

# INTERNET OF THINGS SECURITY



## **Presenters:**

Taghreed Mohammed Alotaibi

Ghosson Abdulrahim Banjar

Eman Abid Almalki

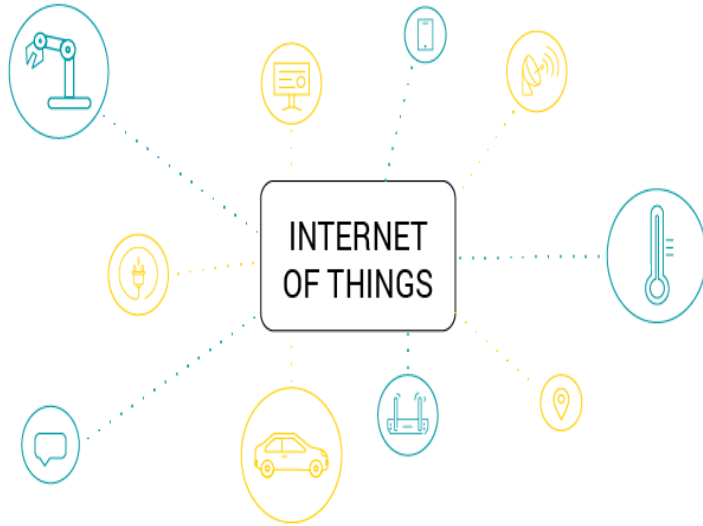
Shatha Salem Alshehri

Aisha Zakaria Mardlly

Yasmin Mahmoud Alkaddour

**Presented to: Rana Al-harbi**

# Introduction



The number of users of the technologies are increasing with the variety of the technologies to ease people life as much as possible. For that the security for these technologies is very important to protect people privacy and data. This project will discuss the security of internet of things and the reason of choose this technology is because that this technology has been widespread and used almost in every house

## **Background of IoT**

Internet of Things (IoT)  
Definitions

**01**

## **Methods and Architecture of IoT**

Examples For Middleware

**04**

**Why is Security so  
important in IoT?**

**02**

## **IoT security Algorithms**

Lightweight cryptography

**05**

**IoT Lifecycle and How  
the IoT works**

**03**

## **Use Case**

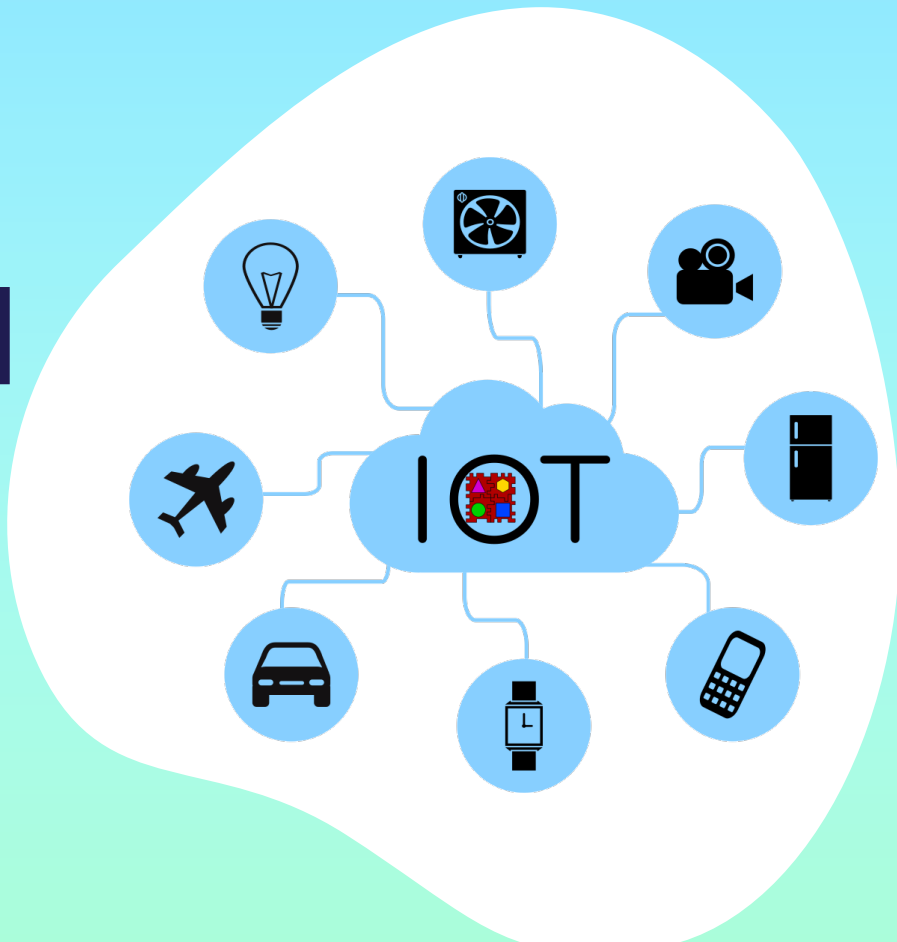
How to protect NFC Reader  
Systems

**06**

# 01

## Background

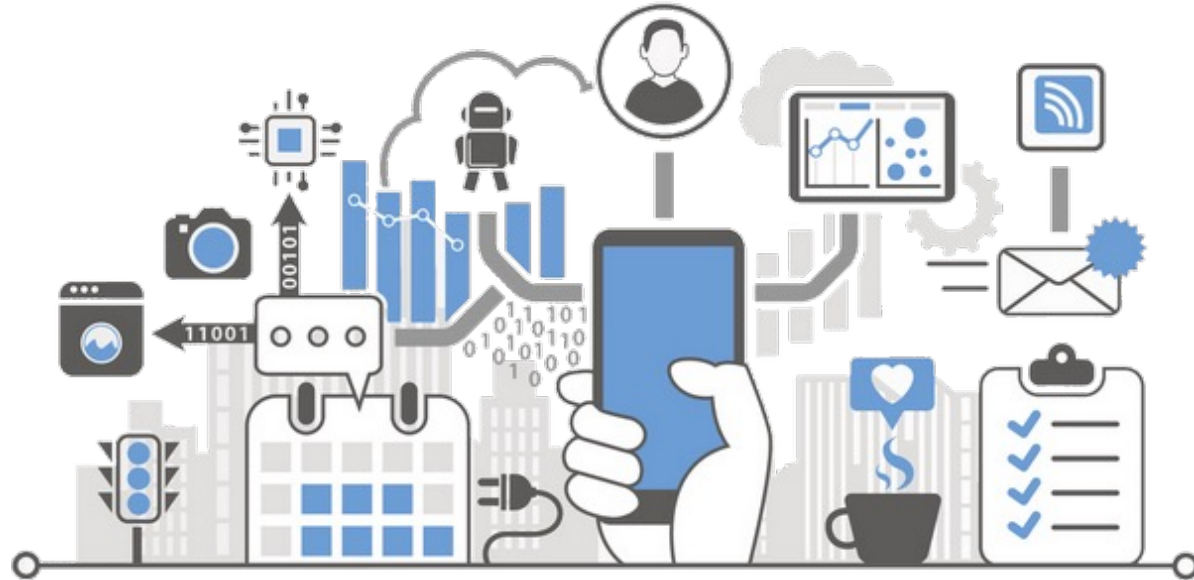
Internet of Things (IoT)  
Definitions



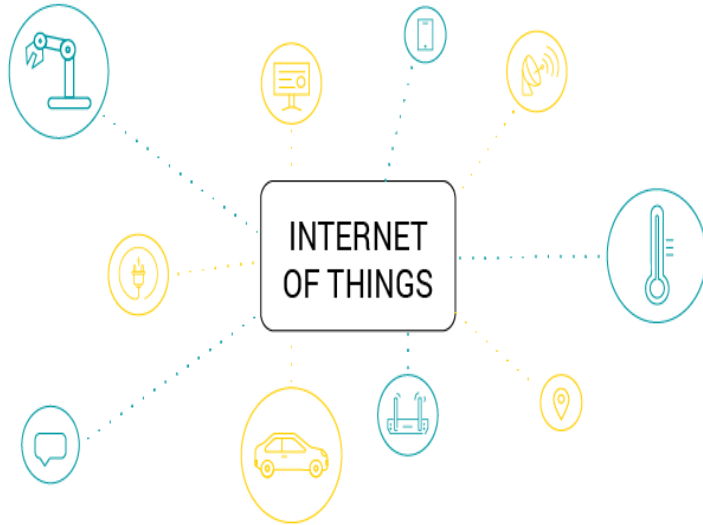
# Background

- Definitions
- Historical notes
- Usage
- Application

# IOT



# Definition



## Internet of Things (IoT) Definitions

a model in which objects equipped with sensors, engines, and processors communicate with each other to serve a meaningful purpose. IoT is not only one technology, it is a set of different technologies.

What is the meaning of sensors and Engine?

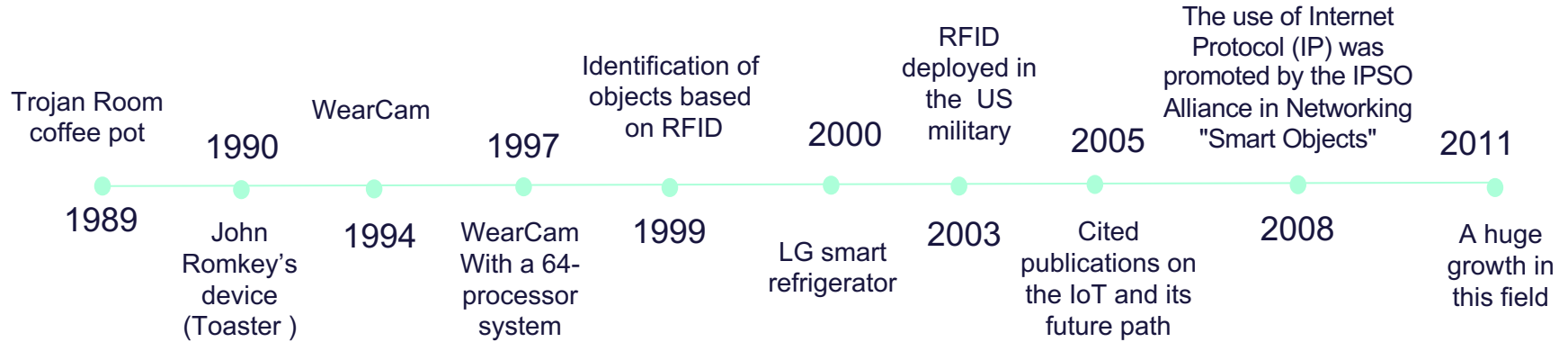
Sensors and engine are devices that help interact with the environment. The mobile phone or microwave oven can be considered as a sensor.

The engine is:

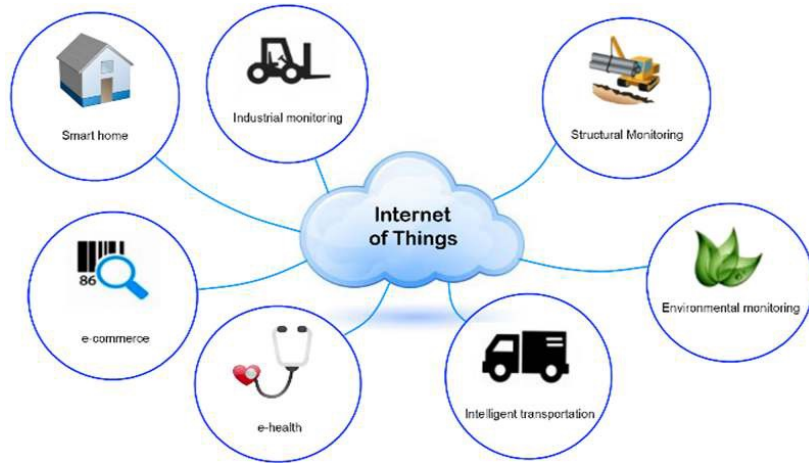
a device used to make a change in the environment, such as the air conditioner remote

that represents sensors, engine, computer servers, and the communication network, the basic infrastructure of the Internet of Things framework.

# History



# Usage



Uses of IoT (internet of things) are the industries that are implementing IoT devices and technologies for technical advancement. The uses and new capabilities are adding to this technology and are growing in year-on-year basis. Most organizations are using this technology to help human life easier. [9]

Uses of IoT in various Industries

IoT will be the largest category of IT services in the upcoming years, which can change the industrial landscape. Let's discuss various use cases of IoT grouped by type of industry.



# Usage



## 1. Agriculture Industry

As industry agriculture follows the traditional experience-based operations, which are heavily dependent on human intervention. But with the changing economic landscape and the population increment, the supply-demand gap is huge. Changing environmental conditions, global warming is also a part of the challenge. IoT is probably the most powerful weapon for the agriculture and farming industry to fight this. IoT enables farm managers with real-time crop monitoring, precision farming, livestock management, smart greenhouse management, etc. Industry-grade drones also have multiple use cases in smart farming. On the one hand, drones are used to monitor air, soil, moisture quality; and the other hand; they can help with physical activities like automated spraying of fertilizers, preventing physical breakouts in farms, etc.

## 2. Healthcare

One of the important sectors that will get benefit mostly from Industry grade IoT is healthcare. The popularity of smart devices, wearables are increasing day by day. This enables researchers with more and more data to incorporate IoT solutions. Data from wearables are used to prevent heart attacks, constantly monitoring the heart rate, steps taken, tracking sleep, sitting postures, etc. IoT based solutions with nano-technology are even used to monitor cancerous cells inside the body. IoT, along with machine learning, is changing the industry at a rapid scale



# Applications



IoT application has been introduced in many domains such as social media, health, transport, medicine, etc. The advantages and requirements of IoT solution depends on the needs of the industry. Few domains such as health care, business analytics, transport, and smart homes/city will be discussed in this section [10]

## 1. Medicine and Health care

Health care has been a major user of IoT applications, where IoT applications are helping the users to gather statistical data and further control and automate the medical process. According to a recent survey, the IoT market share has been increased from USD \$298 Billion in the year 2014 to USD \$700 Billion in the year 2017. IoT technology is being embedded in health care devices, including wearable and implantable devices used to monitor and improve patients' medical conditions. With the advancement in IoT in the medical and health care domain, investors and the public will benefit in many ways. Overall life-sustaining care costs will decline, and improved health monitoring systems will benefit millions of people every day. A method was proposed at IoT annual meet in 2018, which was aimed at reducing childhood obesity. A robot was built with the help of AI and was assigned to collect medical data with the help of sensors placed on the chest of the children. Further, a questionnaire-based survey on the food diet, physical activities, and other environmental factors were collected from the population and transmitted over to the web. This is one of the examples of advanced IoT functionality in the health care sector.

# Applications



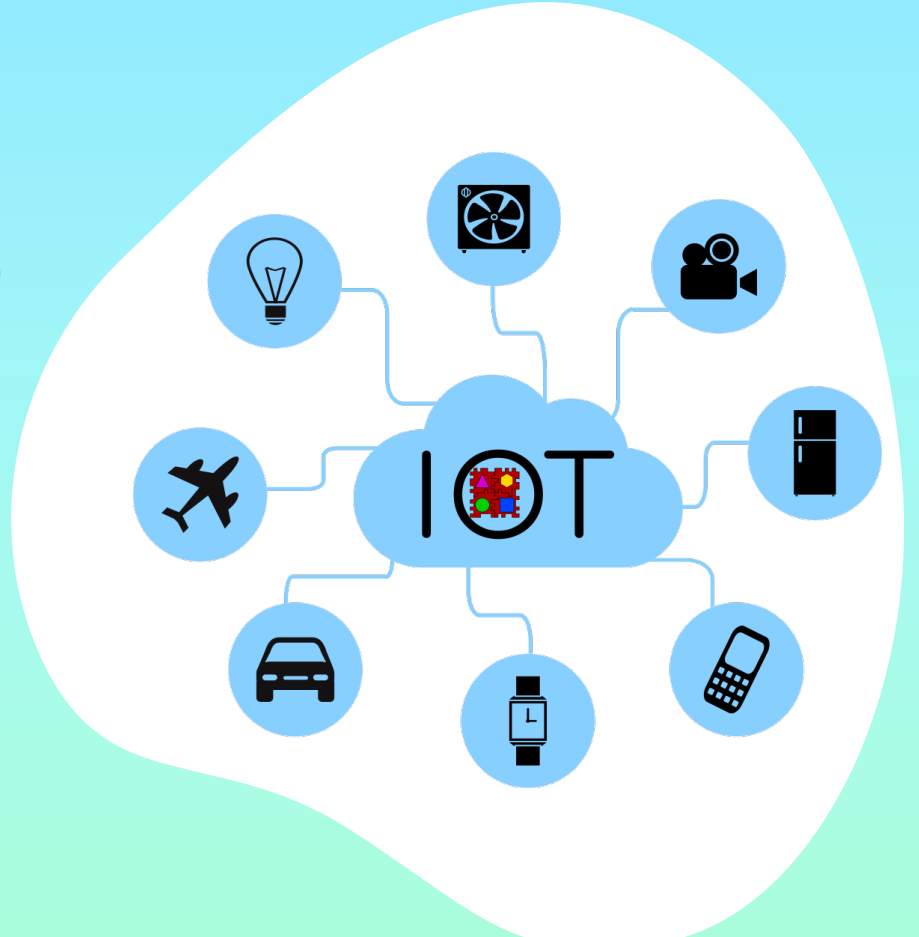
## 2. Smart city and Homes

Smart city IoT application is designed to provide improved and better-living conditions. With the growth in technology and population, IoT will play a major role in managing the city and population. Many services such as energy-saving lights, weather reporting systems, and streetlights will be embedded with IoT solutions for sustainable and cost-effective reasons.

Home automation has seen rapid growth in recent times. Consumers have been provided with services like lightning control for their homes, voice-based controlling, smart air quality adjustment, AI experience, and smart locks with the IoT enabled in homes. The biggest reason people are attracted to smart home technology is because of security features. For example, with the help of a simple IoT device, the lights of the house can be monitored when on vacation; this function will keep the intruders away. Webcams can be installed with the help of this application to monitor the home; the major advantage here is one can control the connected devices remotely using a web interface or just a simple mobile application.

# 02

## Why is Security so important in IoT?



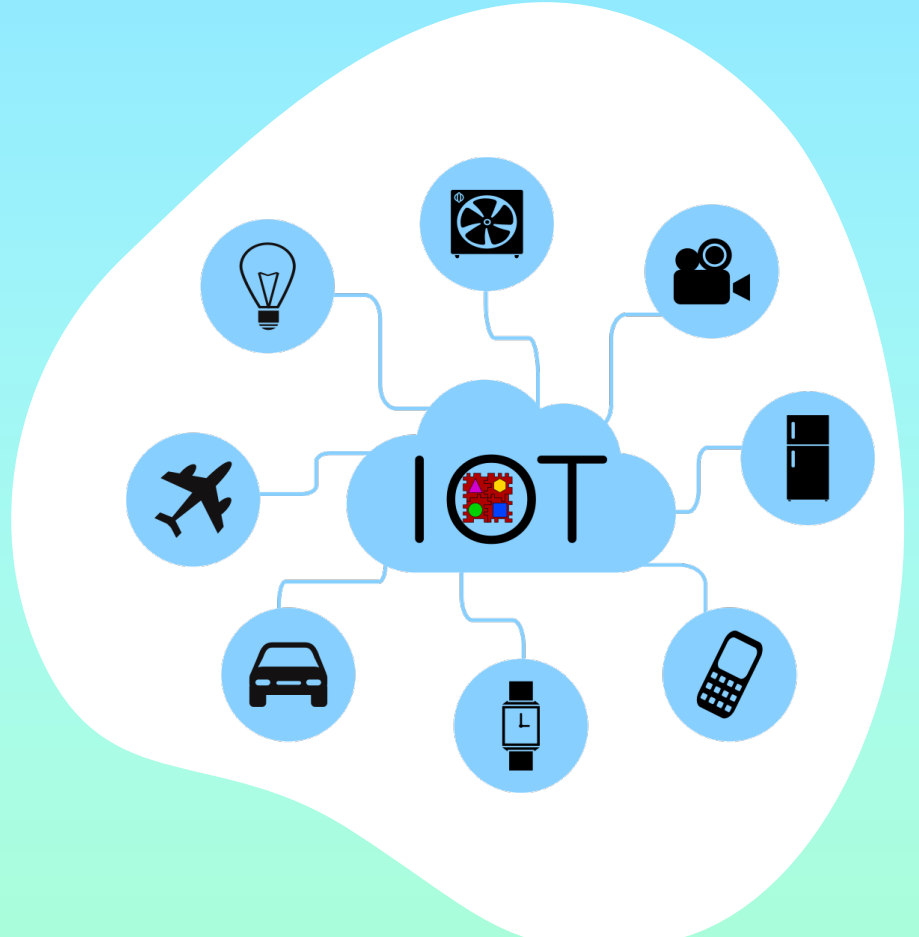
# Why is Security so important in IoT?

Security and Privacy are a very important aspect for IoT application domains. These applications require data **confidentiality**, **authenticity**, **integrity**, and access control within the IoT network.



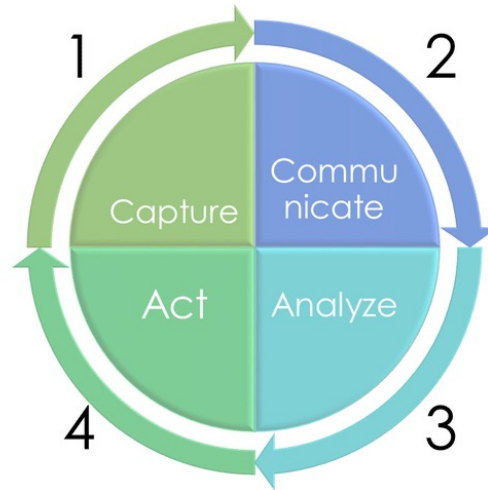
03

# IoT Lifecycle and How the IoT works



# The IoT Lifecycle

- **Collect/capture:** Collect data through devices and sensors from anywhere, such as the home.
- **Communicate:** Sending data over the communication networks of the data center, for example through cloud computing, the data center or the internal home network.
- **Analyze:** Generate useful information from data such as reports, data classification
- **Act:** Doing a certain action based on the data and information received from the devices, for example, the connection of one device to another device. Sending notifications to a specific device automatically, turning on the lights, turning off the printer and others.



# How the IoT works

- What is IoT gateway?

An IoT gateway, or Internet of Things gateway, is communication between different technologies and data. IoT gateways are devices or software that connected devices, controllers, sensors, and external networks (like the Cloud), they translate the variety of protocols or languages that smart devices use, like Wi-Fi, Bluetooth, Ethernet, MQTT, or Serial ports, so that components can connect back to the system that needs their data.

But IoT gateways are smart, meaning they **Collect sensor data, Translate protocols, and Process sensor data, all at the edge of the network, before sending it on to the cloud.**

Doing all of this at the edge is necessary because of the volume of the internet-connected devices or sensors grows, and so does the volume of data they generate.

IoT Gateways filter out routine or unnecessary data to avoid overwhelming the system.

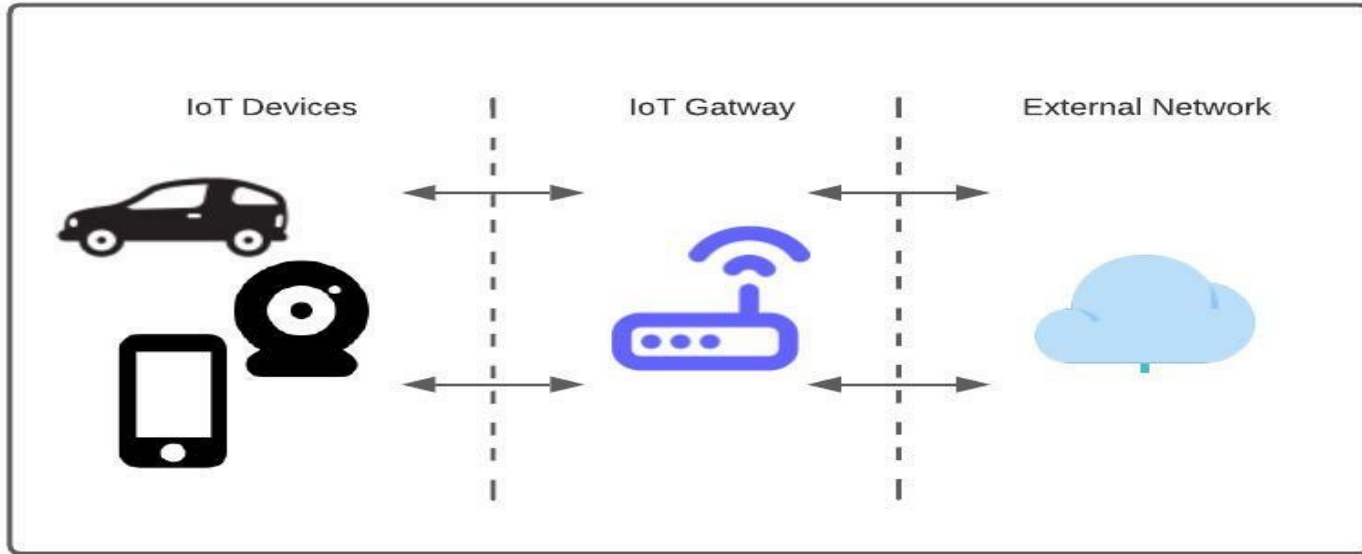
Just one IoT connected office building, for instance, could have hundreds or thousands of sensors that measure temperature, light, air quality, or security systems and each of those generates data every second. So, an IoT gateway here would pass on temperature data to the cloud if it's hotter or colder than predetermined range, filtering out comfortable room temperature data. In addition to protocol translation and data filtering processing.

IoT gateways perform other critical functions like **Device connectivity, Security, Updating, Management, and more.**

Some newer gateways also operate as platforms for code, that can analyze data and take action, like determining that the room temperature is too high, and then turning on the air conditioner.

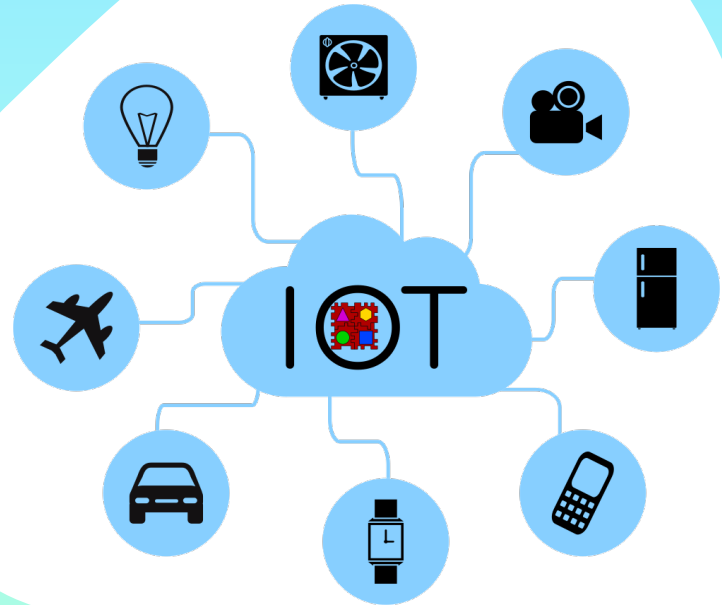


# How the IoT works



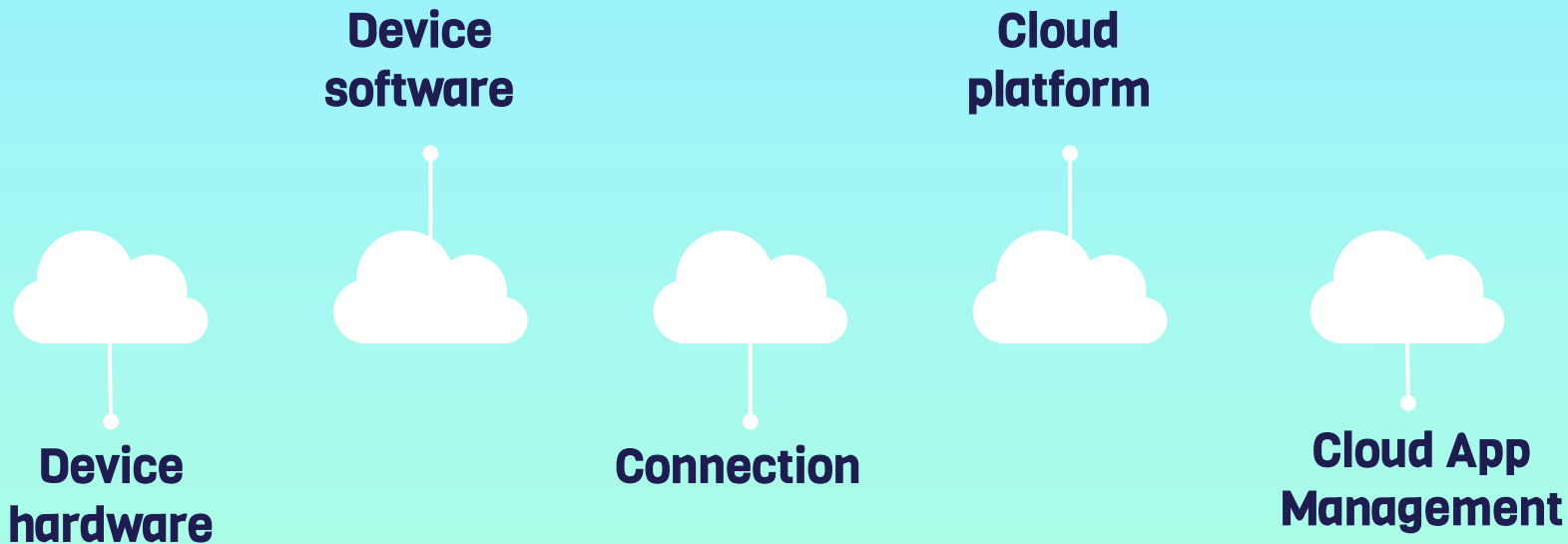
# 04

## Methods and Architecture of IoT



# Methods used in IoT

All these methods should be secure



# Architecture of IoT

There is no universally agreed single IoT architecture, but the most basic and widely used format is the three-layers architecture. It was first introduced when the first research on the Internet of Things was being done. It proposes three layers, which are: perception, network, and application.

## **1 - the Percentage layer**

this is the physical layer that contains sensors that sense and collect information about the environment, such as identifying some smart things in the environment.

## **2- the network layer**

which is responsible for connecting to other smart things, network devices and servers. Its features are also used to transmit and process sensor data.

## **3- applications Layer**

responsible for providing application-specific services to the user. It identifies the different applications in which the Internet of Things can be deployed such as smart homes, smart cities, and smart health.

# Architecture of IoT

The previous structure (three layers) defines the main idea of the Internet of Things, but it is not enough for the research aspect, as the research aspect of the Internet of Things often focusses on the exact aspects. For this reason, we have many multi-layered structures that have been added to the previous layers (processing and business class). [11]

## **4- Process layer**

Known as the middleware layer, it processes and processes huge amounts of data that come from the transport layer and employs many technologies such as databases, cloud computing, and big data processing units.

## **5- The transport layers**

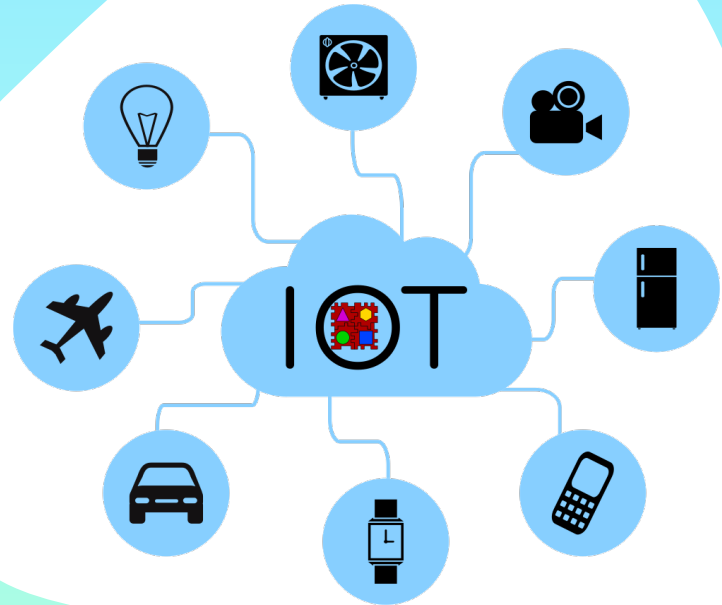
Transfers the data of the sensor from the cognitive layer to the processing layer, and vice versa, how is it transferred?

Through wireless networks, 3G, local area network, Bluetooth.

# 05

## IoT security Algorithms

Lightweight cryptography

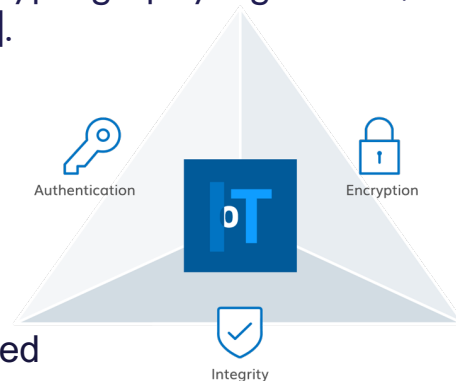


# IoT security Algorithms

Because IoT is small devices that connect together. The Conventional cryptography is not suitable for it because it is very difficult for resource limited environment to implement the standard cryptographic algorithms due to the implementation size, speed or throughput and energy consumption. For this, lightweight cryptography algorithms are developed that have extremely low requirements. Even though no strict criteria are defined for lightweight cryptography algorithms, the features usually include any one or more of [1].

- Minimum size required for hardware implementation.
- Low computational power of microprocessors or microcontrollers.
- Low implementation cost.
- Good security

Lightweight cryptography targets a very wide variety of resource-constrained devices such as IoT end nodes and RFID tags that can be implemented on both hardware and software with different communication technologies.



# IoT security Algorithms

Characteristics		What LWC can offer?
Physical (Cost)	Physical Area (GEs, logic blocks)	<ul style="list-style-type: none"><li>- Tiny key &amp; block</li><li>- Simple rounds with simple consumption</li><li>- Simple key generation</li></ul>
	Memory (registers, RAM, ROM)	
	Battery power (energy consumption)	
Performance	Computing power (latency, throughout)	
Security	Minimum security strength (bits)	<ul style="list-style-type: none"><li>- Strong internal structure</li></ul>
	Attack models (related key, multi-keys)	
	Side-channel and Fault-injection attacks	

Table 1 Characteristics of lightweight cryptography [12]





# Lightweight Cryptography Types

**PRESENT:** is one of the leanest lightweight algorithms and has obtained the ISO/IEC standard for lightweight cryptography. It was designed for hardware performance but can be implemented in software. The applications that mainly uses PRESENT algorithm is for encrypting small or reasonable amount of data. It used in RFID application. [2]

**TEA:** The Tiny Encryption Algorithm (TEA) was developed with the objective to be used on low performing small computers. This block cipher is based on a high performance but mathematically simple encryption algorithm which are variants of a Feistel Cipher.

- TEA encrypts 64-bit blocks which are divided into 32-bit blocks.
- Uses a 128-bit length key.
- TEA is a round based encryption method. The number of the used rounds are variable, but 32 Tea cycles are recommended.

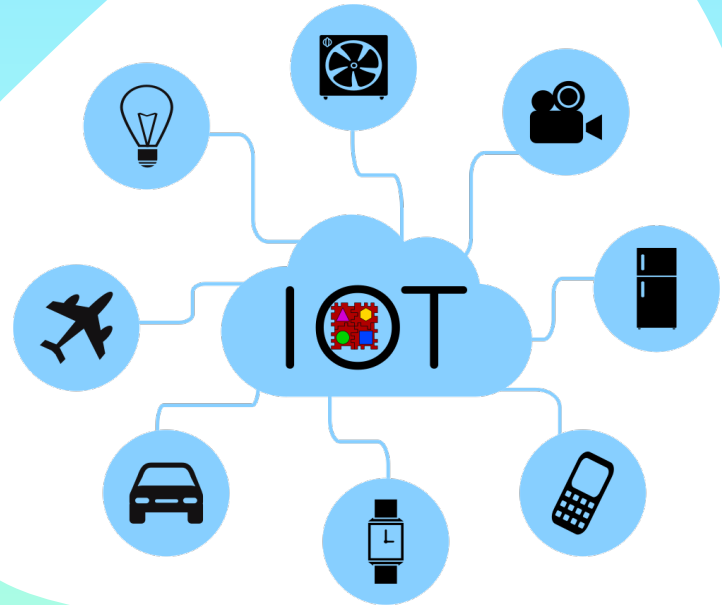
It used in Energy-aware server [2].



# 06

## Use Case

How to protect NFC Reader Systems



# Use Case

First, we will discuss the main basic concepts to clarify the use case.

NFC read/write: Reads data in from device or writes data out (Get information or initiate an action) and Interacts with an NFC-enabled device.

Peer-to-Peer Mode: Establishes two-way communication between NFC -enabled devices and Each device serves as an endpoint.

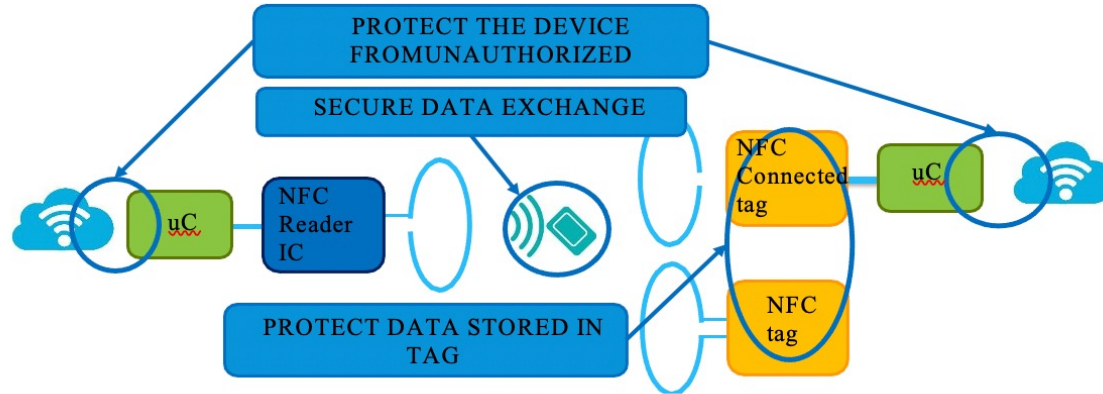


Figure 3

# Use Case

The uC is a microcontroller

## **What do we want to protect?**

NFC systems are interoperable and open by default.

## **So, what are the security need?**

Secure data exchange

Securing data exchanged through RF channel through cryptographic methods.

Using cryptography implies the usage of cryptographic keys on both sides of the communication.

Data is now protected through cryptographic means; NFC system is not open/interoperable anymore.

Protection from unauthorized access

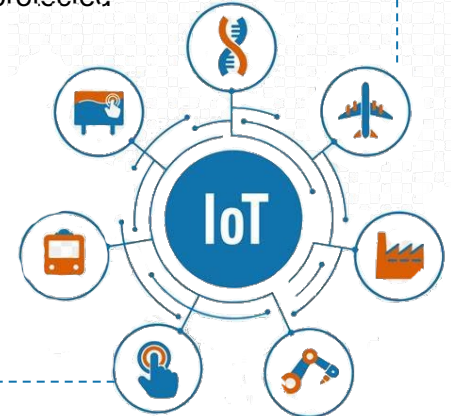
Any device connected to the “cloud” is subject to be compromised and attacked if not properly protected

Need to implement security mechanisms to:

- ♣ Grant access to authorized servers
- ♣ Prevent exposure of user related data (privacy)
  - ♣ Secure communications between device and backend
- ♣ Ensure system integrity
- ♣ Protection of credential

Above objectives can be ensured through:

- ♣ Cryptographic methods
- ♣ Hardware based security



# Use Case

What do we want to protect data exchange?

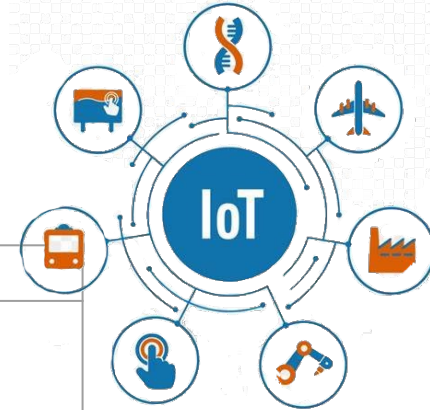
NFC by default is open and interoperable, data exchange is inherently secure due to its proximity. So, we want to secure the information exchanged through the NFC interface between A and B.

Information security goals:

- ♣ Confidentiality
- ♣ Integrity
- ♣ Authenticity

Cryptography as a means to achieve information security goals.

Security goal	Description	Mechanism	Algorithm
Confidentiality	Guarantee that data cannot be read by an unauthorized entity	Encryption/Decryption	TDES, AES,RSA, ECC
Integrity	Guarantee that data cannot be changed by an unauthorized entity	CMAC and Digital Signatures	
Authentication	Guarantee mutual identification of two parties entering into a communication	Static (password, PIN,...) Dynamic (challenge-response protocol)	



# Use Case

Using cryptographic algorithms implies usage of secret keys.

Cryptographic algorithms:

♣ Symmetric: Same key on both sides. TDES, AES.

♣ Asymmetric: Public/private key pair. RSA, ECC.

|



Secret key



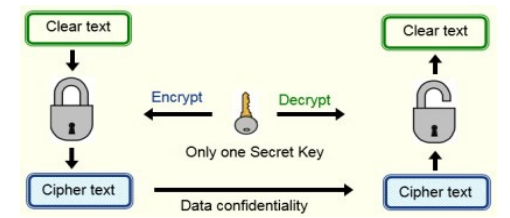
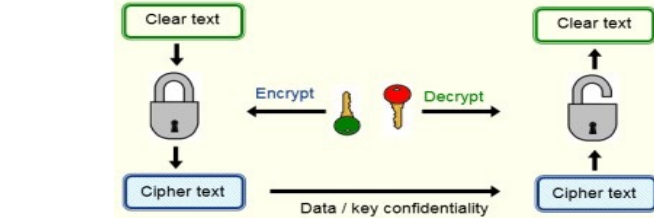
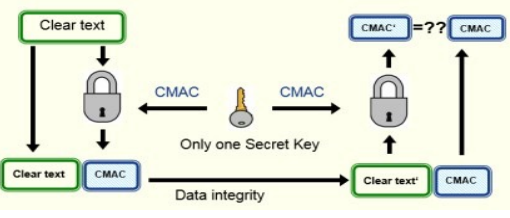
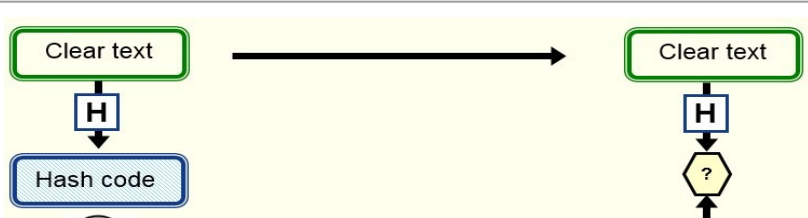
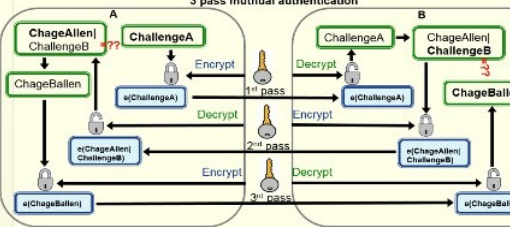
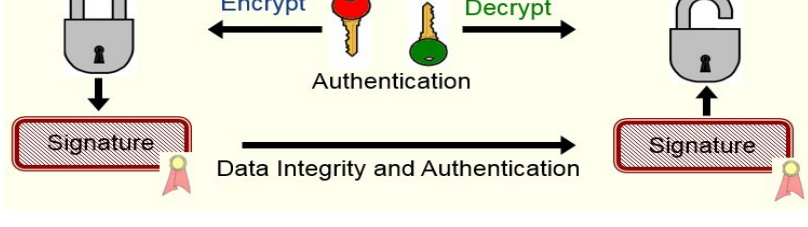
Public Key



Private Key



# Use Case

	Symmetric	Asymmetric
Confidentiality	 <p>Clear text</p> <p>Encrypt</p> <p>Only one Secret Key</p> <p>Decrypt</p> <p>Cipher text</p> <p>Data confidentiality</p>	 <p>Clear text</p> <p>Encrypt</p> <p>Decrypt</p> <p>Cipher text</p> <p>Data / key confidentiality</p>
Integrity	 <p>Clear text</p> <p>CMAC</p> <p>Only one Secret Key</p> <p>CMAC</p> <p>Data integrity</p>	 <p>Clear text</p> <p>Hash code</p> <p>Data integrity and authentication</p>
Authentication	 <p>3 pass mutual authentication</p> <p>Authentication</p>	 <p>Signature</p> <p>Data integrity and authentication</p>

## Case Study

As shown in Figure (3) the keys are not located in the NFC Reader and the microcontroller not designed to protect secret keys. So, adding a SAM to the Reader allows us to securely store and protect the cryptographic Key keys

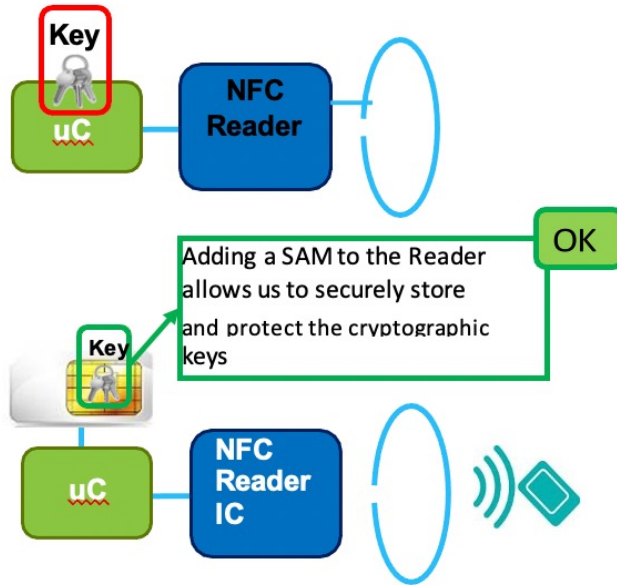


Figure 4





# Use Case

To ensure confidentiality of the written data in the tag:

- ♣ Data stored are encrypted.
- ♣ Secret key to decrypt it stored in SAM in the NFC device.

To ensure data integrity and authenticity of the written data in the tag:

- ♣ Digital signature added to data stored.
- ♣ Secret key to verify digital signature stored in SAM in the NFC device.

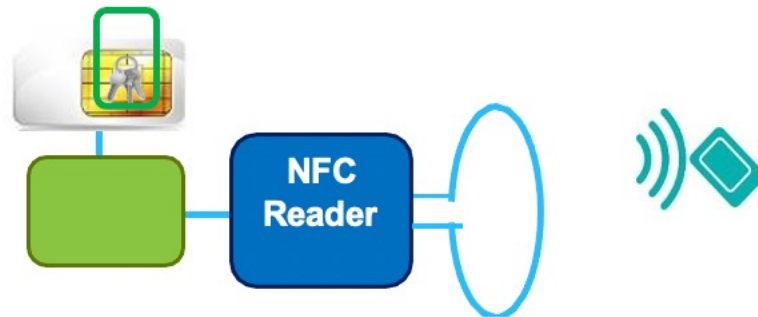


Figure 5



Data stored can be:

- Encrypted
- Digitally signed

# Use Case

## Protection From Unauthorized Access

A-Series ICs from NXP are HW Security Module for IoT Devices

- ♣ Supporting wide variety of use cases and targeting multiple applications
- ♣ Off-the-shelf solutions offering key injection service, on chip application SW and host library with a high-level API

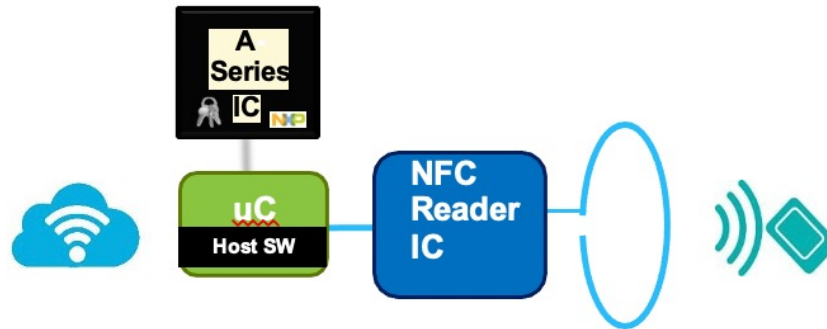


Figure 6



# Use Case

What do we want to achieve in Access Control systems?

- ♣ Secure system with optimized cost
- ♣ Intuitive and fast access
- ♣ Simple and flexible management
- ▶ NFC Technology fully covers the above requirements.
- ▶ Credentials designed to securely store and protect cryptographic keys.
- ▶ NFC Readers shall be designed to offer the same level of protection.



We can divide NFC threats in 2 parts as we shown in table:

Operating Modes	Attack
Card Emulation mode	Eavesdropping in the card emulated mode
	Relay Attack
	Denegation of attack
Reader Writer mode	Phishing attack
	Ticket cloning
	Identity Authentication



# NFC Threat and attack Analysis

Advantage and disadvantage of NFC mode communication [12]



	Card Emulation mode	Reader Writer mode
<b>Standard</b>	ISO/IEC 14443	ISO/IEC 14443
<b>Advantage</b>	Combine many digital valued card in one phone	It can read tags information in darkness and contact soon
<b>Disadvantage</b>	The content of card can be read by others when mobile phone is out of battery or in the turn off status.	The price of the active tags is high. It need more cost for mass production than produce QR code tag.
<b>Application</b>	E-passport, mobile payment, check in and member identification	Museum guiding, transportation tokens, turn on / off some function on the phone quickly

It is important to highlight that passive mode data transmission is somehow difficult to be attacked on compared to active mode. Only solution to this type of threat is to use a secure channel (SCH). The communication over NFC channel should be authentication based [3,15,16].

**Relay Attack:** in this attack the attacker uses another communication link (relay) as a mediator to increase the range. The attacker needs no physical access to the device, but only an antenna and the relay device in reading range.[3]  
Solution: monitor the signal and signal range analysis.

# NFC Threat and attack Analysis

**Phishing:** protection of touching a tag or a reader with the mobile phone is probably much lower than wired connection.

So phishing attacks could easily be applying by replacing or modifying tags. This is a simple and inexpensive way to reach NFC tags data.

Using signatures on tags and transporters would be suitable way to overcome this issue.[15]

**cloning:** in this attack the original tag is read and an exact copy is created. Some papers show that this attack is same as relay attack

, the complexity of attack depends on the tag security and accessibility. A read-only tag (ROT) which stores only a simple ID can be cloned very easily.

There are also simple solutions to change the ID. The reader cannot detect if it is the original or the cloned tag. If some kinds of certification is used

, this attack would get more complex and unsuccessful. This attack compromises the secrecy of an NFC system [15]



## RESOURCES

- [1] A. Alaba, M. Othman, H. Targio and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10-28, 2017.
- [2] Yan, P. Zhang and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120-134, 2014.
- [3] M. Aazam, "Cloud Customer's Historical Record Based Resource Pricing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 7, pp. 1929-1940, 2016.
- [4] Building the Web of Things with Sun SPOTs - [PDF Document]," vdocuments.net, [Online]. Available: <https://vdocuments.net/building-the-web-of-things-with-sun-spots.html>.
- [5] "romkey.com," romkey.com, [Online]. Available: <https://romkey.com/>. [Accessed 2022].
- [6] "Steve Mann, Personal WWW page: "WearCam", myview.html," Wearcam.org, [Online]. Available: <http://wearcam.org/myview.html>.
- [7] "Sensors: the next wave of innovation: Communications of the ACM: Vol 40, No 2," Communications of the ACM, [Online]. Available: <https://dl.acm.org/doi/abs/10.1145/253671.253734> .
- [8] "That 'Internet of Things' Thing - RFID JOURNAL," RFID JOURNAL, [Online]. Available: <http://www.rfidjournal.com/articles/view?4986>.



## RESOURCES

- [9] "Uses of IoT: Top 9 Uses Of IoT Application In Real World In 2020," EDUCBA, 28 October 2021. [Online]. Available: <https://www.educba.com/uses-of-iot/?source=leftnav>.
- [10] "Applications of IoT: Learn 4 Major Forms Of Internet of Things," EDUCBA, 02 November 2021. [Online]. Available: <https://www.educba.com/applications-of-iot/?source=leftnav>.
- [11] I. Woungang, S. K. Dhurandher and A. Visconti, "Internet of Things: Architectures, Protocols, and Applications," *Internet of Things*, vol. 14, p. 100267.
- [12] R. H. Aswathy and N. Malarvizhi, "An investigation on cryptographic algorithms usage in IoT contexts," *International Journal of Engineering & Technology*, vol. 7, no. 1.7, p. 10, 2018.
- [13] S. Trilles, A. González-Pérez and J. Huerta, "An IoT Platform Based on Microservices and Serverless Paradigms for Smart Farming Purposes," vol. 20, no. 8, 2020.
- [14] M. Fathy, A. Samouti, "Analysis, compare and develop the Encryption methods for eavesdropping in Near Field Communication (NFC)", Msc thesis, University of IUST, 2013.
- [15] C.-H. Chen, "NFC Attacks Analysis and Survey," in 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2015.
- [16] N. B. Thorat, "SURVEY ON SECURITY THREATS AND SOLUTIONS FOR NEAR FIELD COMMUNICATION," in IJRET: International Journal of Research in Engineering and Technology, 2014.
- [17] H. S. Korrtdedt, Securing Near Field Communication, Norwegian: Master of science, 2010.