Tishk International University
Science Faculty
IT Department

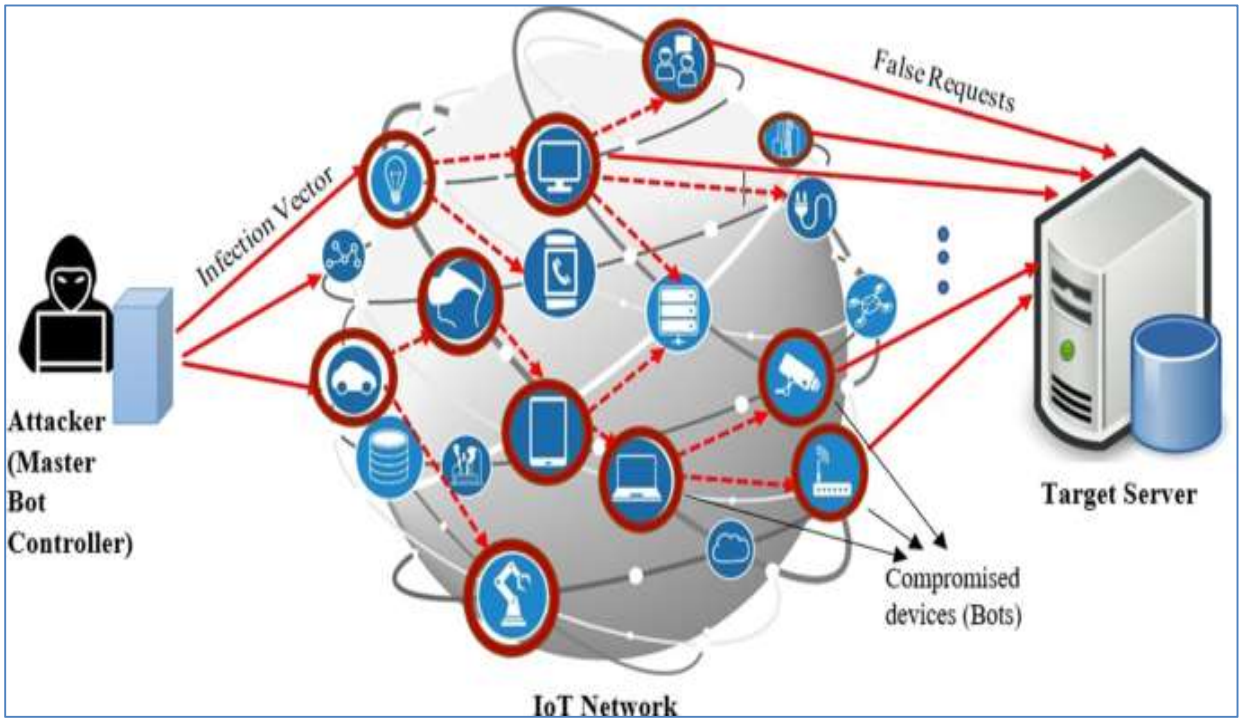
Introduction to IoT

Lecture 05: IoT Security

4th Grade - Spring Semester

Instructor: Alaa Ghazi

Lecture 4
IoT Security



Lecture Topics

- ❑ Why Securing IoT Things?
- ❑ Key IoT Security Challenges
- ❑ Effective Solutions for IoT Security Challenges
- ❑ IoT Device Firmware
- ❑ Why Over The Air Updates?
- ❑ IoT Firmware OTA Update Architecture
- ❑ IoT OTA Operations
- ❑ Problems and Solutions for OTA Updating
- ❑ IoT Cloud Security Considerations

Why Securing IoT Things?

- According to Statista, the number of IoT devices worldwide is over 15.9 billion in 2023. It is expected to reach more than 32.1 billion IoT devices by 2030. From this, we can expect that the demand for IoT integration is going to rise at a rapid speed.
- However, with the rising need for IoT, here comes a critical question: How secure are these Internet-connected devices?
- The Internet of Things includes a network of interconnected machines that collect and have a lot of data. Although IoT-connected devices are convenient and efficient, there are multiple security concerns that you must address. It is crucial to tackle IoT security challenges to protect the integrity of the data collected by these IoT devices.
- So, as IT specialists, we must understand and mitigate these challenges.

Key IoT Security Challenges

1- Weak Authentication and Authorization: IoT devices often rely on weak authentication and authorization practices, which makes them vulnerable to threats. For example, many devices use default passwords making it easier for hackers to gain access to IoT devices and the networks they use for communication. In addition, rogue IoT devices (i.e., undetected) that are connected to the network can be used to steal data or launch attacks.

2- Lack of encryption: The majority of IoT device network traffic is unencrypted making confidential and personal data vulnerable to a malware attack such as ransomware or other form of data breach or theft. This includes IoT devices used for medical imaging and patient monitoring, as well as security cameras and printers.

3- Vulnerabilities in firmware and software: The short development cycles and low price points of IoT devices limit the budget for developing and testing secure firmware. Without this built-in IoT security, IoT devices are vulnerable to the most elementary forms of attack.

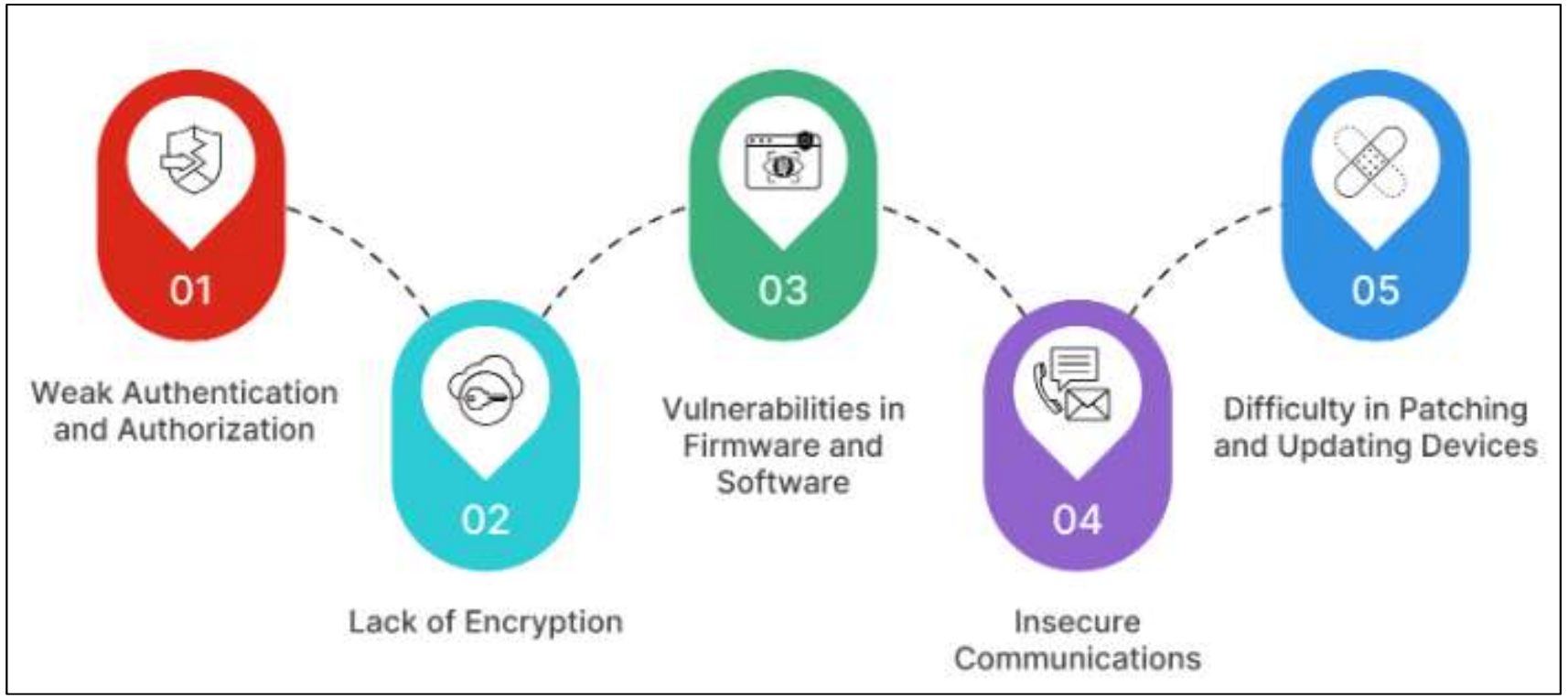
Key IoT Security Challenges

4- Insecure communications protocols and channels: IoT devices are often connected to the same network as other devices, which means that an attack on one device can spread to others. Lack of network segmentation and oversight of the ways IoT devices communicate makes them easier to intercept.

For example, the automotive industry's adoption of Bluetooth technology in IoT devices resulted in a lot of data breaches, as well, protocols like HTTP (Hypertext Transfer Protocol) and API–are all channels that IoT devices rely on and cyber criminals can exploit.

5- Difficulty in patching and updating devices: IoT manufacturers don't focus on building IoT security into their devices to make hardware tamper proof and secure. Many IoT devices are not designed to receive regular IoT security updates, which makes them vulnerable to attacks. Without built-in IoT security it's difficult to ensure secure upgrades, provide firmware updates and patches, and perform dynamic testing.

Key IoT Security Challenges Diagram



Effective Solutions for IoT Security Challenges

1- Implement Strong Authentication Mechanisms:

To handle weak authentication, a multi-factor authentication (MFA) and even robust password policies can be used. By doing this, only authorized users and devices can access IoT networks and have sensitive data. Also a biometric authentication to add an extra layer of security can be implemented.

2- Encryption:

Covered in Information Security Course.

Effective Solutions for IoT Security Challenges

3- Implement Device and Network Monitoring:

Continuously monitoring your device and network is crucial to maintaining IoT ecosystems' security and integrity. You can monitor unusual or suspicious activities. Business owners can quickly identify and respond to potential threats by monitoring network traffic. As IoT devices handle more personal data, it's important to consider how users give permission.

There are several tools such as Intrusion Detection Systems(IDS) and security information and event management (SIEM) solutions to gather, analyze data and prevent unauthorized access. By utilizing these resources effectively, you can identify and respond to threats in real-time.

Effective Solutions for IoT Security Challenges

4- Regular Firmware and Software Updates:

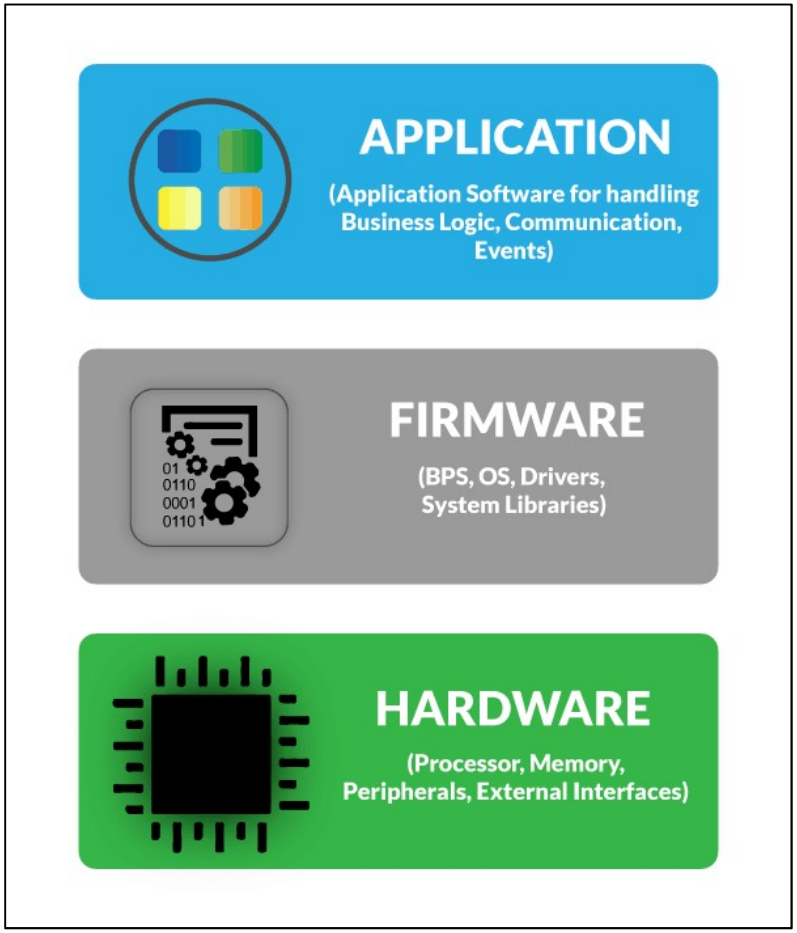
Regular updates are important due to the following reasons:

- Updates can provide patches to fix vulnerabilities and prevent potential exploitation by attackers. Without timely updates, your IoT devices may be exposed to several threats and hackers can easily target your system.
- Firmware and software updates can fix bugs easily. It ensures that your device will operate smoothly.
- To optimize the performance of IoT devices, you need to enhance your firmware. It will improve battery life, and processing speed and will provide a better user experience.

IoT Device Firmware

The components of an IoT device can be split up as a three-layered stack starting from the base, comprising of hardware, firmware and application.

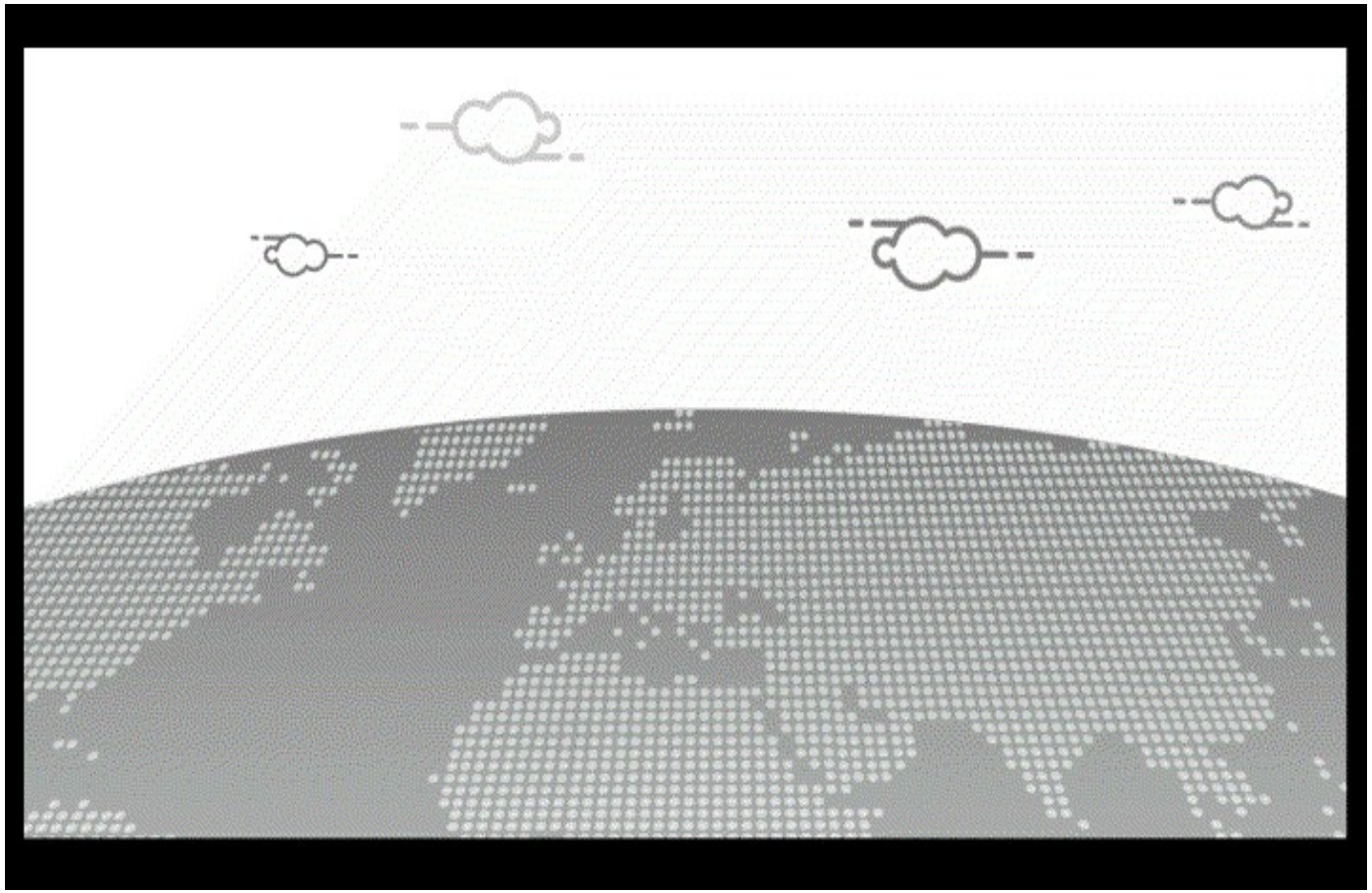
The IoT firmware is a piece of code that resides in a non-volatile part of the device that allows and enables the device to perform the functions for which it was created. It consists of several **components**, such as the **kernel**, **bootloader**, **filesystem** and additional resources. In addition, the firmware makes various hardware components work properly.



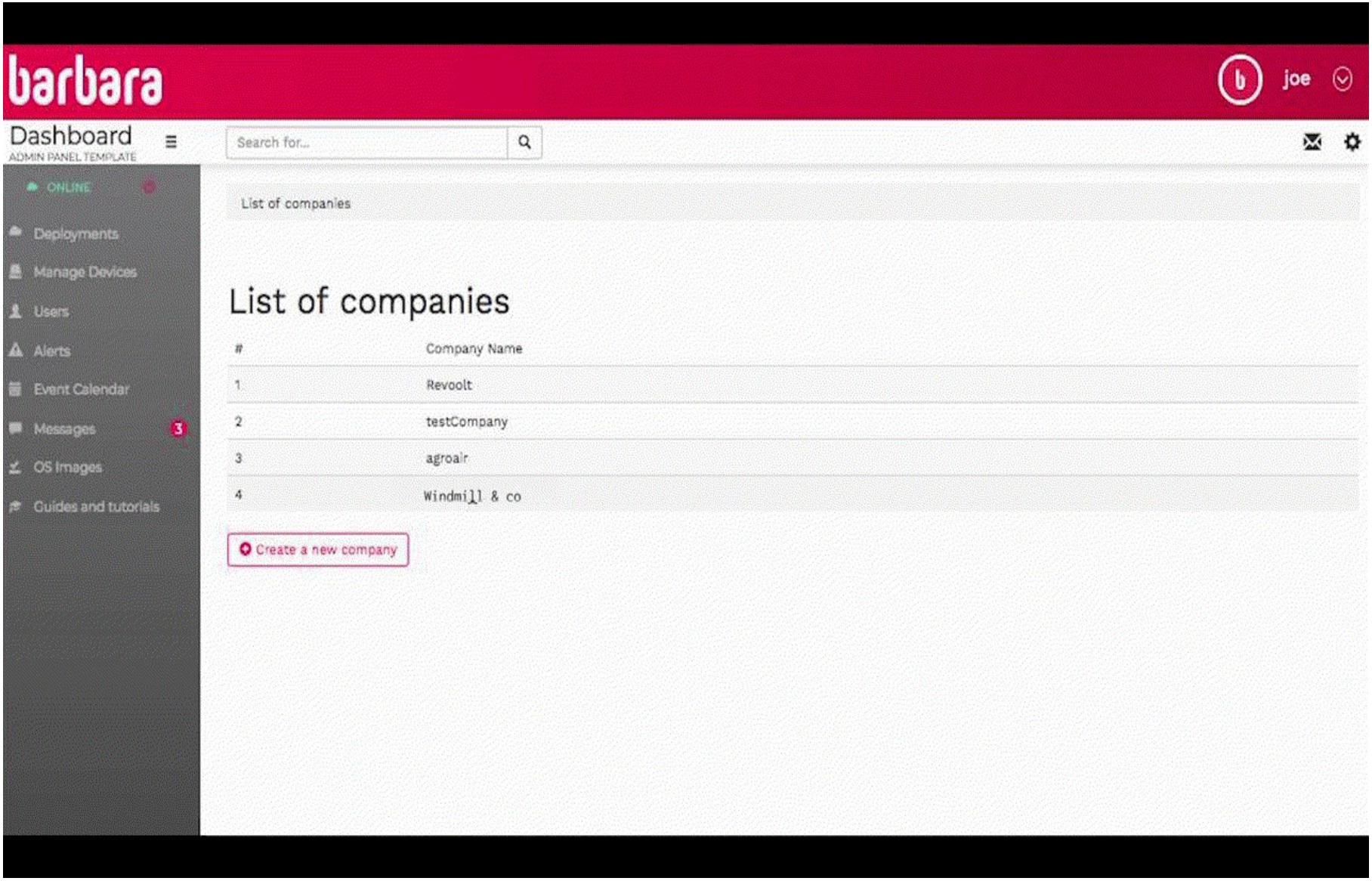
Why Over The Air Updates?

Updating the devices manually on the field is an expensive process since operator has to perform them physically.

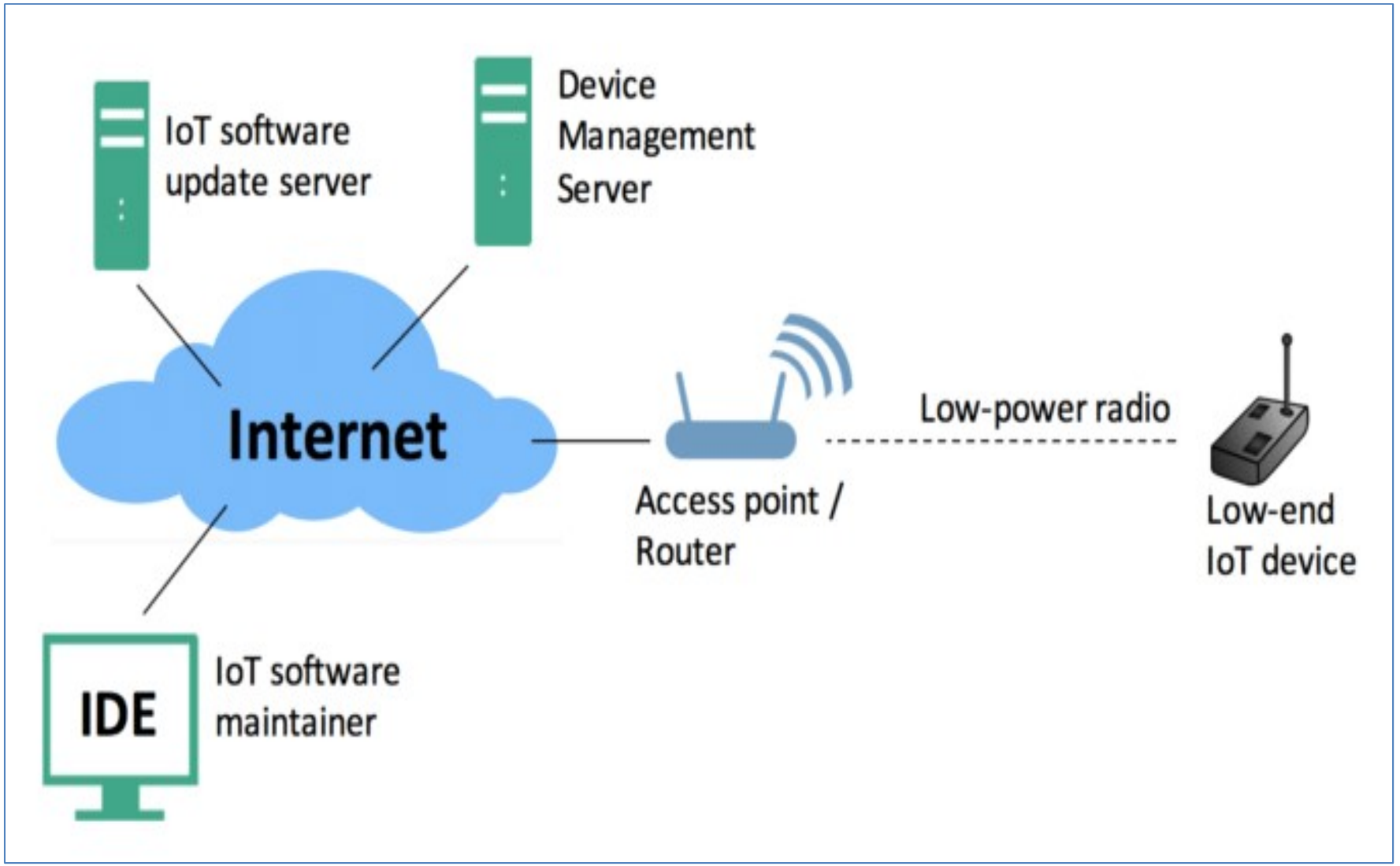
Over The Air (OTA) updates ensures quick smooth and secure update for hundreds of IoT devices.



IoT OTA Update – A Demo



IoT OTA Firmware Update Architecture



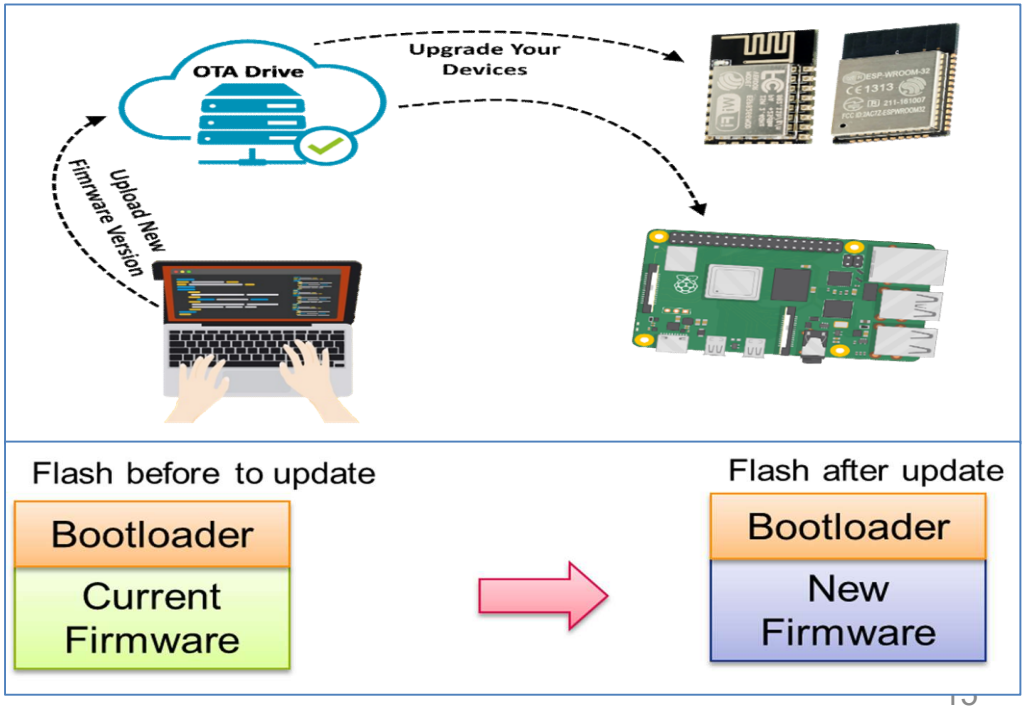
IoT OTA Operations

An IoT device is connected through a low-power wireless network to a device management server, which runs on the Internet.

Over the lifetime of this IoT device, an authorized IoT software maintainer should be able to:

1) Produce firmware updates

2) Trigger the device to fetch (via push or pull) and the firmware image, and then reboot.



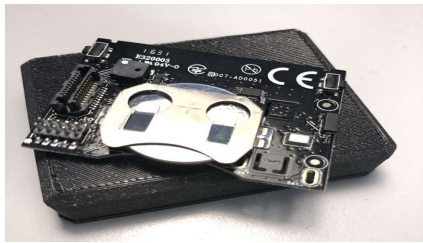
Problems and Solutions for OTA Updating

Problem 1 : Limited memory and processing power

IoT nodes are restricted embedded devices with limited memory and processing power. To address this limitation, lightweight algorithms in software as well as hardware-based acceleration of cryptographic operations should be considered.

Problem 2 : Battery Powered

IoT nodes are often battery-operated, thus constrained in terms of energy. The total power consumption is significantly affected by the size of the data to be stored, and for this reason, firmware update size minimization is of utmost importance.



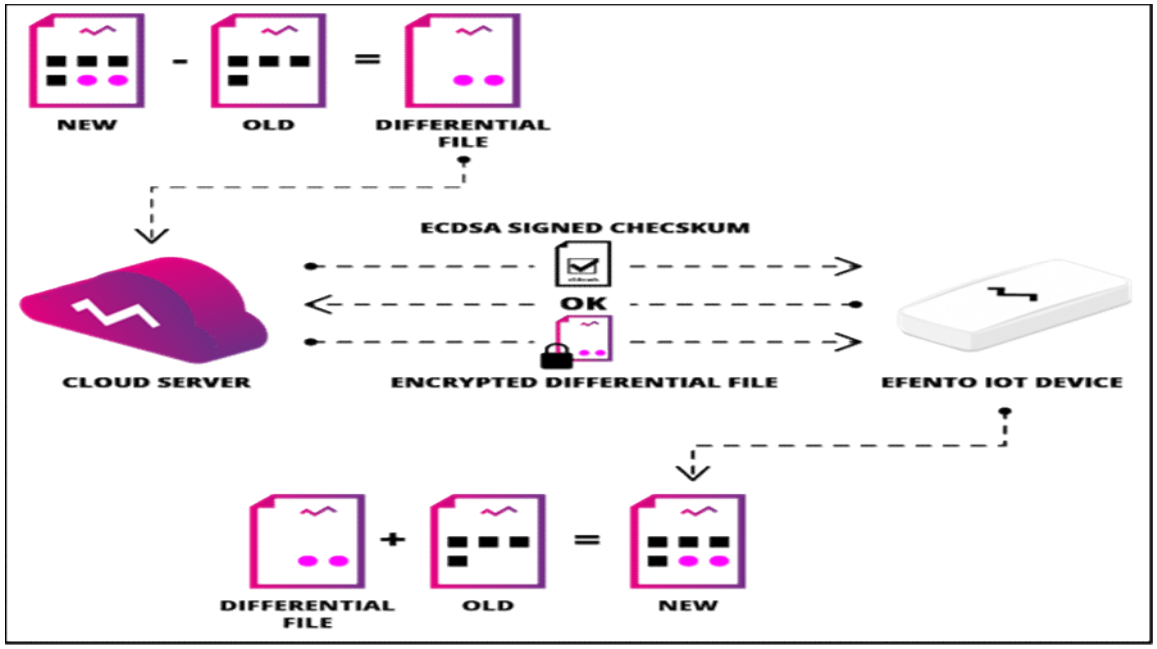
Problems and Solutions for OTA Updating

Solution 1 & 2: Differential Updates

1. After completing the work on the new version of the software, a differential file that is the difference between the new and current versions of the software is pushed to the cloud server.

2. The cloud server notifies IoT devices about the available update.

3. The IoT device pull the differential file and add it to the current firmware to generate the new firmware.



Problems and Solutions for OTA Updating

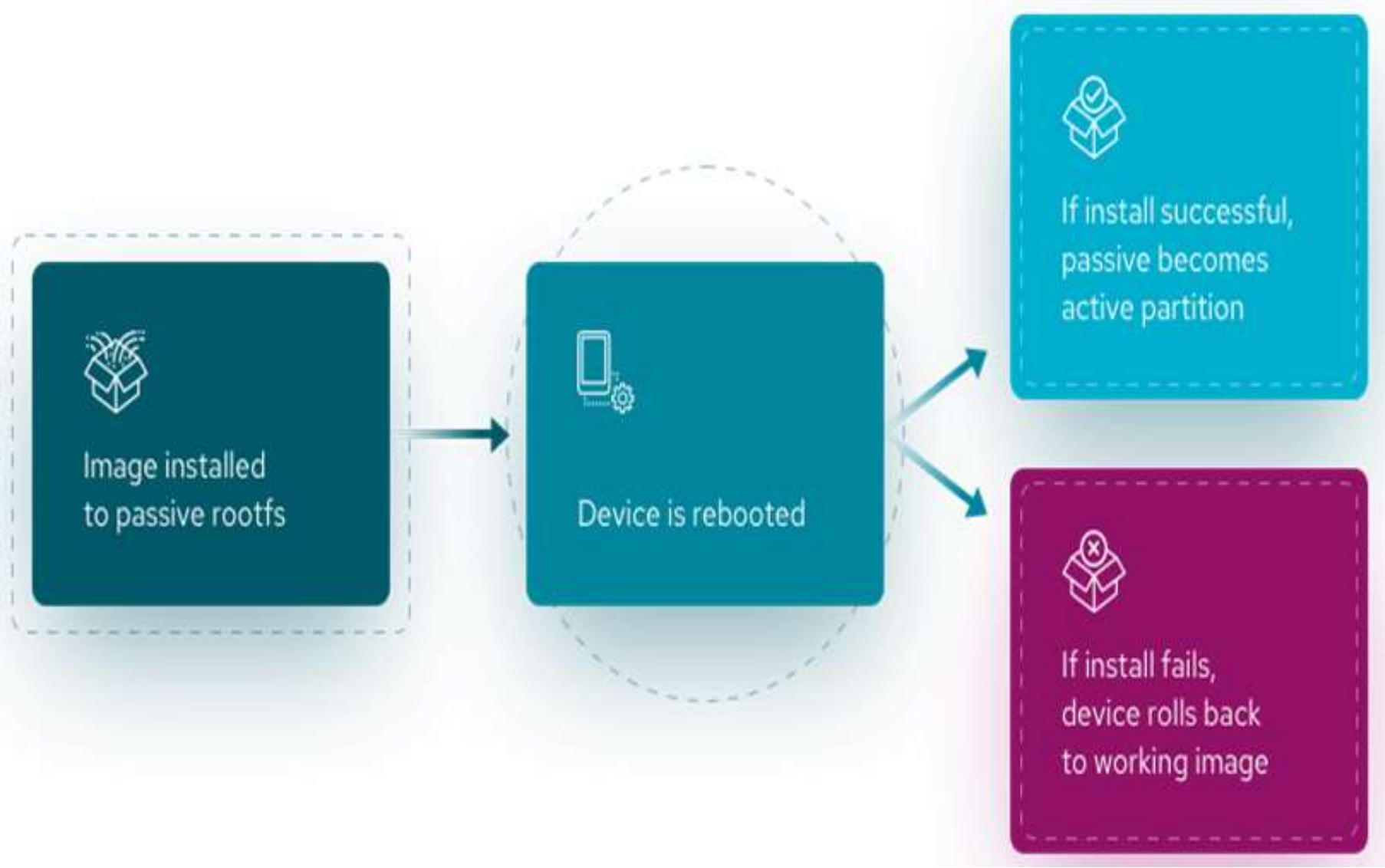
Problem 3: Firmware Update Failure

Traditionally, in-place approach has been used. In this method, the microcontroller only stores one firmware image, which might occupy all the available flash memory. In this case the update cannot be done while the microcontroller is running and if the update process did not finish correctly it can be difficult to recover the old image

Solution 3: Dual Firmware

1. Update to the new firmware
2. Test The new firmware operation
3. If successful keep it
4. If not successful return to old firmware

IoT Device Dual Firmware Update



Problems and Solutions for OTA Updating

Problem 4: Flash memory degradation

Caused by the large number of erase and write operations during an update. When the erase threshold of a block has been reached, it is marked as a bad block and cannot be used in the future, thus limiting the available storage.

Solution 4: Use The storage blocks evenly

In order to increase the lifetime of flash memory, a new firmware image has to be stored in a smart way, so one can achieve a uniform and smooth degradation of the available blocks.

Problems and Solutions for OTA Updating

Problem 5- Malware is injected in the firmware during the update

Many attacks have already taken place having compromised thousands of IoT devices around the world, an attacker can demonstrate large-scale DDoS attacks against critical infrastructures; It is of importance IoT nodes to be supported by a secure OTA mechanism.

Hackers have targeted platform firmware as a place to embed malware and hide other malicious code that can ultimately compromise a system

ZigBee Worm was able to trigger a chain reaction of infections, initialized by a single compromised IoT device (light bulb), using a malicious firmware update image.

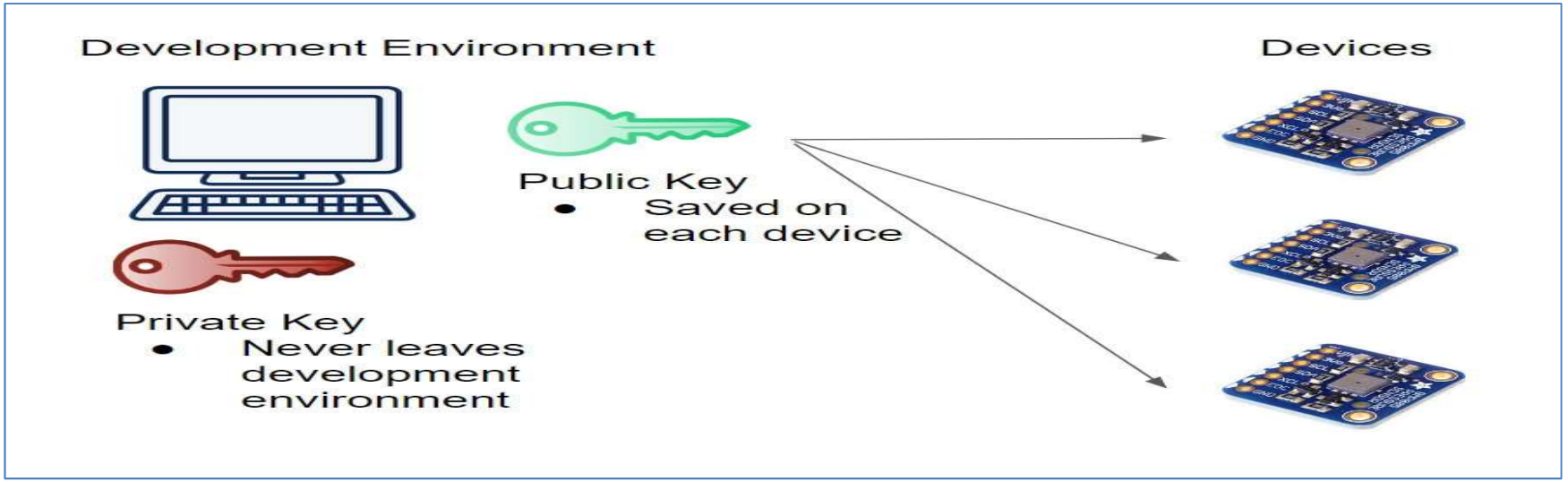
Problems and Solutions for OTA Updating

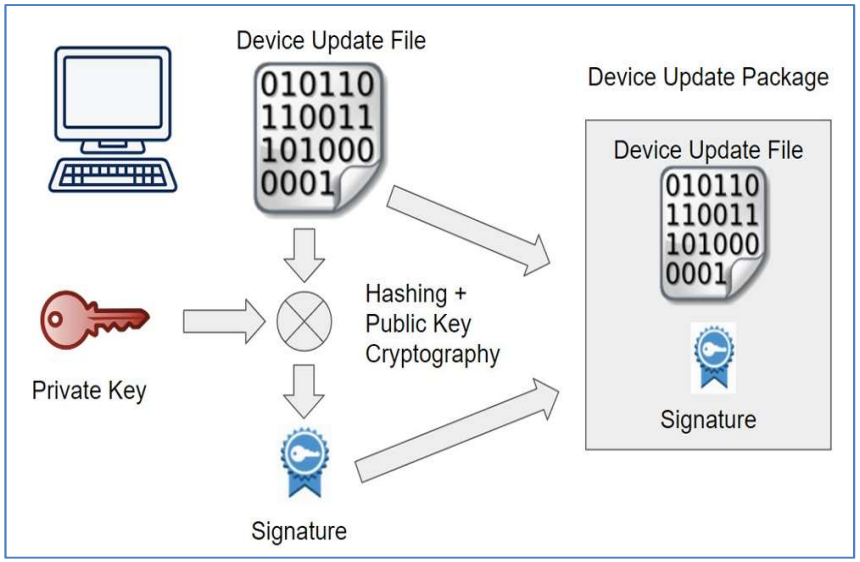
Solution 5- Digital Signature for the Firmware Update

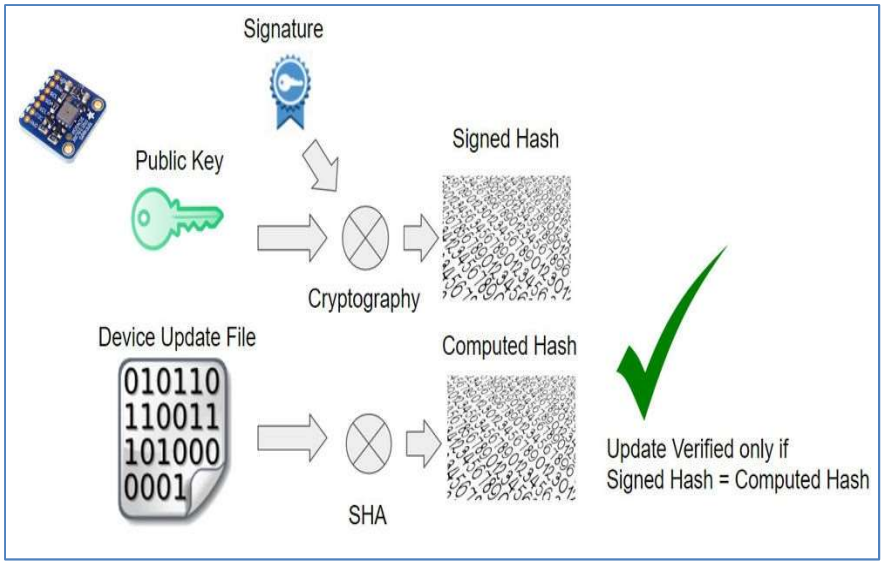
The main security challenge is ensuring that an update has not been tampered with in-transit to the IoT device and that the update originates from the expected update servers. The solution is to digitally sign the firmware by the vendor, as explained in below procedures:

1. The vendor must better secure their update servers to avoid replacing valid firmware with malicious firmware.
2. The vendor must include its public key in the initial IoT device firmware.
3. The IoT device should include cryptography-enabled microcontrollers.
4. Each firmware update must be digitally signed by the vendor's public key, and the digital signature must be attached to the firmware before transmission.
5. After receiving the new firmware, the IoT device must verify the firmware signature before applying the new firmware.

OTA Secure Update Diagram







IoT Cloud Security Considerations

- **Device Authentication:** Use strong authentication mechanisms, such as certificates or tokens, to verify the identity of devices connecting to the system securely.
- **Data Encryption:** Encrypt data in transit and in the storage to prevent unauthorized access and protect sensitive information from potential breaches and hackers.
- **Access Control:** Implement strict access control policies to limit user privileges and prevent unauthorized access to system resources and configurations immediately.
- **Regular Updates:** Keep all system components, including IoT Cloud Application and MQTT broker, up to date with the latest security patches to mitigate vulnerabilities.
- **Network Security:** Use firewalls, intrusion detection systems, and VPNs to protect the network infrastructure from external threats and unauthorized access at once.