Analysis and study of data security in the Internet of Things paradigm from a Blockchain technology approach

Titulació: Màster Universitari en Enginyeria de Telecomunicació UOC-URL
Autor: David Rull Aixa
Consultor: Raúl Parada Medina
Responsable: Carlos Monzo Sánchez
Gener,2018

UOC
Universitat Oberta de Catalunya

UNIVERSITAT
RAMON
LLULL

Index

- Aims of the project
- IoT paradigm
- IoT Architectures (3-layer architecture)
- Vulnerabilities
- Blockchain technology
- IoT and Blockchain technology convergence
- Proposed Scenarios
- Conclusions

Aims of the project

- Analysis of the most important technologies of the IoT and the common scenarios and their vulnerabilities

- Study the IoT solutions to address security issues

- Study of security solutions that combine the Blockchain technology with IoT

- Collect all the key information and articles related to IoT and Blockchain

- Analysis of the opportunities that Blockchain technology can bring to IoT paradigm and propose some innovative scenarios with their convergence

IoT paradigm

IoT key concepts

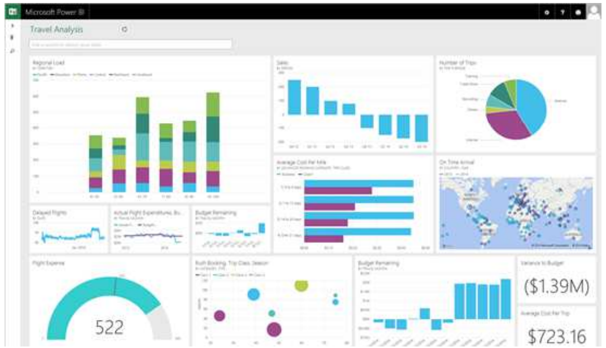
- *Sensors* collect the data from the environment through different technologies.

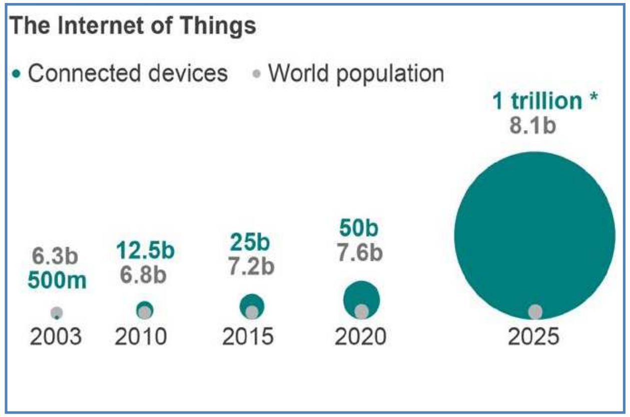
- *Connectivity* allows the connection between all the elements within IoT.

- *Store and analysis***.** Through different IoT devices the data is collected and can be shared with other data using cloud-based services.

- *Visualization* it is important in order to allow the interaction between users and data.

- *M2M***.** IoT has more devices connected than M2M and is used more in the consumer space while M2M has a stronger industrial connotation.
  M2M is used in various applications such as maintenance of machines, measurements, security, chain supply, asset tracking or remote control.





IoT architectures

Perception Layer

- Collect the data from the environment through sensors
- Technologies: RFID, WSN i NFC

Network Layer

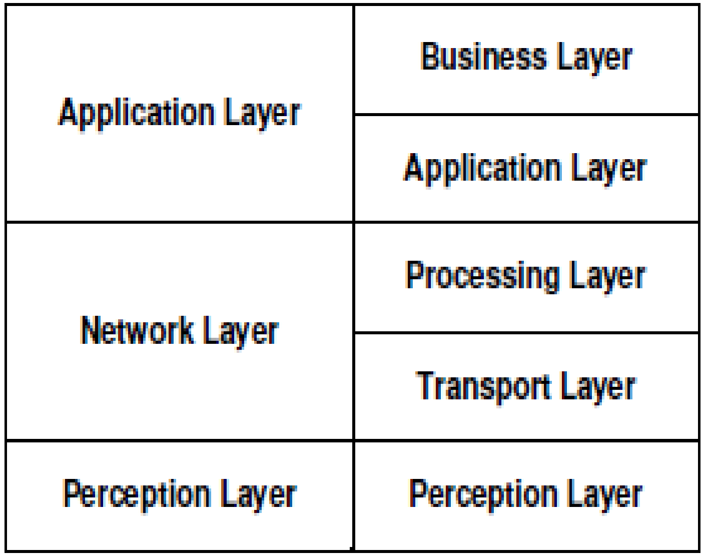
-It is the most important layer, and transmits the data that has been collected by the Perception layer

-Technologies: Bluetooth, BLE, Wi-Fi, WiMAX, ZigBee, Z-Wave,LoRa

Application Layer

-The objective of this layer is to provide a service to customers so that they can store, consult and process the data in a safe way

- Cloud Computing paradigm



Application Layer	Business Layer
	Application Layer
Network Layer	Processing Layer
	Transport Layer
Perception Layer	Perception Layer

3-layer architecture(left) and 5-layer architecture (right)

IoT vulnerabilities

Perception Layer ***(RFID, WSN, NFC)***

The security problems in the Perception layer include the physical security of the devices and the security in the collection of information .Some common attacks that occur in this layer are:

-*Eavesdropping* (RFID). An unauthorized individual uses an antenna in order to record communications between legitimate RFID tags and readers. ***Countermeasure****:* encrypting the communication between the tag and reader.

-Spoofing (WSN). It refers to the use of identity theft techniques with malicious purposes, where an attacker falsifies the origin of the packages, making the victim believe that they are from a trusted host. ***Countermeasure****:* implement an WSN authentication protocol and data encryption.

-*Phishing attack* (NFC). The attacker, known as phisher, is posing as a trusted person in an apparent official electronic communication. ***Countermeasure***: 2-Factor Authentication .

Network Layer ***(Bluetooth, BLE, Wi-Fi, WiMAX, ZigBee, LoRa, Z-Wave)***

The security issues in the Network layer include:

-Man-in-the-Middle attack (Bluetooth). An attacker secretly relays and possibly alters the communication between two devices that believe are communicating with each other. ***Countermeasure***: use the Bluetooth link layer security features.

-Masquerade attack (WiMAX). The masquerading consists of assuming, by a system, the identity of another one ***Countermeasure*** create innovative algorithms that can efficiently detect the suspicious actions.

-***Password cracking* (Wi-Fi).** Wireless access points that use older security protocols are easy targets because these passwords are easy to crack. ***Countermeasure****:* implement WPA2 wherever possible. Although it is vulnerable, guarantees more security than the WEP or WPA.

IoT vunerabilities

Application Layer ***(Cloud Computing)***

In the application layer the main problems are the manipulation and modification of the information that is stored in services and applications such as the services that give the cloud computing.

-Flooding attack*.** These attacks happen when an attacker generates fake data, which could resource some type of code to be run in the application of a legitimate user. ***Countermesure: all the servers in the cloud could be organized as a group of of servers. Each group can be designated for a specific job. When a server is overloaded, a new server will be deployed in the group.

C.Stergiou analyze the security issues of both IoT and Cloud computing technologies and their combination. To protect data they propose the combination of AES and RSA algorithms in the integration of IoT and Cloud technologies

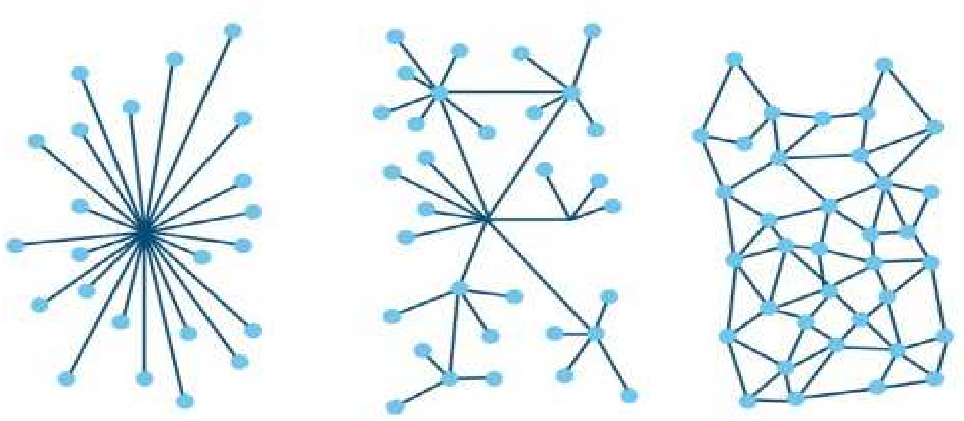
C. Stergiou, K. E. Psannis, B. Kim, B.Gupta, "Secure integration of IoT and Cloud Computing", ScienceDirect,Future Generation Computer Systems vol. 78,part 3,

January2018,http://0www.sciencedirect.com.cataleg.uoc.edu/science/article/pii/S0167739X1630694X

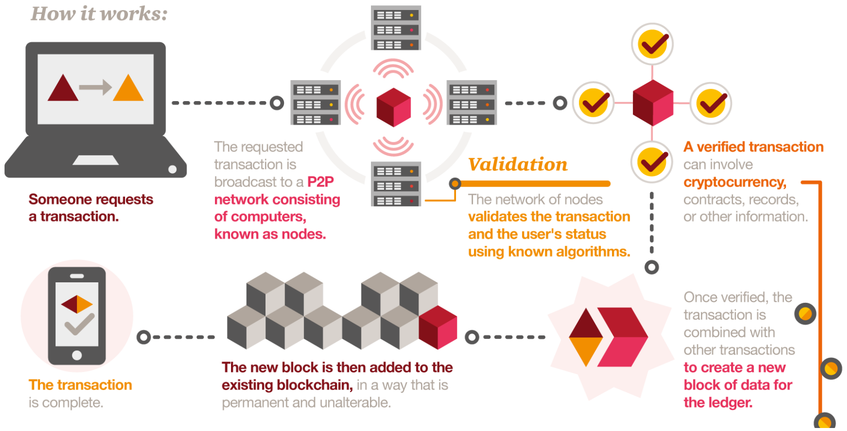
Blockchain technology

Blockchain is a distributed database that registers an ordered list of records of transactions which are immutable linked together through a chain, on blocks.

-The **transaction** is broadcasted to a public **P2P network** (Blockchain network) consisting of multiple nodes.
- The network of nodes validates the transaction using known algorithms.
- Once verified, the transaction is combined with other transactions to create a new **block** of data for the ledger.
- The new block is added to the existing Blockchain, in a form that is unalterable permanently.
- Finally the transaction is successfully done.



From left to right :centralized, descentralized and distributed (Blockchain) networks



How it works:

Someone requests a transaction.

The requested transaction is broadcast to a **P2P network consisting of computers, known as nodes.**

Validation

The network of nodes **validates the transaction and the user's status using known algorithms.**

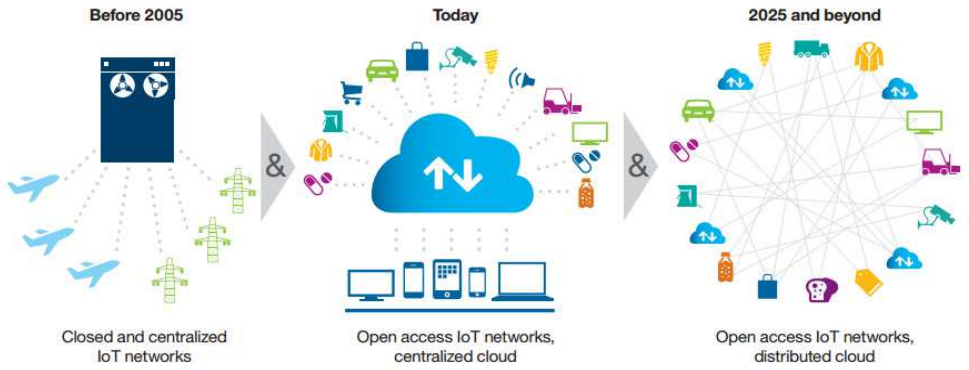
A verified transaction can involve **cryptocurrency,** contracts, records, or other information.

Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger.**

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

The transaction is complete.

IoT and Blockchain convergence


Before 2005
Today
2025 and beyond
&
&
Closed and centralized IoT networks
Open access IoT networks, centralized cloud
Open access IoT networks, distributed cloud

[-]Lack of maturity and standards to promise interoperability among competing ledgers and platforms.
[-]*Legal issues*: It is a completely unknown territory without any legal code to follow, and this could be a problem for manufacturers and service providers.

[+]A private blockchain can store cryptographic hashes of individual device firmware. This record can prove that a specific device has not been manipulated or attacked. When that is proved, that device is allowed to connect with other services or devices.
Blockchain-based identity and access management systems can fight successfully against attacks related to IP address forgery or IP spoofing.
[+]Blockchain provide secure and more integrity for data vulnerabilities through verification; transactions are signed and verified cryptographically to prove that the originator is the one who have sent the message.

Proposed scenarios

- Sport Center with IoT and Blockchain technology

  -Digital Identity

  -Reservation of paddle tracks

- Smart museum with Blockchain technology

  -Payment of employees' salaries

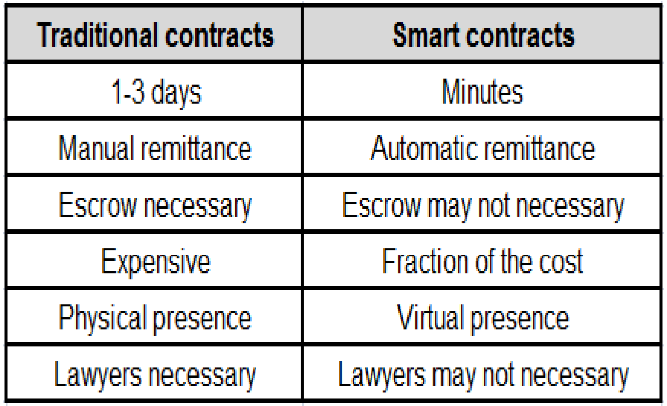
  -Supply chain

  -Purchase of products

- Football Club with Blockchain technology

  -Purchase of tickets

  -Voting



Traditional contracts	Smart contracts
1-3 days	Minutes
Manual remittance	Automatic remittance
Escrow necessary	Escrow may not necessary
Expensive	Fraction of the cost
Physical presence	Virtual presence
Lawyers necessary	Lawyers may not necessary

Conclusions

- Main security concerns in IoT paradigm are:
  - the first concern is the physical security of devices
  - the second concern is the security in networks that allow the connectivity of devices and all the elements that take part within.
  - the privacy and security on the platforms offered by the services to store and process the data such as cloud computing

- Many IoT solutions are focused on addressing authentication and identification issues.
  There are projects using Blockchain technology to solve IoT issues. (Physically Unclonable Functions, algorithms..)
  There are also projects of the Blockchain in combination with the M2M to improve communications and security in industrial processes. Some of these solutions are based on CPS (Cyber-Physical Systems).

- *The weaknesses* of the Blockchain technology are the slow implementation and the regulatory problems that depend on the individual policies of each country.
  The strengths are the transparency, the absence of intermediaries, and the security.
  Many companies are already implementing projects with Blockchain, and if everything goes as well as it is expected, it will be the most important technology in the future for the IoT devices connection and data protection.

Analysis and study of data security in the Internet of Things paradigm from a Blockchain technology approach

Titulació: Màster Universitari en Enginyeria de Telecomunicació UOC-URL

Autor: David Rull Aixa
Consultor: Raúl Parada Medina
Responsable: Carlos Monzo Sánchez
Gener, 2018

UOC
Universitat Oberta de Catalunya

UNIVERSITAT RAMON LLULL