



IOT operating systems and it's security

Presented by: Omer Aiman

Contents

- Introduction to IOT
- Introduction about IOT devices
- Introduction about IOT OS's
- Uses of IOT
- Security problems
- Solutions

Internet of Things(IOT)

- The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.
- The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention.



IoT Parts:

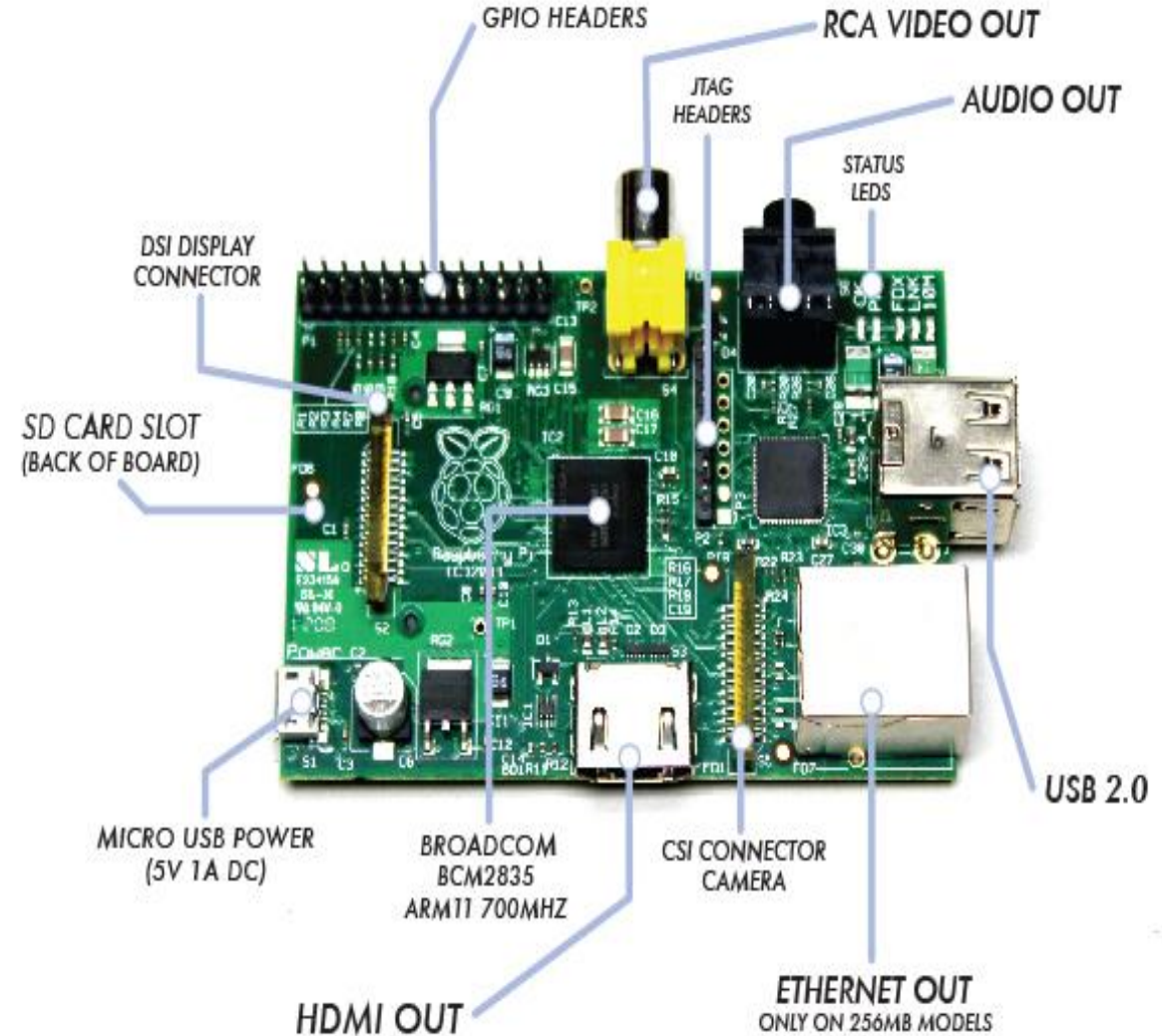
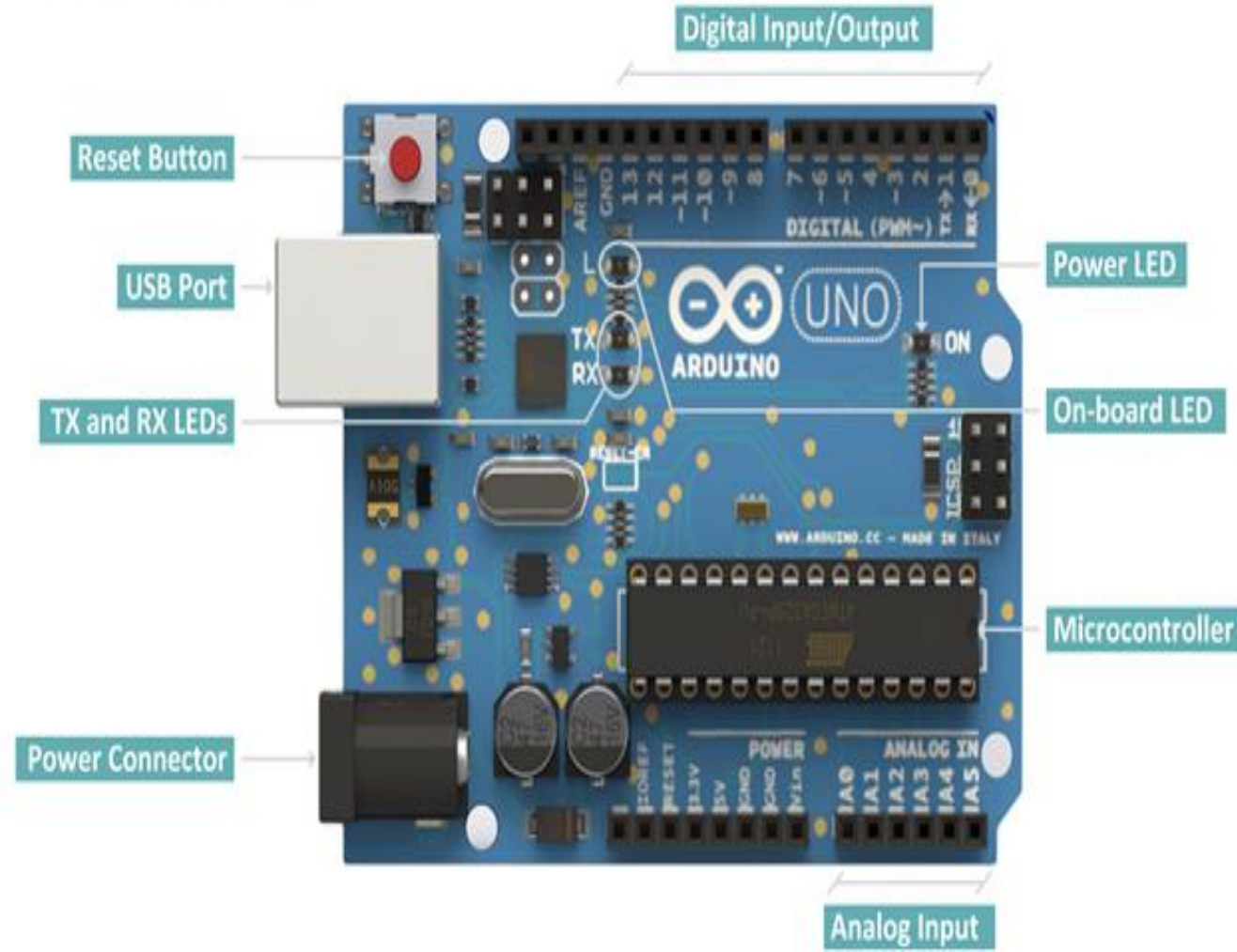
- Hardware or physical devices
- Operating system
- Applications
- Internet or Network connection

IoT Devices

There are many products developed for IoT usage, and the most famous and used are:

- Arduino boards that contains microcontroller in it, for smaller application.
- Raspberrypi and Intel Products like Edison and Joule. these devices contains Microprocessor and Rams with higher capabilities, for the processors starts from 1 GHz and above, and with Ram starts from 512Mb and above, With GPU and Ethernet or wifi adapters.

Boards:



IoT Operating systems

Most operating system used are Linux distribution, with a lot of platforms built from many companies for easy deployment. Also Windows are used and mac. IoT devices are capable for holding operating system and development. Also we have the capability to develop on another machine or inside similar virtual machine to test application before upload it on a real device. But also there is mini version from many operating system that compatible with these small devices.



And these are some operating systems for IoT devices:


- Ubuntu core, smaller version of Ubuntu, compatible with raspberrypi2 &3, Intel Joule & NUC, DragonBoard 410c, and Samsung Artik 5 & 10.
- Windows IoT core, compatible with raspberrypi2 &3, Intel Joule, DragonBoard 410c, and Minnowboard max.
- And there is no MAC for IoT, so for MAC users they can install IoT platforms and start developing!

- Brillo -- In the year since Google released Brillo, the lightweight Android-based distro has seen growing adoption among hacker boards such as the Intel Edison and Dragonboard 410c, and even some computer-on-modules. The future of Brillo is tied to Google's Weave communications protocol, which it requires. Weave brings discovery, provisioning, and authentication functions to Brillo, which can run on as little as 32MB RAM and 128MB flash.
- Raspbian -- There are some other distributions for the Raspberry Pi that are more specifically aimed at IoT, but the quickly maturing Raspbian is still the best. Because it's the most popular distro for DIY projects on one of the most widely used IoT platforms, developers can call upon numerous projects and tutorials for help. Now that Raspbian supports Node-RED, the visual design tool for Node-JS, we see less reason to opt for the RPi-specific, IoT-focused Thingbox.
- ARM Mbed -- ARM's IoT-oriented OS targets tiny, battery-powered IoT endpoints running on Cortex-M MCUs with as little as 8KB of RAM, and has appeared on the BBC Micro:bit SBC. Although originally semi-proprietary, single threaded only, and lacking deterministic features, it's now open sourced under Apache 2.0, and provides multithreading and RTOS support.

IoT Developing platforms

Most of Boards producers are offering development environment that work in different machines and systems. But Big companies got involved in the process and started to produce environment too.

Also, This happened because there are different developers types, some prefer C++, Python, C#, PHP, or Java.



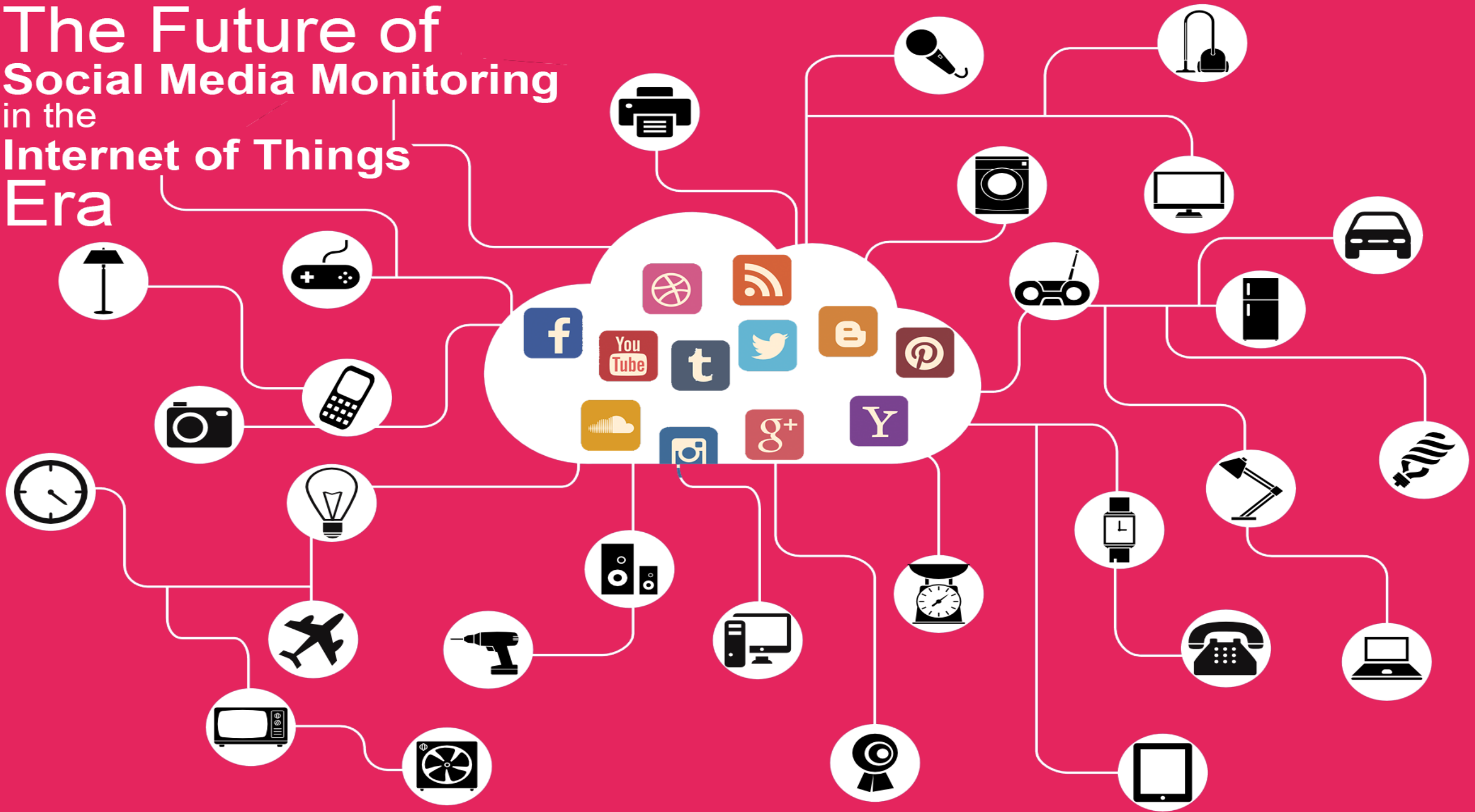
For this reason there are many platforms like:

- Eclipse IoT (Kura) -- The Eclipse Foundation's IoT efforts are built around its Java/OSGi-based Kura API container and aggregation platform for M2M applications running on service gateways.
- Kaa -- The CyberVision-backed Kaa project offers a scalable, end-to-end IoT framework designed for large cloud-connected IoT networks. The platform includes a REST-enabled server function for services, analytics, and data management, typically deployed as a cluster of nodes coordinated by Apache Zookeeper. Kaa's endpoint SDKs, which support Java, C++ and C development, handle client-server communications, authentication, encryption, persistence, and data marshalling.

IoT Applications

- Media
- Environmental monitoring
- Infrastructure management
- Manufacturing
- Energy management
- Medical and healthcare
- Building and home automation
- Transportation
- Metropolitan scale deployments
- Consumer application

The Future of Social Media Monitoring in the Internet of Things Era





IoT Infrastructure





Internet of Things in Manufacturing



MANUFACTURING PLANT

Monitor production flow in near-real time to eliminate waste and unnecessary work in process inventory.

Manage equipment remotely, using temperature limits and other settings to conserve energy and reduce costs.

Implement condition-based maintenance alerts to eliminate machine down-time and increase throughput.

Aggregate product data, customer sentiment, and other third-party syndicated data to identify and correct quality issues.

GLOBAL FACILITY INSIGHT



CUSTOMER SITE

Transmits operational information to the partner (e.g. OEM) and to field service engineers for remote process automation and optimization.



Provide cross-channel visibility into inventories to optimize supply and reduce shared costs in the value chain.



GLOBAL OPERATIONS

Management



I can see my production line status and recommend adjustments to better manage operational cost.

R&D



I gain insight into usage patterns from multiple customers and track equipment deterioration, enabling me to reengineer products for better performance.

Field Service



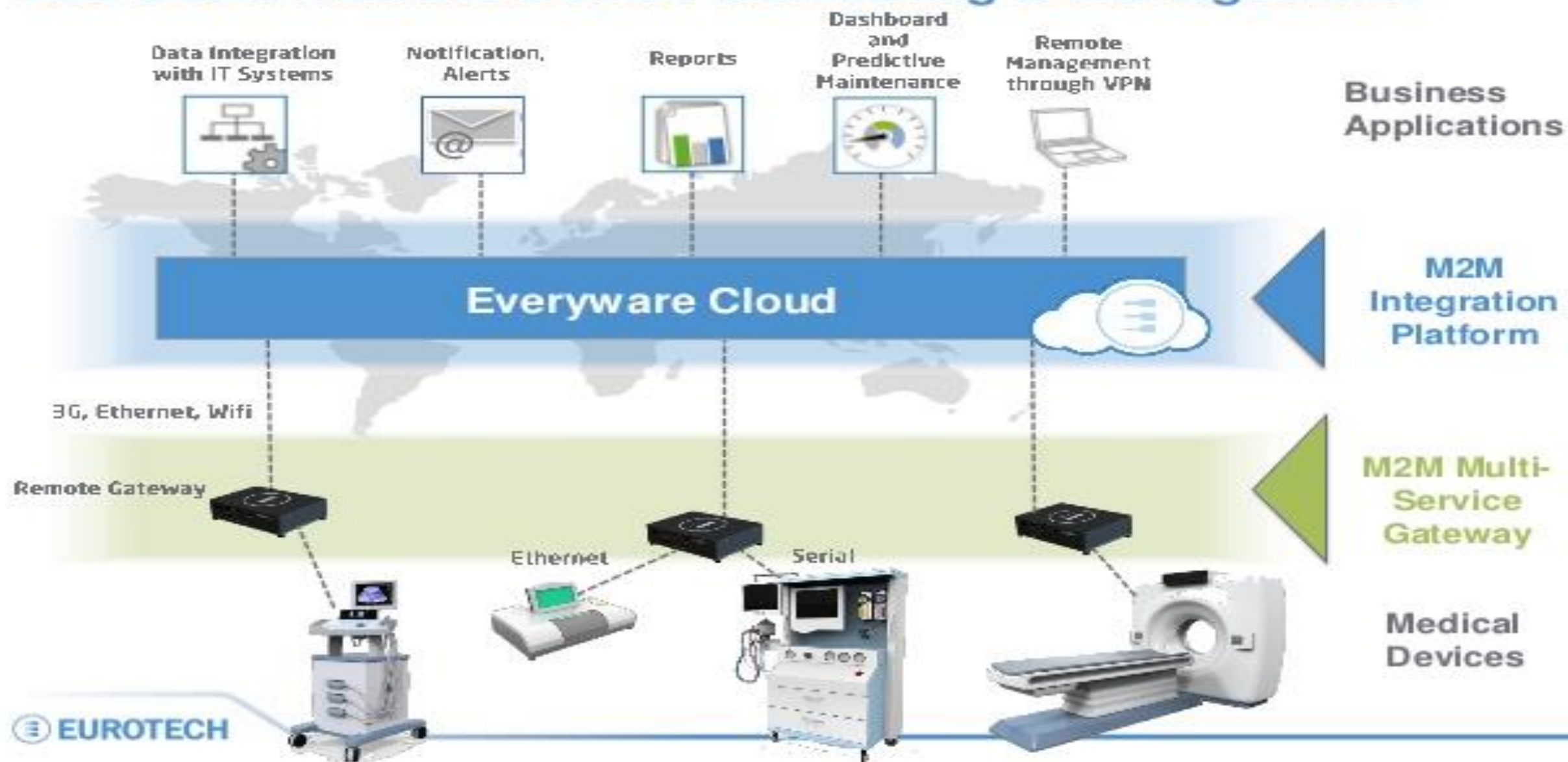
I know when to deploy the right resources for predictive maintenance to minimize equipment failures and reduce service cost.



THIRD-PARTY LOGISTICS

Medical & Healthcare IoT Applications

Use Case: Remote Device Monitoring & Management



Risk & Security of using IoT

From previous slides, We showed some important uses of IoT, and as it is important we should secure it. The risk here is coming from using internet and networking, and any gap in software development could lead to big hacking risk. Hackers who attack all these systems—home, car, and health—are typically trying to do one of three things: take control of the apparatus, steal information, or disrupt service. and there is many examples happened in previous years, like hacking Iran nuclear Power Plant. From this issues many companies offered some solutions to avoid this risks, some offered software platform and debugging, others depend on hardware components and physical communication.

CISCO proposed:

To address the highly diverse IoT environment and the related security challenges, a flexible security framework is required. The next Figure illustrates the security environment from an IoT perspective.

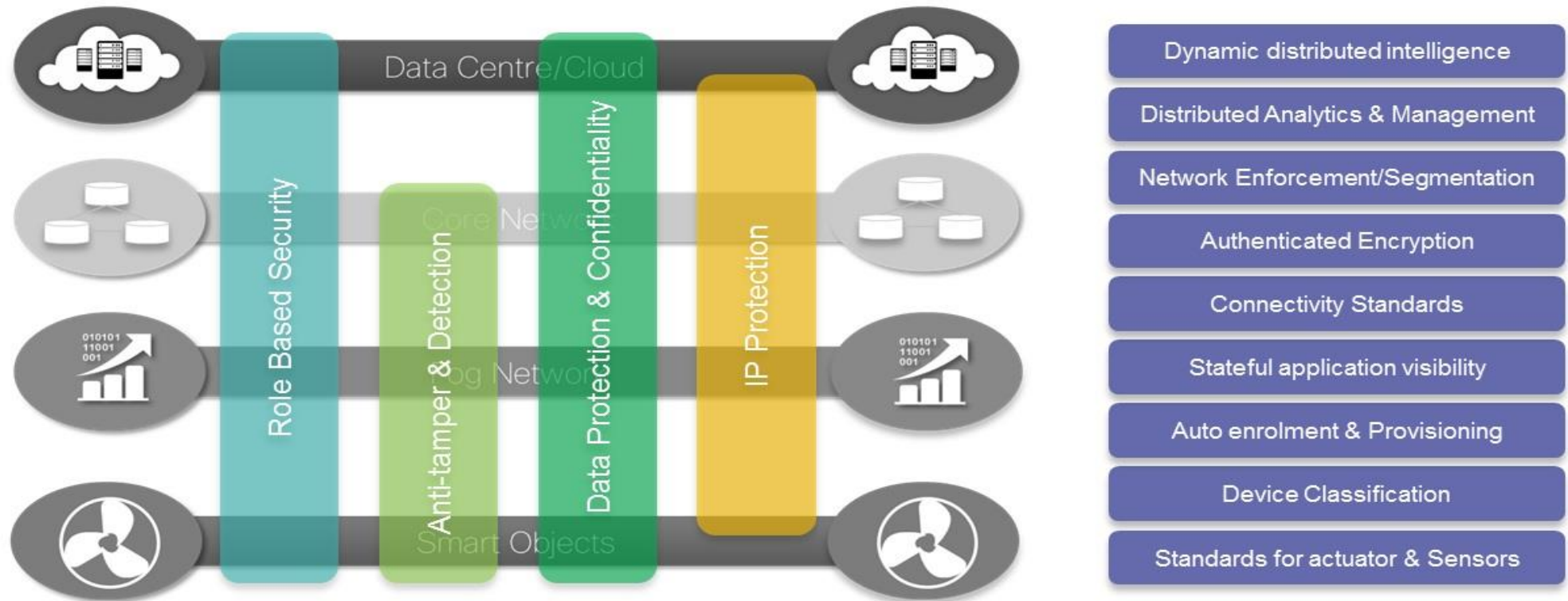
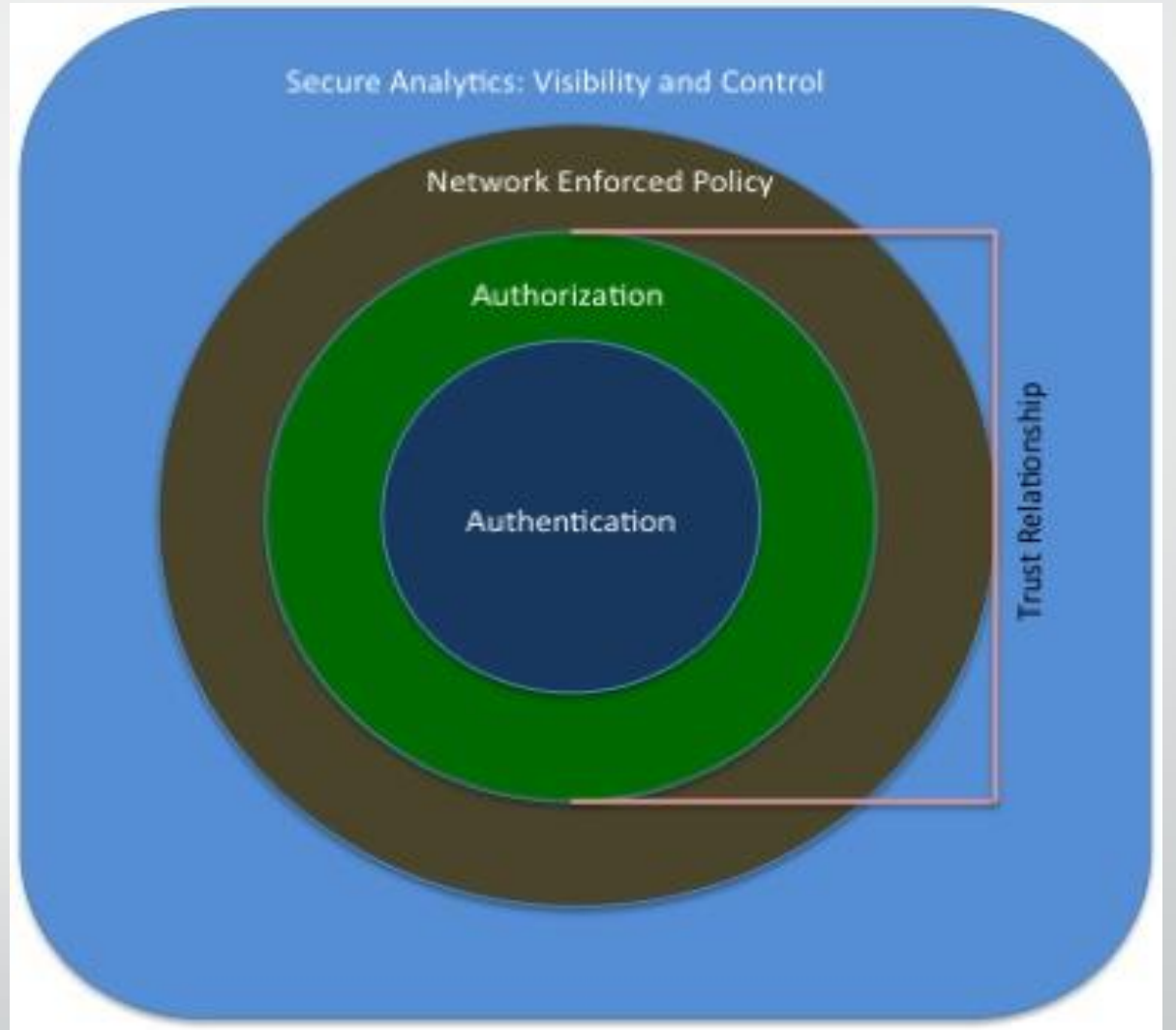
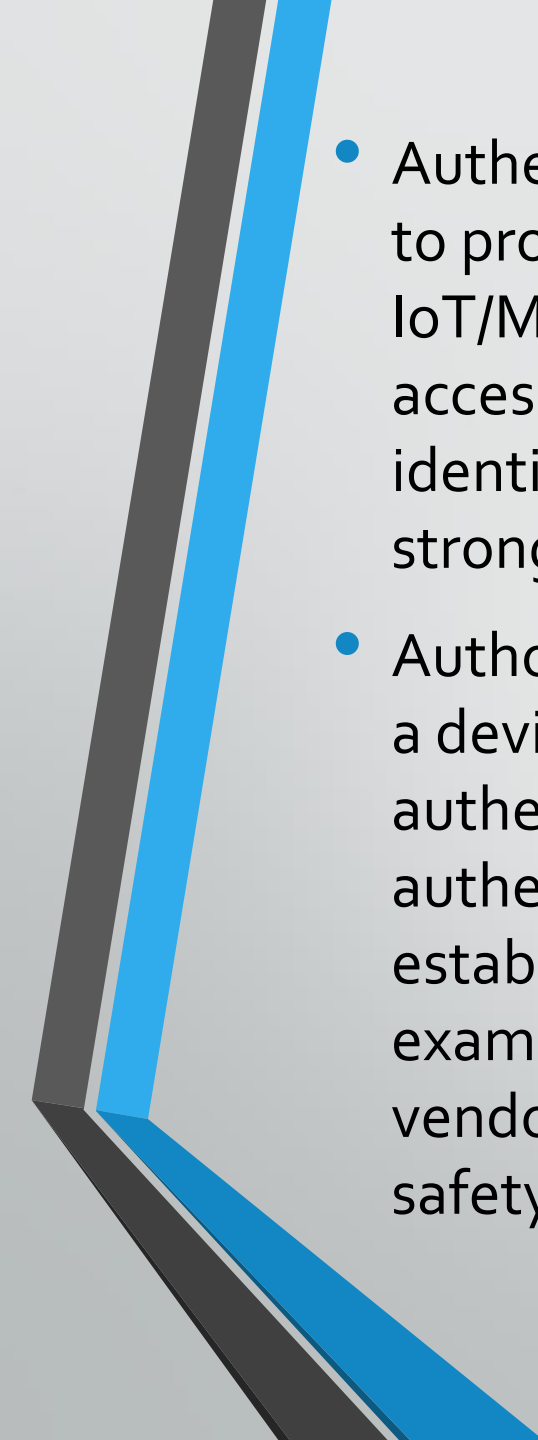



Figure shows a framework to secure the IoT environment and is comprised of four components:

- Authentication
- Authorization
- Network Enforced Policy
- Secure Analytics: Visibility and Control



- 
- **Authentication:** At the heart of this framework is the authentication layer, used to provide and verify the identify information of an IoT entity. When connected IoT/M2M devices (e.g., embedded sensors and actuators or endpoints) need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device. Establishing identity through X.509 certificates provides a strong authentication system.
 - **Authorization:** The second layer of this framework is authorization that controls a device's access throughout the network fabric. This layer builds upon the core authentication layer by leveraging the identity information of an entity. With authentication and authorization components, a trust relationship is established between IoT devices to exchange appropriate information. For example, a car may establish a trust alliance with another car from the same vendor. That trust relationship, however, may only allow cars to exchange their safety capabilities.

- 
- Network Enforced Policy: This layer encompasses all elements that route and transport endpoint traffic securely over the infrastructure, whether control, management or actual data traffic. Like the Authorization layer, there are already established protocols and mechanisms to secure the network infrastructure and affect policy that are well suited to the IoT/M2M use cases.
 - Network Enforced Policy: This layer encompasses all elements that route and transport endpoint traffic securely over the infrastructure, whether control, management or actual data traffic. Like the Authorization layer, there are already established protocols and mechanisms to secure the network infrastructure and affect policy that are well suited to the IoT/M2M use cases.

Resources:

- <https://www.linux.com/news/linux-and-open-source-hardware-iot>
- <https://www.linux.com/NEWS/21-OPEN-SOURCE-PROJECTS-IOT>
- <https://developer.microsoft.com/en-us/windows/iot/Docs/Whatsnew>
- <https://snapcraft.io/docs/build-snaps/publish>
- <http://platformio.org/get-started/ide?install>
- <https://www.linux.com/news/open-source-operating-systems-iot>
- https://en.wikipedia.org/wiki/Internet_of_things
- <http://www.zettajs.org/>
- <http://spectrum.ieee.org/telecom/security/how-to-build-a-safer-internet-of-things>
- <http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html#9>