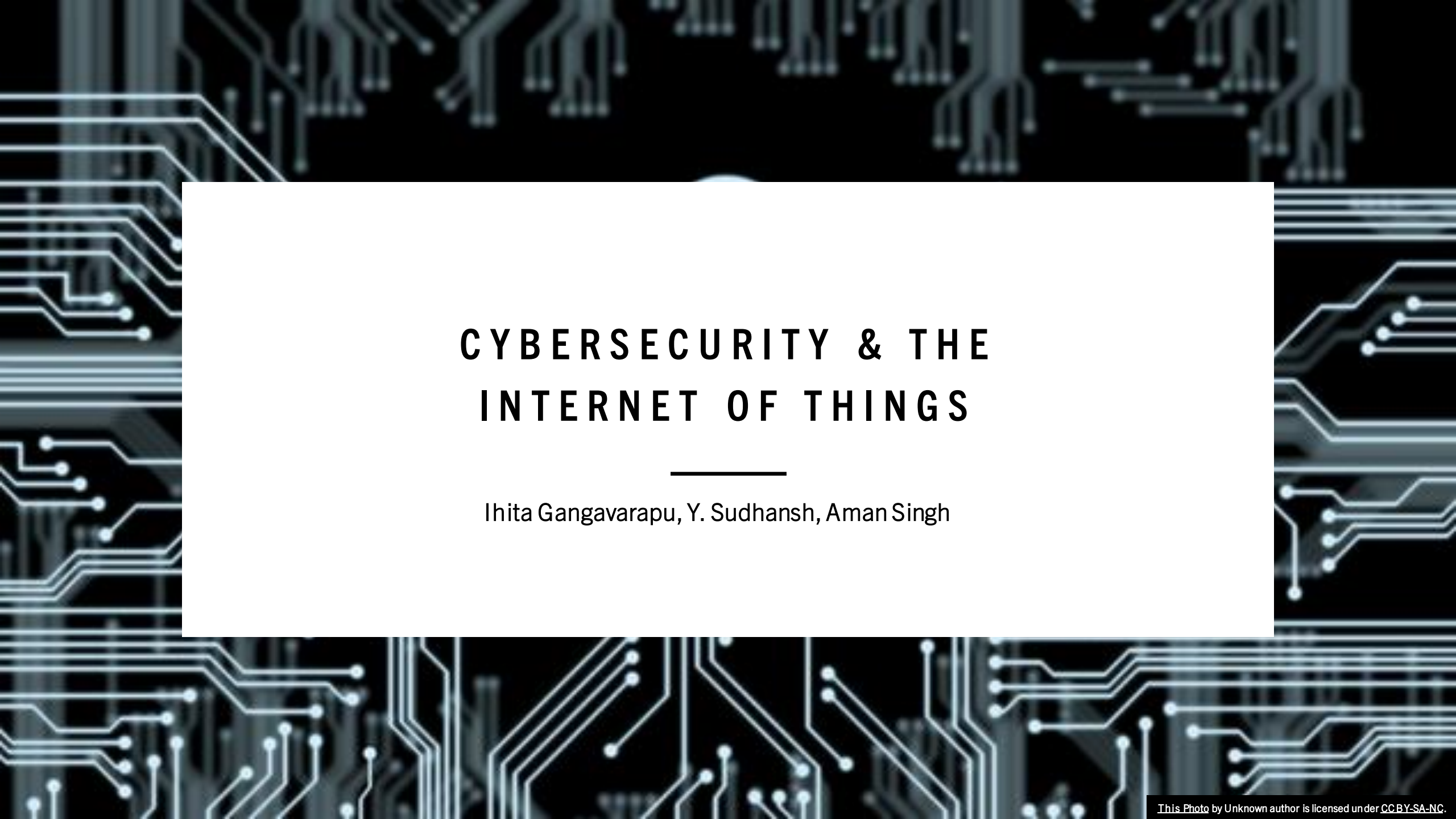


# CYBERSECURITY & THE INTERNET OF THINGS

Ihita Gangavarapu, Y. Sudhansh, Aman Singh

# TODAY'S PRESENTATION WILL COVER

- Cybersecurity basics
- Internet of Things security
- ESW problem statement with demonstration

# INFAMOUS SECURITY ATTACKS

- **Solarwinds attack** (malware): September 2019 attack initiated with corrupted software updates sent out on March 26, 2020.
- **Mirai botnet attack** (attack on IoT systems, DDoS): October 1, 2016 Mirai source code released on GitHub and Dyn.com attacked on October 21, 2016. (Check out: https://www.shodan.io/)
- **Colonial Pipeline** (ransomware attack): Data stoled on May 6, 2021 and malware attack intiated on May 7, 2021

# BASIC PRINCIPLES OF SECURITY

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

AUTHENTICITY

NON-REPUDIATION

# CAN YOU NAME SOME CYBER ATTACKS/THREATS COMPROMISING THE PRINCIPLES?

Go to https://www.menti.com/ and use code 83834310 (EXPIRED)

# TOP 15 CYBER THREATS | 2021


https://www.enisa.europa.eu/

# TYPES OF SECURITY

HARDWARE SECURITY

NETWORK SECURITY

CLOUD SECURITY

APPLICATION SECURITY

# HARDWARE SECURITY

- Hardware security module (HSM): Physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions.
- Common Vulnerabilities and Exposures(CVE) : Unique, common identifiers for publicly known information-security vulnerabilities in publicly released software packages.
- MITRE: globally-accessible knowledge base of adversary tactics and techniques based on real-world observations (https://attack.mitre.org/)

# NETWORK SECURITY

- Identity
- Perimeter security
- Data privacy
- Security monitoring
- Policy management

# ELEMENTS OF RISK

- What are the threats?
- What are the vulnerabilities?
- What is the likelihood of a threat exploiting a vulnerability?
- What would be the impact of this to your systems/business?

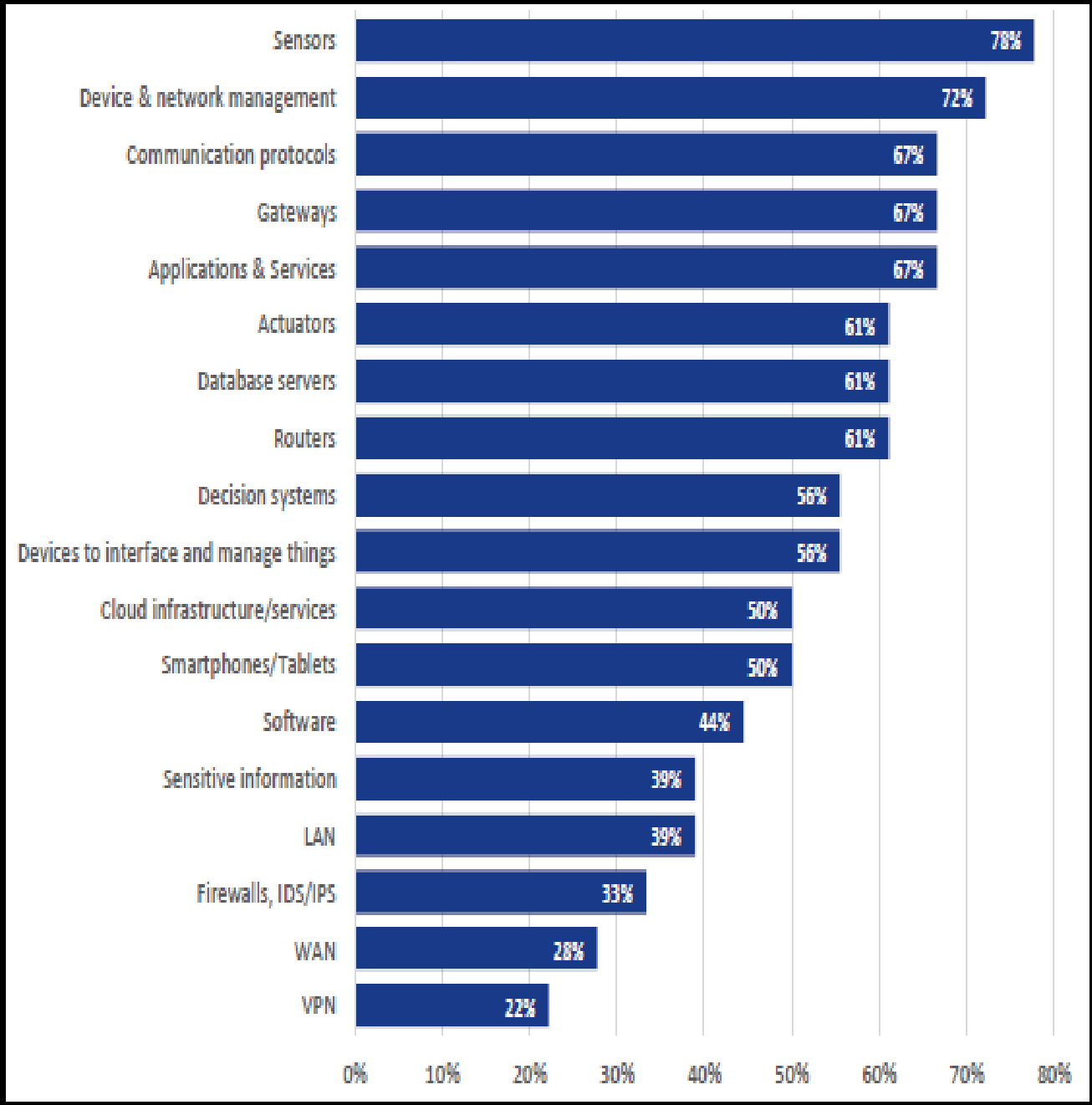


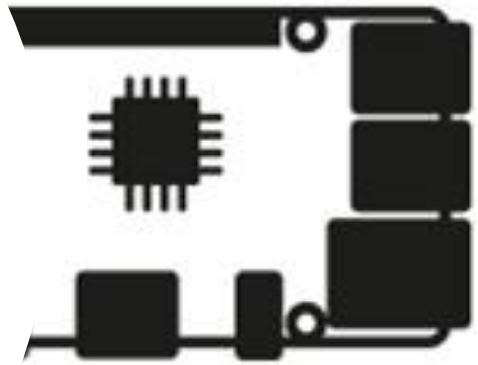

Fig: Asset Criticality (https://www.enisa.europa.eu/ )

# INDICATORS OF COMPROMISE (IOCS)

IOCs serve as a forensic evidence of potential intrusions on a host system or network

- Unusual traffic going in and out of the network
- Network traffic that traverses in unusually used ports
- A Substantial Rise in Database Read Volume
- Large numbers of requests for the same file

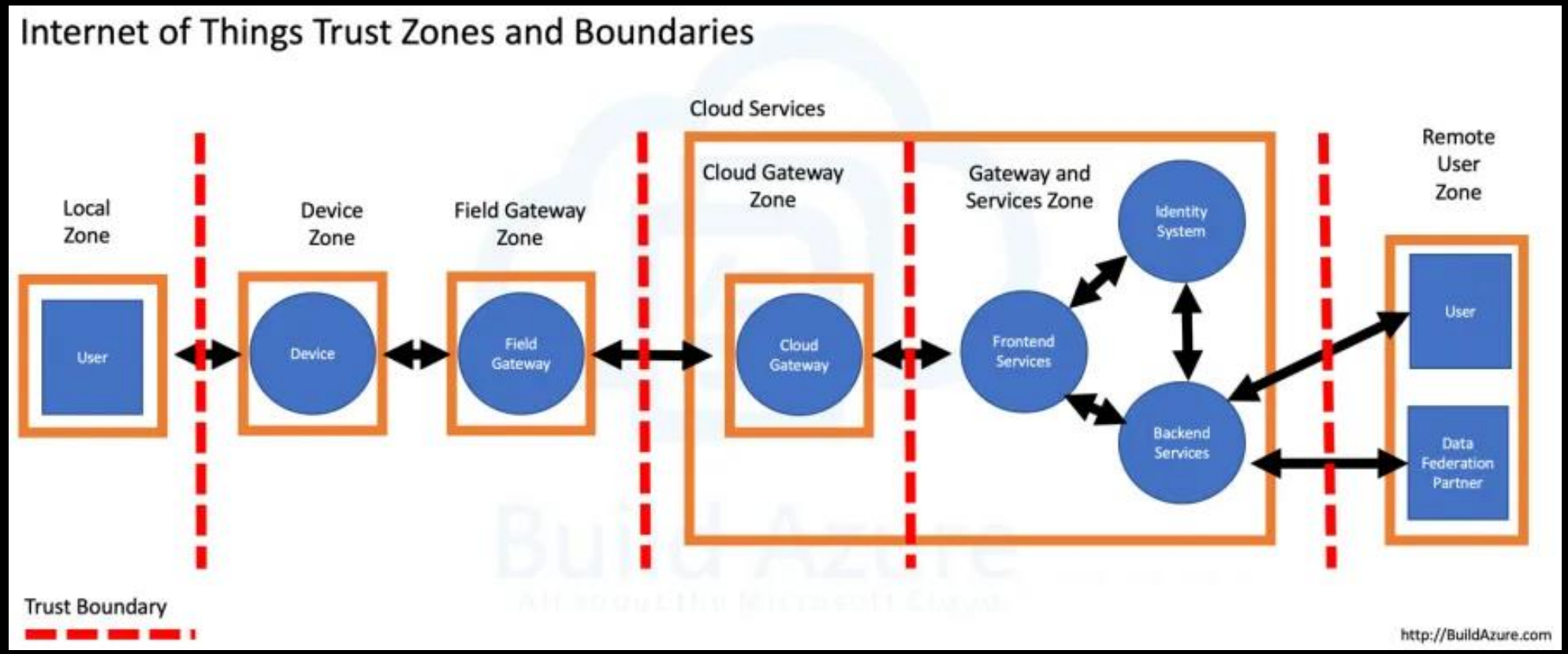
# INTERNET OF THINGS SECURITY



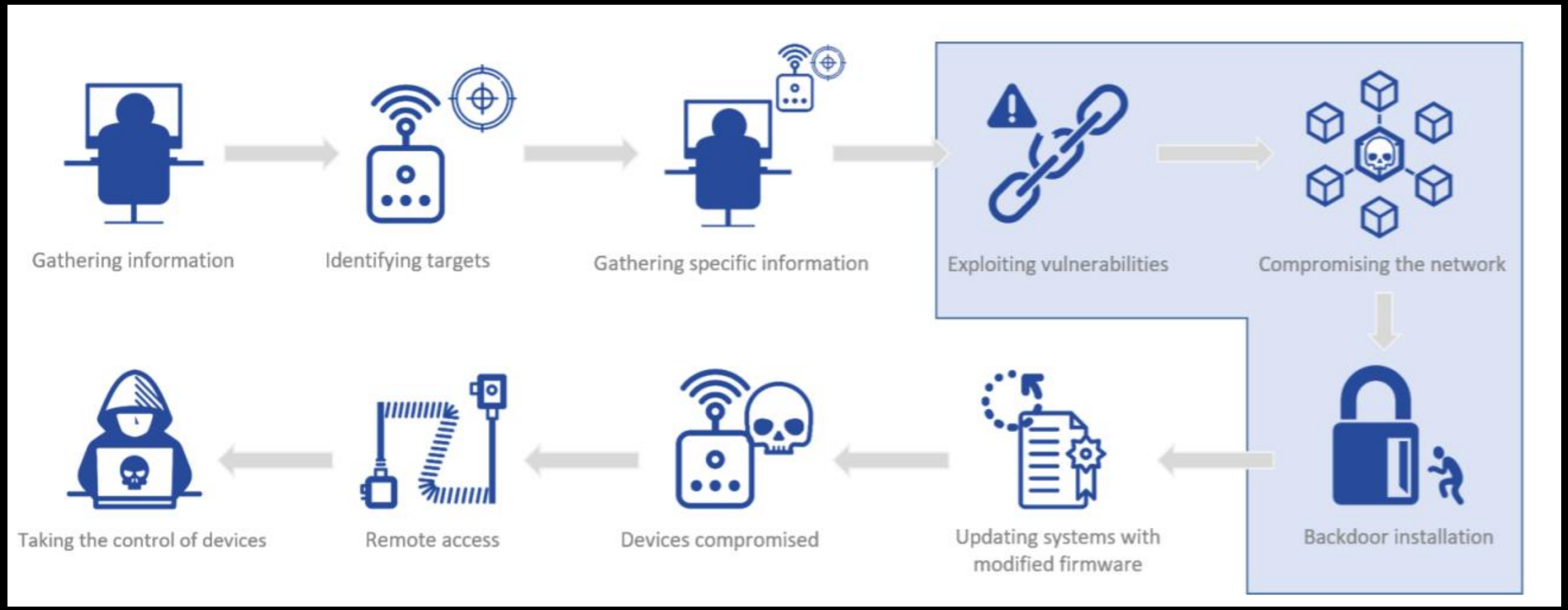
# CHALLENGES IN IOT SECURITY

- Very large attack surface
- Limited device resources
- Fragmentation of standards and regulations
- Lack of expertise
- Unclear liabilities
- Complex ecosystem
- Low cost

# IOT SECURITY TRUST ARCHITECTURE



# GENERAL ATTACK SCENARIO




https://www.enisa.europa.eu/

# BASELINE RECOMMENDATION

- Privacy by design
- Security by design
- Hardware security
- Trust and integrity management
- Data protection and compliance
- System safety and reliability
- Authentication
- Secure software and firmware updates
- Authorisation
- Access control
- Secure and trusted communication
- Secure interfaces and network services
- Monitoring and Auditing

ESW

# WE WOULD LIKE YOU TO,

Design and implement a scheme to maintain the integrity and confidentiality of the data in your project.

This includes,

**PART 1:**

- Selecting a cryptographic algorithm to encrypt the sensed data for confidentiality and privacy

- Selecting  a cryptographic hash algorithm and hashing the data to maintain its integrity

**PART 2:**

- Which cryptographic algorithm works better for your project and why? You may do a latency analysis

# UNDERSTANDING THE DIFFERENCE BETWEEN HASHING AND ENCRYPTION

# WHAT WE WANT WHEN SENDING MESSAGES/DATA ON THE INTERNET?

1.We want to let the other person know that the message has been sent from you-not from anyone else.

2.We want the message to be in the exact same format without any alternation or modification.

3.We want the message to be protected from the reach of ill-intended people-hackers, fraudsters and other types of cyber criminals.

# SO, HOW EXACTLY THIS IS DONE??

These three functions can be designated as:


The answer to achieve these are Hashing and Encryption. Now, you must be thinking 'Doesn't that make them the same thing?,The answer is NO.

# HASHING-###

Hashing protects the integrity of your data. It protects your data against potential alternation.

Basically, a hash is a number that is generated from the text through a hash algorithm.

The algorithm is designed in such a way that no two hashes are the same for two different texts. It is impossible(almost!) to go back from the hash value to the original text.

That's one of the most indispensable properties of Hashing-its uniqueness. There cannot be the same hash value for different text.

Even the tiniest data of change/modification will alter the hash value completely. This is called the Avalanche Effect.

Let's understand this with an example, we have applied the SHA-1 algorithm. Let's see how it goes.

TEXT: Everybody loves burgers

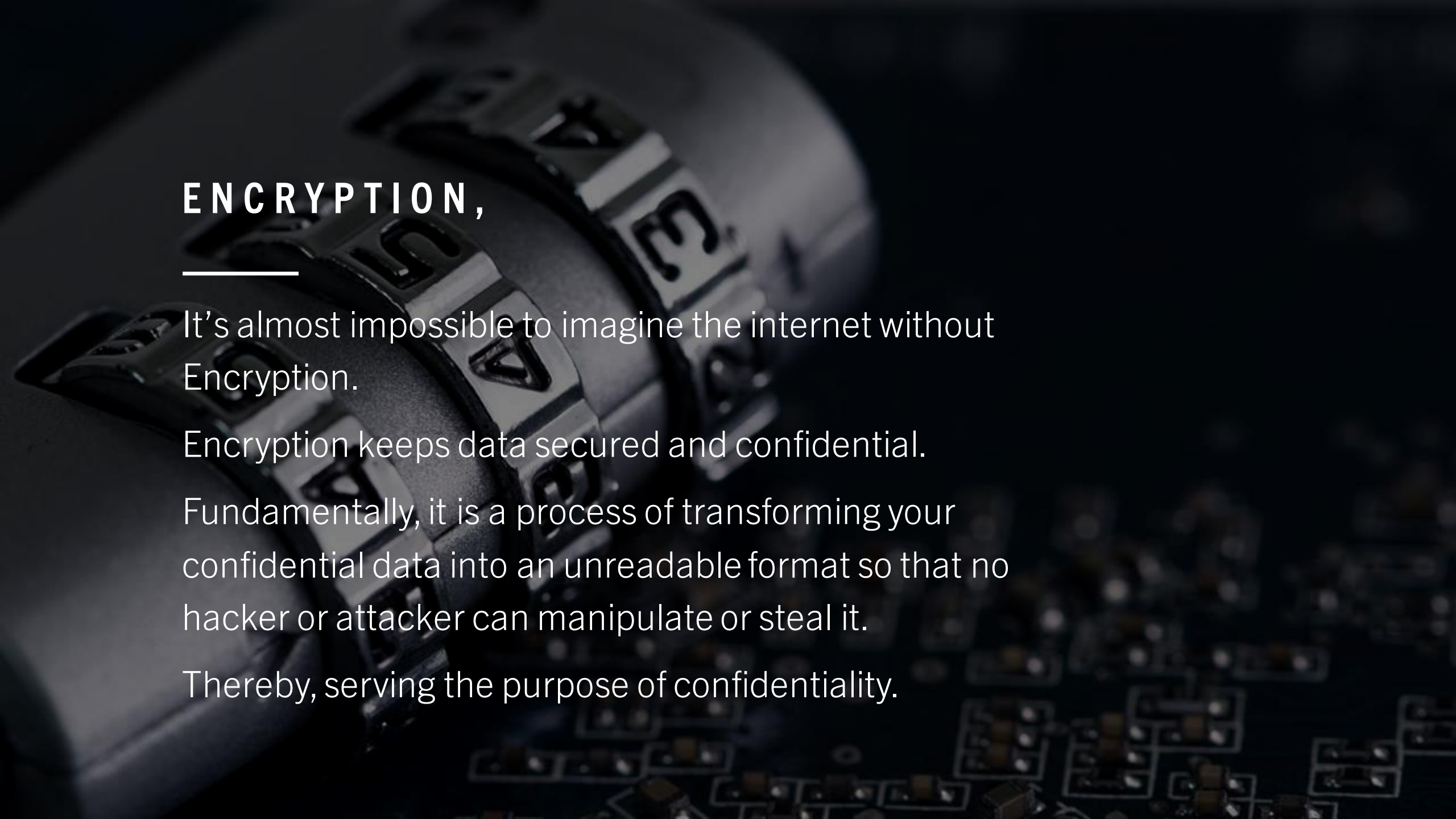
SHA-1 Hash value:369241a7d32854d9aeaa6311145201439d38e587

Now if we make  a tiny bit of change in the sentence above, the hash value will change entirely, let's see how it goes.

New TEXT: everybody loves burger.

SHA-1 Hash Value:0c2c34d28adf91d14938557fb7225ea63ec192c6

See how the hash value changed entirely when we removed the 's' from burgers? That's what hashing does for you.



# ENCRYPTION,

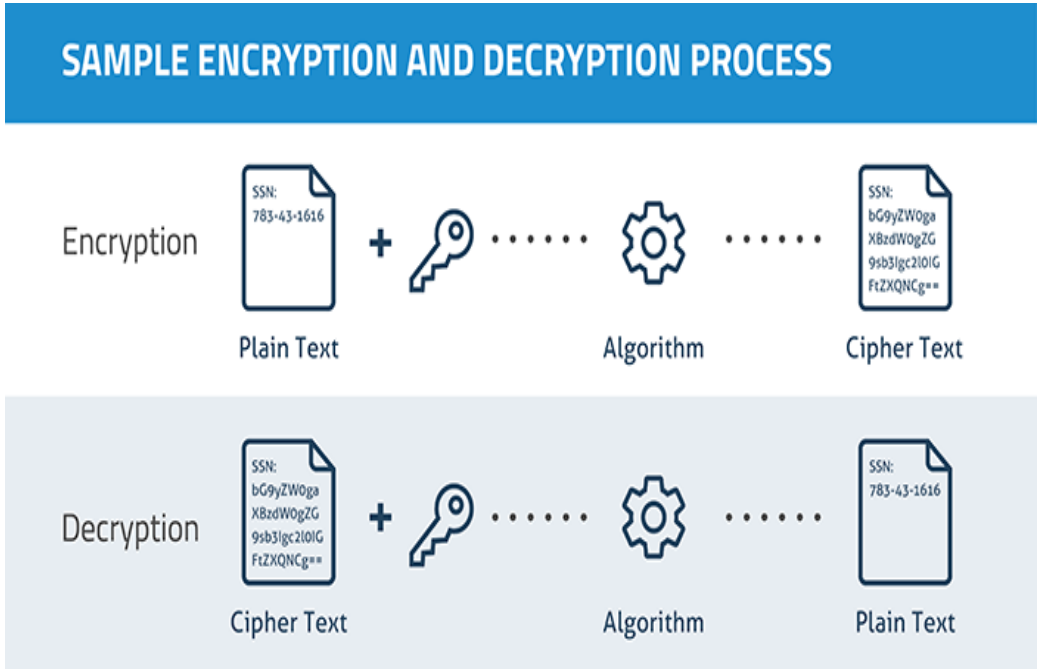
It’s almost impossible to imagine the internet without Encryption.

Encryption keeps data secured and confidential.

Fundamentally, it is a process of transforming your confidential data into an unreadable format so that no hacker or attacker can manipulate or steal it.

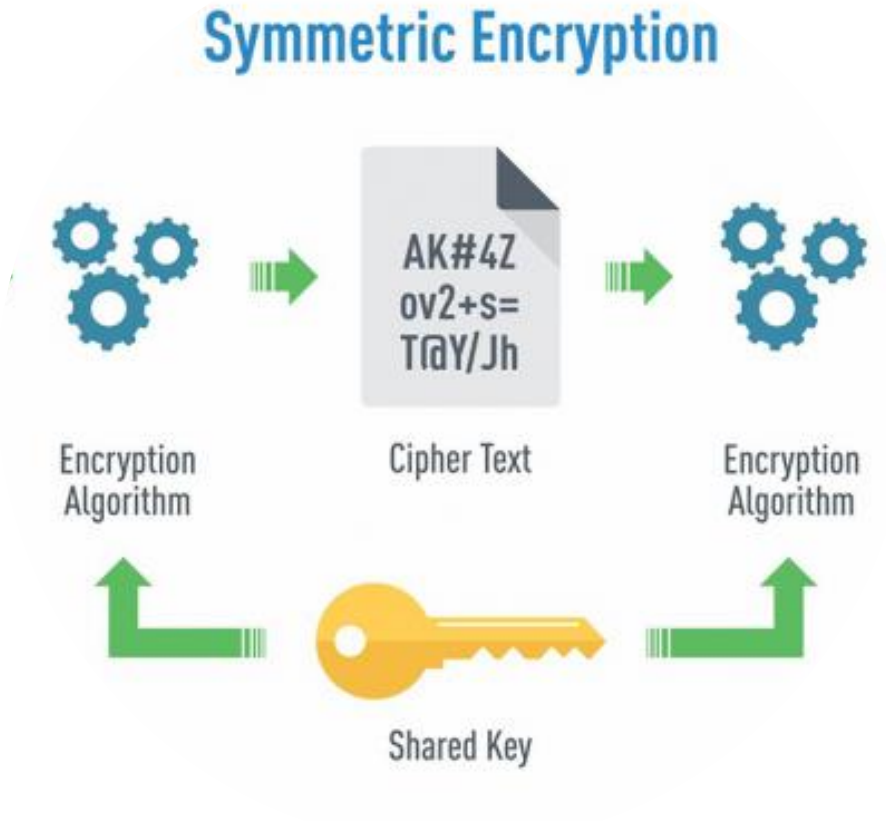
Thereby, serving the purpose of confidentiality.

The encryption of data is executed through cryptographic keys. The information is encrypted before it's send and decrypted by the receiver. Therefore, the data is safe when it is "in the air".



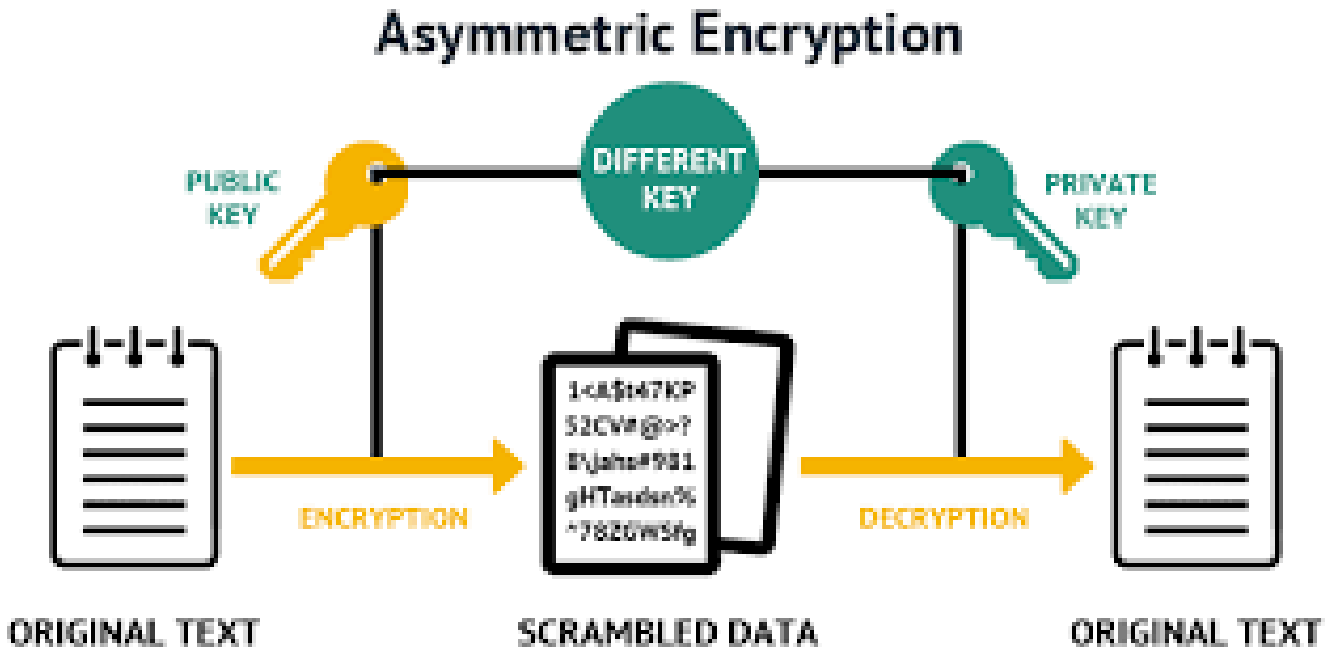
# SYMMETRIC ENCRYPTION

In symmetric encryption, the data is encrypted and decrypted using a single cryptographic key. It means that the key used for that the key used for encryption is used for encryption as well.



# ASYMMETRIC ENCRYPTION

It involves the use of two different keys, one for encryption and one for decryption purposes, one key is known as 'Public key' and the other is regarded as a 'Private key'.



# DEMONSTRATION

Refer to:

- https://nodemcu.readthedocs.io/en/release/modules/crypto/

# DOES IT WORK? HOW DO WE VERIFY? (OPTIONAL)

- Use Wireshark to monitor the network and check the transmitted payload for encryption.
- Comparing the file/data's hash value to a previously calculated value for verifying data integrity

# DEMONSTRATION

Refer to:

- https://www.wireshark.org/

# QUESTIONS TO PONDER (OPTIONAL)

- The cyphertext you generate will not be readable by Thingspeak, thus it will not be able to visualise your cyphertext. How can we solve this challenge?
- Did you know that power analysis provides a way to "see inside" otherwise 'tamperproof' hardware? You can find out which cryptographic algorithm is being used through variations in power consumption. Tutorial: https://www.youtube.com/watch?v=bFfyROX7V0s