptocurrency demands colossal CPU and GPU resources, and another IoT security issue has emerged due to this precondition — cryptomining with IoT bots. This type of attack involves infected botnets aimed at IoT devices, with the goal not to create damage, but mine cryptocurrency.

The open-source cryptocurrency Monero is one of the first ones to be mined using infected IoT devices, such as video cameras. Although a video camera does not have powerful resources to mine cryptocurrency, an army of them does.

IoT botnet miners pose a great threat to the crypto market, as the have the potential to flood and disrupt the entire market in a single attack.

# Summary

After the Mirai attack, people realized that any device connected to the Internet is a potential ally for an army of bots. But that was only the beginning.

For now, IoT and security are still not found in the same place. There are still many risks and security challenges of IoT now — and more will inevitably emerge in the coming years.

The more variations of IoT devices we see out there, the more complex IoT security problems will become. International organizations and governments will need to create universal IoT standards to control the security in cities, homes, locations like nuclear plants, the manufacturing process, and other areas and locations.

We have seen the emergence of IoT as a trend in the last few years. There are smart devices coming out that we never thought needed an Internet connection: smart toothbrushes, beauty mirrors, tables, pillows, beds, and the list continues to grow. The world is turning into a network of objects collecting our personal, sensitive information.

We can only imagine the amount of important data hackers could steal from those IoT devices if they do not have proper security. So, the top IoT security threats listed above are just the beginning. If we want our devices smart, we need them to be secure as well.