BLOG

128 REASONS TO ENCRYPT DATA IN IOT

The process that ensures secure data transmission is reliant on a robust and reliable data encryption to be transmitted between different platforms/devices.

The value of information and its privacy is a theme that is hundreds of years old. Proof of this are the message encryption systems designed by our ancestors, in times where data flow was much lower than today and where the technology index was widely reduced.

Probably the encryption system which became pioneer in its days was the Enigma machine, used by the germans in World War 2 to protect the content of their communications. Since then data protections methodologies have progressed on an upward scale in various contexts to encryption used in the digital age.

VISION

Massive amounts of data are generated daily by a plethora of devices across the globe. The unambiguous globalization of the network means that established communications tend to be as secure as possible to ensure the reliability of information and compliance with data privacy policies of entities and individuals and enable users to enjoy a safer online experience. The data floats through the most diverse types of networks, resulting in a clear exposure of the information to whom intentionally or unintentionally can access it. The process that ensure secure data transmission is reliant on a robust and reliable encryption of data to be transmitted between different platforms/devices, through complex encryption algorithms, engender to move all kinds of information.

AES – WHAT IT IS?

The **Advanced Encryption Standard** (AES) data encryption algorithm was developed between 1997 and 2001 by the **National Institute of Standards and Technology** (NIST) following the search for a successor to the Data Encryption Standard (DES) encryption block witnessing a deterioration of its capabilities as a result of technological progress. Following the assessment of the AES encryption system and performance tests, its inclusion in technology systems of entities such as the **National Security Agency**, commonly referred by its acronym NSA and the **United States of America Government**, pointed the confidence placed in this algorithm and its statement as a process of increasing security in data transmission.

AES is a globally used standard encryption algorithm for data protection that supports 128, 192, 256 bits long keys. It is defined as a symmetric block cipher system. What's different about asymmetric blocks? Briefly, it turns the encryption and decryption process faster due to the low use of computational resources and is based on the application of the same key for encryption and decryption of the message.

Choosing the encryption key sets how many rounds will be needed to pass the plaintext through the cipher and result in the encrypted text. 128-bit keys require 10 rounds, while the 192-bit keys require 12 rounds and a 256-bit keys will require 14 rounds. How longer the selected key, more secure the encryption becomes. However, the process requires more time to complete in both encryption and decryption processes.

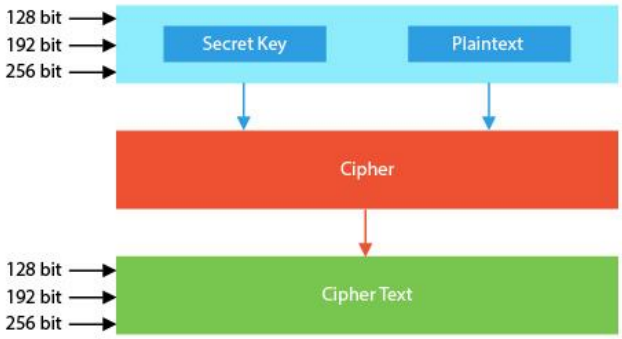

Figure 1 - AES encryption graphic scheme

Some common uses of AES algorithm:

- VPN's (example: **ExpressVPN** - uses 256-bit AES encryption for channel control);

- Compression tools (example: **WinRAR** - uses 256-bit AES encryption for compressed file passwords);

- Messages applications (example: **WhatsApp** - uses 256-bit encryption for media file transfer);

To experiment the application of AES encryption algorithm, DevGlan has developed an **online tool** that enable to simulate the encoding and decoding of information. We can gauge the complexity of encrypted information and how easily it can be decrypted by having access to the required decryption features.

SECURE WIRELESS COMMUNICATION

Globally, we see an increase in sensor application for monitoring critical environments and controlling applications in wireless networks. Gathered data at different terminals should remain readable only to their recipients to avoid misuse of information that may indirectly reveal other data. A case study is the example of the privacy policy implemented by the NSA, which does not publish the energy consumption information of its data centers in order to protect the possible estimation of computing resources used.

The information protection provided by wireless connections has been subject of almost daily scrutiny, a discussion caused around the news about security breaches in wireless networks triggered by numerous computer attacks. Yet, there are still more properly secured connections than those that are not. It is a matter of media notoriety. The vulnerability of wireless networks is overcome with the deployment of increased security measures that have almost all guaranteed correct and reliable use.

As an organization distinguished by its commitment to research and development of wireless solutions, the security and privacy of data collected are for **Tekon Electronics** an added value that implements in its wireless solutions with the purpose of providing a safe effort to be implemented in the industrial sphere. Data accuracy in **Industry 4.0** promotes the application of robust security measures for data transmission.

DUOS and **PLUS** wireless product families built on the **Internet of Things** (IoT) technology concept shift the responsibility of data protection to their communication process across platforms. The encrypting process of collected data by sensors installed on transmitters until the communication with the gateway is ensured by using the AES algorithm with the 128-bit long key.

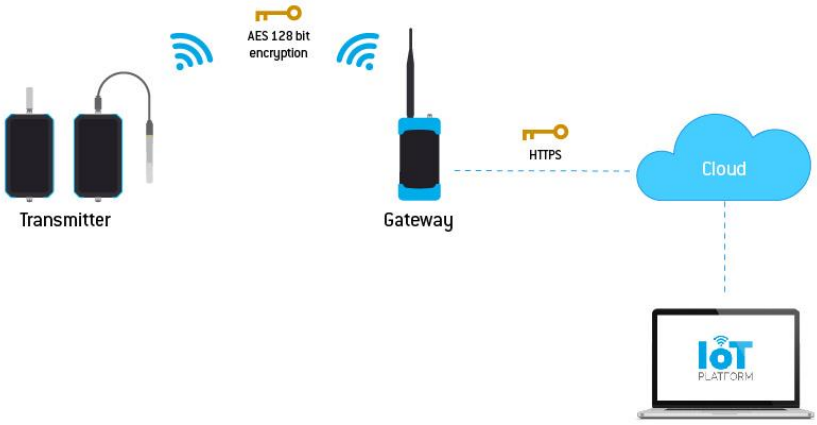

Figure 2 - Graphic demonstration of Tekon Electronics wireless device encryption

The initiative of complete planning and development of the device solution and **IoT** platform, instils **Tekon Electronics** with the task of ensuring right and reliable communication between our devices and the information sharing cloud. The subsequent transfer of information results from the responsibility of security systems defined by third parties, as they no longer fit into the typologies directly related to the practical use of wireless solutions.

FINAL CONCLUSIONS

Data encryption remains a major topic in one of the increasingly attention-grabbing procedures - **data security**. The rightful focus of these systems is synonymous with the value they add to organizations, highlighting their use in the modernization of industry and production processes. Developing technology products with the aim of providing a high level of data transmission security continues to highlight IoT products and services in the competitive global marketplace.

The lack of valid records that indicate some vulnerability of the **AES** encryption algorithm has contributed to the solidification of the reliance placed in this solution, which remains a choice by reference entities in the assorted technological applications in our daily lives.