IOT SENSORS AND SECURITY

2016 MEGATRIS COMP. VIEW

INTRODUCTION

Instant connectivity has completely changed much of society. Now a new revolution is upon us: **The Internet of Things (IoT).**

The depth and breadth of IoT connectivity will create new businesses, provide new markets for existing businesses, and improve operational efficiencies. Gartner predicts that the number of IoT devices will grow **to 26 billion units by 2020 in the US.**

IoT and machine-to-machine (M2M) communications increase operational efficiency by giving businesses visibility into the details of their operations in ways that could not have been measured before.

In **Cisco's "Internet of Everything" 2013 report,** the highest percentage (27%) of value in future IoT revenue will be in manufacturing.

Accenture's 2014 report, "Driving Unconventional Growth Through the Industrial Internet of Things," finds that manufacturers **could boost their efficiency by 30% using IoT**.

Here we introduce our 2016 view about IoT sensors and security.

WHAT WE WILL TALK ABOUT

IoT sensors and security.

IoT/M2M Sensors

Sensors are the specific mechanism used to measure physical parameters.

Conversion to Digital Data

Conversions can create error, calibration and specialized sensors are fundamental.

Security Objectives

In the context of IoT/M2M, privacy is concerned with ensuring that data access is limited to the appropriate and authorized parties only.

Security Issues for IoT/M2M

There is no single security solution for all possible security requirements for all applications.

IOT/M2MSENSORS

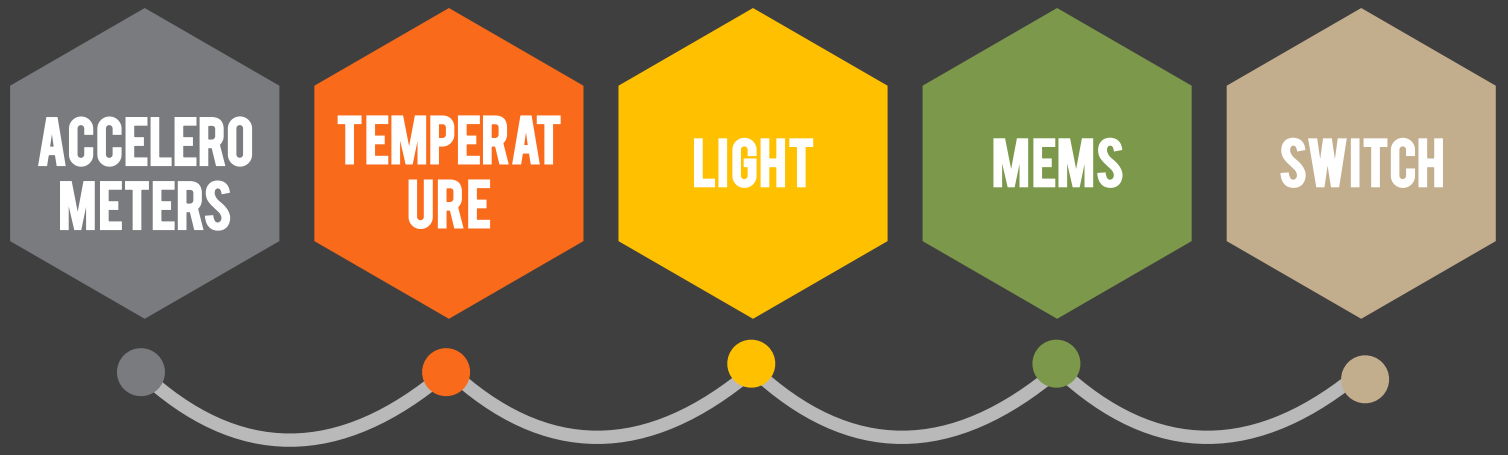
- When deploying Internet of Things and machine-to-machine application devices, the connected device generally needs to report more than just its physical location. **We will talk about a few of the more common sensors and what they do.**

- For example, an IoT/M2M device may measure a particular **physical parameter** at that location these physical parameter measurements require sensors that are capable of recording the specific value of that parameter for the device application to fulfill its functions.

- Sensors are often integrated circuits that are designed for these kinds of **IoT/M2M applications**, since the small size and low cost of these chips make them appropriate choices.

- For example, many of the sensors described in this webinar are available in high-end smartphones. These include accelerometers, thermometers, gyroscopes, magnetometers, and heart-rate monitors.

SENSORS TYPES



ACCELEROMETERS SENSORS

Acceleration is a measure of a change in velocity (**change of speed or direction**). Accelerometers are devices that measure acceleration.

The parameter being measured may be a static force, such as gravity exerted on a device. Other sensors make dynamic force measurements to measure motion changes and vibration.

- ✓ An example of an acceleration sensor is a chip in a moving vehicle that measures changes of speed and uses high acceleration readings (such as during an accident) to **trigger an airbag to protect the passengers**.

- ✓ In some industrial applications, the **vibrations detected** by an acceleration sensor could be an excellent indicator of a potential problem with a moving part—such as a motor with bearings that are worn. Timely transmission of the data from vibration sensors enables early detection of problems where preventative maintenance **could avoid catastrophic failures**.

TEMPERATURE SENSORS

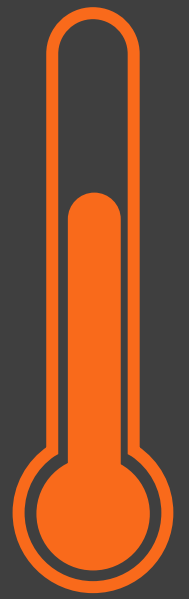
Depending on the desired measurement range, there are various types of available sensors:

- **Silicon chip** (semiconductor) sensors are easily used in the range from -50 to +150 degrees Celsius. These are quite accurate and linear—to within 1 degree—without the need for extensive calibration. They are relatively inexpensive.

- **Thermistor** sensors can cover a wider range—from -100 to +450 degrees C for more applications.
  A thermistor is often more accurate than a silicon chip, but it has a slightly higher cost per sensor. It requires a complex correction to achieve good linearity and accuracy over the desired temperature range.

- **Resistance-Temperature Detectors (RTD)** provide yet more range, from -250 to +900 C, but are quite difficult to use since they are more fragile than other types of temperature sensors. They are the most accurate—often a hundred times more accurate than a silicon chip sensor, although this carries the same complex solutions for linearization as thermistors, and some models can be quite expensive.

- **Thermocouple** is the correct choice for high range from -250 to +2000 C. It is used for many industrial applications, such as chemical process monitors and high-temperature furnaces used in the semiconductor industry.



The response time for the sensor data can be quite slow, since temperature changes are not as "rapid" as other measured physical parameters.

LIGHT SENSORS

Light sensors cover a broad range of potential applications—from **automated brightness control in cellphones to medical diagnostic equipment.**

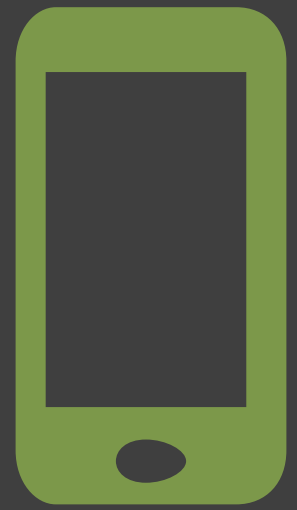
- ✓ A very early example of ambient light sensors used in local consumer applications are **photocells** within lamps that automatically turn the lamps on at dusk and turn them off at sunrise.
- ✓ Simple light sensors can also be for **proximity detection.** Counters in manufacturing systems use the presence or absence of light on photocells to measure products being moved past the counter on conveyors.
- ✓ Garage door systems can reverse direction **to avoid hurting children** or pets who cross under a closing garage door and temporarily cut the light from a source sending a beam of light across the door opening onto a photocell.

As with other types of sensors, the mechanism used to measure ambient light varies depending on the application. Simple Cadmium Sulphide (CdS) or Cadmium Selenide (CdSe) photo-resistors **change their resistance as a function of the ambient light.**

Photo-diodes and photo-transistors, with active semiconductor junctions, are used when greater accuracy is required, since the ambient light is converted into a measurable current that can be amplified or converted for a measurement

MEMS SENSORS

In 2015, half of all wearable sensors are based on MEMS technologies. Inertial measurement units (**IMUs**) are found in every smart watch and fitness tracker, making the most of mature MEMS components that are **reliable, familiar and cheap.**



In modern, high-end smartphones, integrated chip sensors to measure motion, direction, pressure, magnetic fields, etc., are becoming quite common. These can be used to **augment the location information and human motion in the cellphone.**

In chip form, these are usually Micro-Electro-Mechanical Systems (**MEMS**) sensors for many different parameter measurements. The implementation of MEMS **uses ultra-miniaturized physical structures**—beams, arms, and associated electronics—to measure the motion of the structures when the chips moved. The device essentially converts a mechanical (physical) motion into an electrical signal.

A gyro sensor, for example, senses rotational motion and changes in orientation. These can be used in a variety of applications, such as correcting for **hand-held shake in video** and still-image cameras and human motion sensing for video games.

MEMS sensors are generally manufactured in the same large-scale facilities as semiconductors or chips. This means that the mechanical precision of the devices can be very high and allow for **excellent, reliable performance at low cost**.

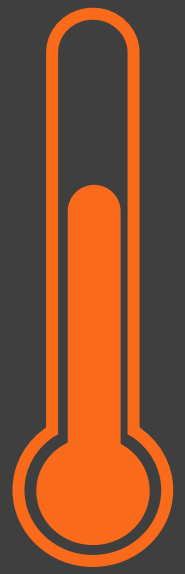
SWITCH

Switches are the simple state or position sensors that provide an “open” or “closed” state. A door or window sensor used in **security systems** is often a simple magnetic reed relay switch that opens or closes an electrical circuit depending on the position of a small magnet relative to the switch.

These simple magnetic reed relay switches can also be used for sensing when a cabinet—such as a medicine cabinet, oven door, or food storage compartment—has been opened in a **senior citizen’s home-monitoring IoT application**. A detection of the change of state of such a switch—from open or closed or vice-versa—can be interpreted as evidence that the monitored parent has performed their expected regular daily routine.

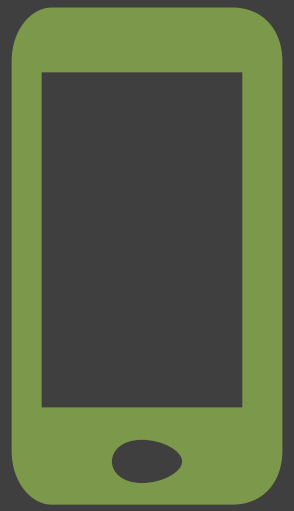
OUR ON FIELD APPLICATIONS

Our company has developed a lot of solutions using the sensors described before:



Monitor performance of solar panels using temperature thresholds.

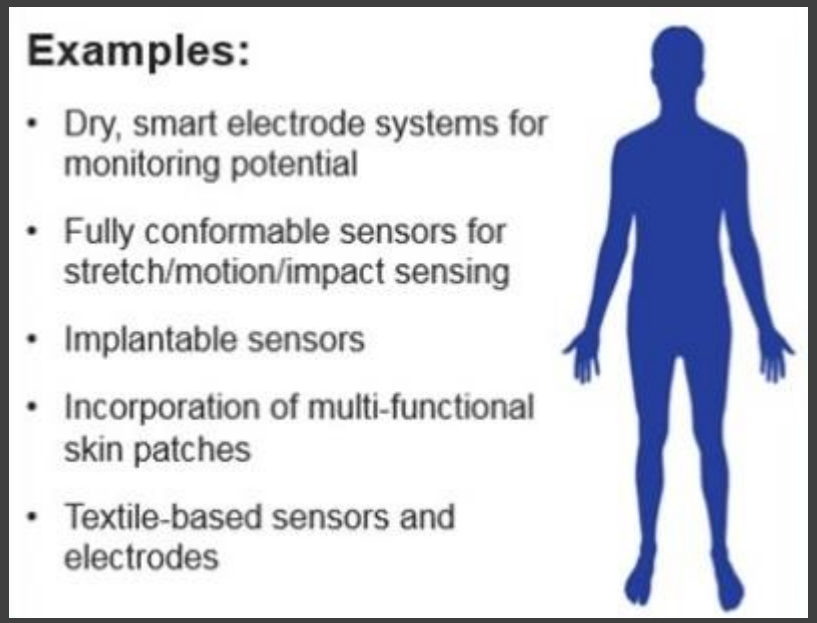
Measure the daily light in order to monitor the output of a solar plant.



Use MEMS sensors of a smartphone to monitor the fitness activity of the user.

Use a switch (Denkovi Relay) to turn off a power inverter in case of alert.

WHAT WE LIKE TO DO: SENSOR FUSION



Our daily challenge here is in turning raw data into useful, or 'actionable' data. **Sensor fusion** is the process of combining sensor outputs from multiple sensors to gain greater total insight.

The most common example is using individual xyz acceleration and rotation data (e.g. from a 6-axis IMU) into motion data. **This in turn can be used to count steps, differentiate between activity types, and so on.** Another example with MEMS IMUs is to use them alongside optical sensors to manage motion artifacts experienced in optical heart rate monitoring.

SENSOR FUTURE: CONVENTIONAL VS PRINTED ELECTRONICS

	Conventional Electronics	"Printed Electronics"
Materials	High temperature: Silicon, Ceramics, Glass	Low Temperature: Organic polymers, Specialty inks
	⬇	⬇
Manufacturing technique	Photolithography, micromachining, ablation, etc.	Printed on plastic, textile, paper, foil
	⬇	⬇
Product feature	Rigid, brittle, miniaturized 	Flexible, robust, large area 

SENSOR THAT CAN BE FULLY PRINTED

- ✓ Biosensors
- ✓ Capacitive sensors
- ✓ Piezoresistive sensors
- ✓ Piezoelectric sensors
- ✓ Photodetectors
- ✓ Temperature sensors
- ✓ Humidity sensors
- ✓ Gas sensors

CONVERSION TO DIGITAL DATA

Analog-to-digital conversion is an electronic process in which a continuously variable (analog) signal is changed, without altering its essential content, into a multi-level (digital) signal.

Sensors are often used in local applications, where their signal is processed using circuitry designed for that local application. However, in a sensor that is used for remote data transmission of the measurement, the **electrical signal must be converted into a digital value**, or number, for the transmission.

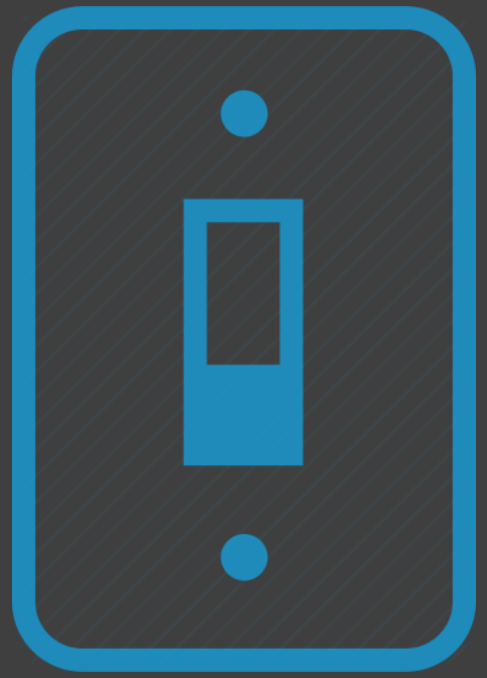
The specific electrical signal from different sensors may vary over **a wide range of current or voltage** or other electrical parameters (such as resistance or capacitance) and often must be converted and **amplified into a voltage that can be measured.**
If necessary, the signal must be filtered to eliminate noise or to reduce the frequency of the measurement for the requirements of the application.

For example, a temperature sensor generally changes its value relatively slowly as the sensor matches its environment. Therefore, a rapid change in reported temperature may be an inaccurate reading, which should be filtered to reduce potential errors.

SIMPLE OFF AND ON SWITCHES

In simple switch applications, where the state is “open” or “closed,” using a digital pin to measure this state and report its value (“0” or “1”) is an easy choice.

For more complex needs with simple switches, the device may also report **when the transition from one state (such as “open”) to the other state** (such as “closed”) occurs. That is, it may be equally, or more, important to report a change of state rather than the present state of the simple switch.



SECURITY OBJECTIVES

- Traditional financial and consumer markets have been targets for misuse of information stored on their systems—including personal **credit information**, identify theft, misuse of credit cards by unauthorized persons, **personal privacy violations**, and loss of corporate intellectual property.
  The **financial losses** sustained by these security breaches are in the **billions of dollars**.

- While attempts have been made to criminalize such nefarious activities, they continue to occur with increasing frequency and are a serious problem for governments, businesses, and individuals.

- Business deploying IoT/M2M solutions will be held responsible for protecting data and devices, as well as corporate proprietary information.

“any device that is connected to the Internet is at risk of being hijacked.”

Chairperson Edith Ramirez - US Federal Trade Commission

SECURITY OBJECTIVES

Trust in the Data Content

Authenticated Sender and Receiver

Confidentiality of Information

Sender and Receiver Accessible

SENDER AND RECEIVER ACCESSIBLE

In any data connection, it is important for the sender and receiver of information to be authenticated to each other—regardless of whether the device is the sender or the receiver.

- ✓ As a security principle when transmitting data, the device must ensure that it is sending its information to the correct server, and when receiving data and control messages, **it must ensure that the information is coming from the correct server.**

AUTHENTICATED SENDER AND RECEIVER

In any network, the sender and receiver must always be accessible when needed. If the network is not functional, or the server is not executing the correct programs to receive the data, the purpose of the application may be lost. Mission-critical applications, such as automatic crash notification or medical alerts, may fail to work properly if the connection is not reliable. **The lack of communication itself means a lack of security.**

CONFIDENTIALITY OF INFORMATION

The confidentiality of the information must be maintained. **Only the correct recipient should have access to the transmitted data**, since it may contain proprietary or confidential information. Indeed, privacy laws in many countries require extra care with information regarding individual citizens—for example, in the US, the Health Insurance Portability and Accountability Act (HIPAA) provides specific rules for individually identifiable medical information.

TRUST IN THE DATA CONTENT

The accuracy in the content of the transmitted data is essential—if a device does not encode and transmit data correctly, or the connection is not error-free, the quality and accuracy of the data becomes suspect. Even good data becomes unreliable, and business actions that are taken on the content of the data may not be appropriate.

Mission-critical information is particularly important to keep as error-free as possible. The cost of business actions taken on receipt of incorrect data may be high.

SECURITY ISSUES FOR IOT/M2M

Security risks can be recognized and understood, and the implementation of security methods should be incorporated in the IoT/M2M device and software associated with that application.

Most obvious holes in security can be resolved quickly and efficiently. It is vital to recognize that risks cannot be completely eliminated, and there is no single security solution for all possible security requirements for all applications.

Thus, it is critical to assess the level of security implementations that are appropriate for different kinds of data.

This assessment must be done early—during the design of the application.

We believe that the most important security layer for the IoT are the cloud services, where there is the bigger value for the customer.
Security can't be 100% guaranteed on physical devices, but it can be on a centralized cloud system thanks to many tools like encryption, statistics and deep learning algorithms.

ISSUES TO BE CONSIDERED

Multiple Networks

Some IoT/M2M devices operate in more than one transport network or technology for redundancy or hybrid solutions. For example, a short-range wireless technology such as Wi-Fi can have quite a different security threat vector and potential for breaches compared to a long-range cellular service.

Multiple Types of Services

Applications and devices may be using multiple services, where the required authorizations for allowing a device to access a particular service may differ from one application to another. The authentication mechanisms may also differ.

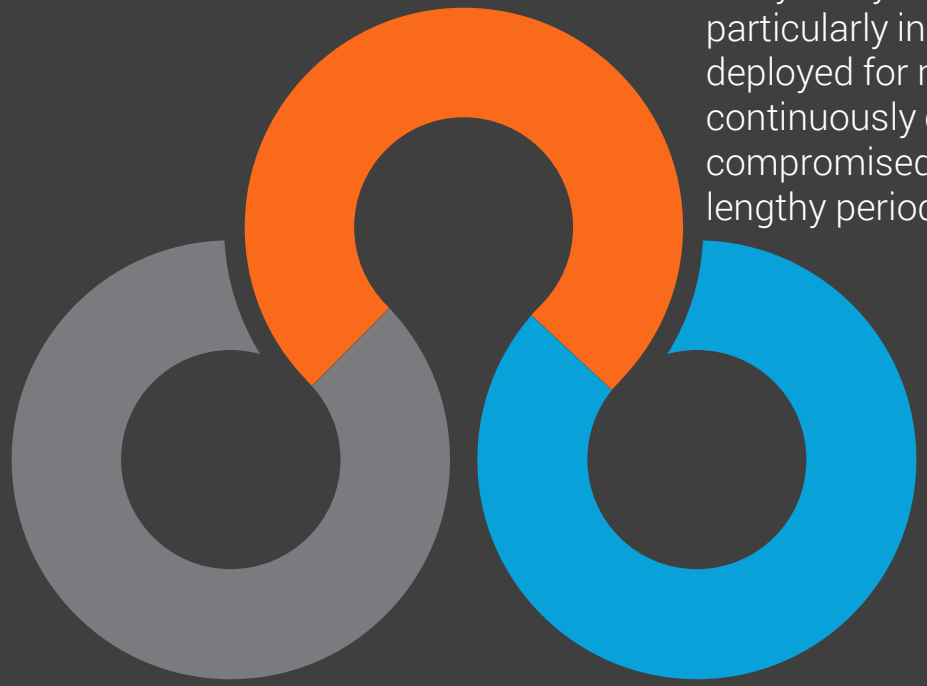
Scaling Growth

In IoT/M2M deployments, there are predictions of explosive growth in the near future—billions of potential devices within the next 5 to 10 years. Thus, in any application where a security problem exists, the overall problem could be greatly magnified by the large numbers of devices that may be affected.

ISSUES TO BE CONSIDERED

Automated Functionality

Automated programs process the received data and take business actions based on the content.
If the transmitted data is compromised, any simplistic responses or automated functions to that compromised data could cascade into difficulty.



Long Lifecycles

Unlike handsets used by people who change them every few years on average, IoT/M2M devices—particularly in industrial applications—may be deployed for many years and operate relatively continuously over that time. Devices with compromised security could stay operational for lengthy periods.

Remote Updates

It is essential to plan and design for device updates over-the-air (OTA). When a device security breach is sufficiently critical that the device programming must be updated, the ability to re-program the functionality remotely is vital.

SECURITY BREACH CHECKLIST

Assess the potential for damage caused by a security breach, and implement security solutions accordingly. Here the checklist:

- ✓ If a single device is compromised, can it be used to compromise other devices?
- ✓ If an application is compromised and misused, what impact does that security event have? Is it life-threatening?
- ✓ Can a data content breach cause financial harm to an individual or more?
- ✓ How quickly can the specific breach or intrusion be detected? Is it using a well-known target mechanism (such as might exist in a widely used cellular device operating system)?
- ✓ Can a compromised device or set of devices be isolated from the application rapidly?

A compromised sensor could be used to inject false data into the application, where an incorrect action could be taken by a server or human at the remote end of the chain. A possible solution consists in the usage of statistical patterns.

ENCRYPTION AS AN IOT TOOL

A way to secure data is to encode it so that only the authorized recipient can decode the data.

The basic goals of encryption are to provide:

• Proof that the **sender is valid**— Proof of who sent data is crucial so that a hacker doesn't steal a session and then pretend to be that user (**spoofing**).

• Proof that **data was not altered**—Encryption functions can be used to ensure that a change to the data renders the content unusable.

• Proof that **data cannot be read by a third party**—Encryption protects data from being read in transit or upon receipt, except by someone with the correct decryption method.

A compromised sensor could be used to inject false data into the application, where an incorrect action could be taken by a server or human at the remote end of the chain.

WEAKNESSES IN ENCRYPTION

No encryption method is perfect—depending on the computing power available at a particular location or the time used by the encryption method, the algorithm may be weak or strong.

Strong algorithms may seem impossible to break, but applying enough computing resources to the task could reveal weaknesses that allow the data to be decrypted by unauthorized systems or people.

Bugs may be discovered in the method itself, or in the particular software implementation. A recent example is the Heartbleed security bug in OpenSSL discovered in 2014. This potentially allowed encrypted data to be read. Patches were made to OpenSSL, and a majority of web servers have since been updated.

The heartbleed security bug in openssl, discovered in 2014, affected about 17% of the world's web servers.

IOE SECURITY IS NOT AN HEADACHE

IoE security is not an headache for us, we strongly think that with efficient and robust cloud services it’s possible to guarantee an high level of security.

This is accomplished thanks to specific services that use:

- ✓ Machine Learning
- ✓ Statistical approaches
- ✓ Simulations
- ✓ Recommendations

Our companion monitors the user activities and sends recommendations about health, fitness but also if there are errors or risks.

QUESTIONS

QUESTION #1

What is the most important software layer for IoT security?

We believe that the most important security layers for the IoT are the cloud services, where there is the bigger value for the customer. Security can’t be 100% guaranteed on physical devices, but it can be on a centralized cloud system thanks to many tools like encryption, statistics and deep learning algorithms.

QUESTION #2

Can you give more details about your temperature sensor application?

We have used temperature sensors to monitor performance of solar panels using temperature thresholds. At first we had some issues because of the properties of thermistors: they were slow and the conversion from analogic to digital had a notable error. We decided to change the type of sensor and we used a silicon chip. It was faster and more precise. Moreover the conversion was automatically made by the chip because it has already a digital output.

QUESTION #3

What is the most common data analytics platform for IoT?

There are many platforms that can be used to analyze data. One of them is Hadoop, using Hadoop to analyze the data collected through machines and sensors connected to the IoT enables organizations to experience benefits in a variety of areas. Weather patterns and other natural phenomena can be monitored and tracked with a Hadoop system, for example. Additionally, predictive analysis allows businesses to better anticipate when repairs will be needed for equipment and infrastructure. The health care industry has experienced multiple benefits from Hadoop too, specifically the ability to record and monitor patients' vital statistics and other health indicators.

QUESTION #4

What kind of sensor should I use to measure temp. of the soil and humidity?

One interesting way to measure soil data is using the SparkFun Soil Moisture Sensor with an Arduino board. Here there are more info: https://www.sparkfun.com/products/13322
There is another interesting Temperature sensor for soil: the SHT-10. It includes both humidity and temperature modules. Humidity readings have 4.5% precision and temperature 0.5%. It's used with Arduino or similar boards. Here more info: https://www.adafruit.com/products/1298
Tutorial: https://learn.adafruit.com/wireless-gardening-arduino-cc3000-wifi-modules

QUESTION #5

Is hadoop Platform popular among IoT?

Your ability to process IoT data at scale requires an integrated software, hardware, and networking approach that includes Hadoop in order to prevent project delays and increased costs. Pairing IoT with Hadoop allows organizations to take full advantage of everything the IoT has to offer. As more devices connect to the IoT, an increasing amount of data is created that can offer valuable insights into a number of areas. Hadoop platforms provide a powerful source of data analysis for the information gathered by the IoT. A Hadoop platform can accommodate 1 trillion files through the use of an enterprise-class storage processing layer, and data snapshots allow users to access device information from a specific timeframe after the fact.

Megatris Comp. LLC

We create cloud services and mobile apps to make people life easier. Our mobile apps are integrated with Megatris Cloud to sell services and goods.

www.megatris.com
1250 Oakmead Pkwy, Sunnyvale, CA 94085, USA