

# ME5100

## IoT Cloud and Device Security Management

*dream*  
CATCHER

"Complete Resources for Lecturers"

**KEYSIGHT**  
TECHNOLOGIES

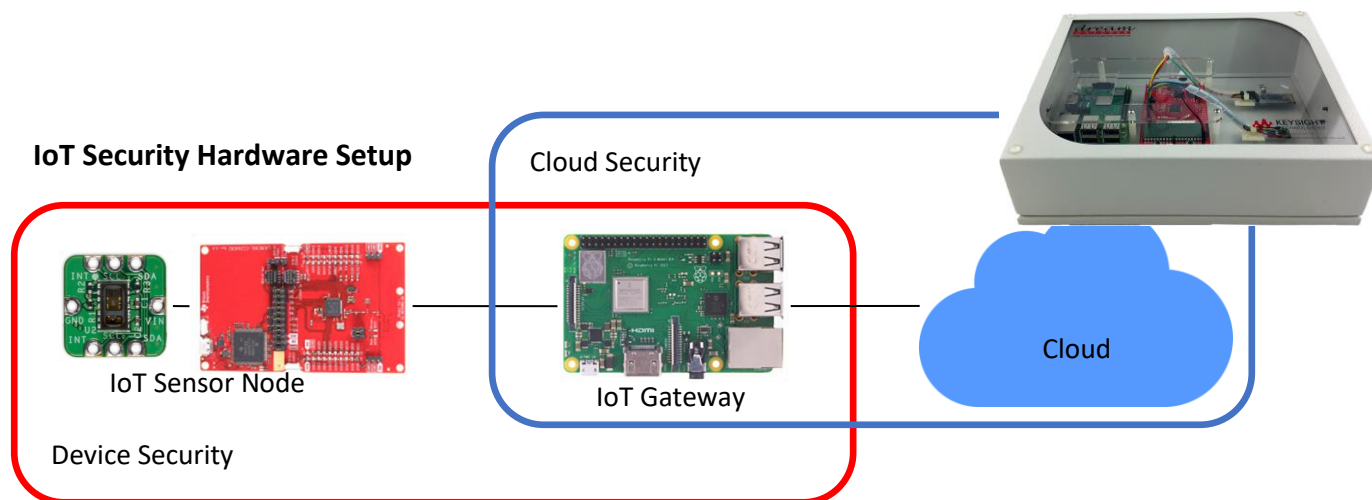
Solutions Partner  
Extending our solutions to meet your needs

### Teaching slides

- Editable Microsoft® PowerPoint® slides
- Covers 40+ hours of classroom sessions

### Training kit

- IoT development kit: gateway & Sensor Node
- Lab sheets (MS Word) and model answers
- Problem-based learning assignments
- Covers 18 hours of lab sessions



| Target university subject  | Target year of study                              | Prerequisite(s)   |
|--|---|---|
| IoT Device and Security Management<br>IoT Cloud and Device Security<br>Privacy and Security in IoT | 3 <sup>rd</sup> year to final year undergraduates | Introduction to IoT<br>C Programming<br>Embedded System Programming |

The ME5100 serves as a ready-to-teach package in the area of Internet-of-Things (IoT) focusing on device and security management of an IoT system.

### Learning Outcomes

Students would be able to:

- Describe various IoT cloud technologies that support IoT applications
- Configure and manage the IoT applications using cloud technologies
- Understand the challenges of cloud and security management when deploying IoT applications
- Deploy cryptography in IoT after understanding the theoretical background of cryptography algorithms
- Implement security features into IoT applications
- Gain practical exposure to application of advanced cryptosystem in IoT context

### Benefits of the ME5100 courseware

- The development kit consists of an IoT gateway (Raspberry Pi) and IoT sensor nodes (TI CC2640R2F) can be program and configure to form an IoT end-to-end system.
- Setup and manage a complete IoT system, which consists of the sensor node, gateway, and cloud service.
- Manage IoT cloud server performance and server security.
- Practical exposure to secure IoT communication between sensor node and gateway through encryption and decryption.
- Implement efficient cryptography algorithms on a resource-constrained sensor node (TI CC2640R2F).
- Use cryptosystem to protect the privacy of IoT applications users.



# Teaching Slides

(PN: ME5100-100)

Editable slides, covering 40+ hours of teaching for one full semester are provided. The slides cover the following topics:

## Overview of Internet-of-Things (IoT) System

Introduction to the architecture of an IoT system. Applications of IoT and future trend. IoT building blocks and enabling technologies. Common IoT software and hardware architecture.

## Communication Management using MQTT and MQTT-SN

This will cover MQTT protocol in detail and includes all the functionalities of MQTT broker. In addition to that, it includes MQTT performance monitoring and also understanding the limitation of MQTT.

## IoT-Gateway Architecture

This will cover various IoT-Gateway Architecture and the potential roles of an IoT-Gateway. This includes the importance of having remote kill switch in Sensor Node and IoT-Gateway.

## Cloud Server and Security Management.

Server management, not limited to performance monitoring. This includes firewall configuration and secure log analysis to identify potential attack.

## Security Challenges for IoT Applications.

Security problems faced by IoT applications. Overview of potential attack scenario. Security target to be achieved in common IoT applications (e.g., data confidentiality, integrity, authenticity and privacy preservation).

## Public and Secret Key Cryptography

Differences between public and secret key cryptography.

*Public Key:* Mathematical background for Public Key Cryptography (PKC). Using PKC for encryption/decryption, key exchange and digital signature. Overview of RSA and Elliptic Curve Cryptography (ECC).

*Secret Key:* Block ciphers for encryption/decryption. Cryptographic hash function for integrity check and authentication (HMAC). Overview of AES and SHA-3.

## Privacy Preserving Computation in IoT

Data processing in encrypted domain. Partial homomorphic encryption: Paillier and ElGamal Cryptosystem. Overview of application scenario.

## Implementing Security in IoT System

Overview of TLS/SSL protocol. The importance of efficient code for cryptography algorithms. Efficient implementation of RSA.

Overview of side channel attack (simple power analysis) and its countermeasure.

## Case Studies:

- i) Comparing various IoT architectures against its application scenario (gateway vs gateway-less architecture)
- ii) Security issues with wearable devices and its countermeasures
- iii) Privacy preserving smart metering system in household area
- iv) Secure machine-to-machine (M2M) communication for smart manufacturing



# Training Kit

(PN: ME5100-200)

## IoT Development Kit:

### IoT Gateway - Raspberry Pi 3B+ (1 unit):

High performance, quad-core CPU (64-bit SoC ARM® Cortex®-A53 at 1.4GHz) to support complex data aggregation in a low power package.

Integrated Wi-Fi®, Bluetooth® Low Energy support.

1GB SDRAM and 8GB SD Card memory simplifies configuration and increases scalability.

### IoT Sensor Node

#### Sensor Node Controller with add-on BT module (1 unit):

Ultra-low-power (ULP) FRAM-based microcontroller (MCU) platform, including on-board emulation for programming, debugging and energy measurements. This device features LCD support with an integrated 10-bit ADC as well as embedded FRAM (Ferroelectric Random Access Memory), a non-volatile memory known for its ultra-low power, high endurance and high speed write access.

#### Sensor board - Heart-rate and Pulse-Oximetry Monitor (1 unit):

A low power, optical heart-rate monitor complete with integrated red and IR LEDs for applications such as Wearables, Heart-rate monitor and Pulse oximeter.

## Software

Code Composer Studio Software Development Kit (SDK).



The Development kit



Heart-rate sensor

## Accessories

The following accessories are provided with the training kit.

| Item                            | Quantity |
|---------------------------------|----------|
| 16GB MicroSD Card with NOOBS OS | 1        |
| 5.1V, 2.5A Power Supply         | 1        |
| Micro USB Cables                | 1        |
| Jumper wire bundle              | 1        |

## Lab Sheets

The training kit includes eight lab sheets in editable format. Each lab requires 2-3 hours to complete. Model answers are provided with all lab sheets. The required instruments for the labs are listed below.

### Lab Sheet

---

#### 1. MQTT connection management

Setting up MQTT Mosquitto Broker using Docker. Learn how to use MQTT Mosquitto for topic management and user access control. Demonstrate sensor node hijacking.

---

#### 2. IoT Data Storage and Visualization using Grafana and InfluxDB

Setting up Grafana and InfluxDB using Docker. Learn how to insert data into InfluxDB and to visualize data in InfluxDB using Grafana. Understand the danger of exposing InfluxDB connection to the Internet

---

#### 3. From Sensor Node to Cloud

Setup of IoT-Gateway to Cloud, learn how to process MQTT data and insert into InfluxDB. Learn how to control the insertion process using MQTT and the issue of malicious IoT Devices / Sensor Nodes

---

#### 4. Secure communication between sensor nodes and gateway: encryption and decryption

Learn the techniques to implement AES-256 on MSP430 microcontroller (sensor node). Experiment on protecting the confidentiality of sensor data communicated from the sensor node to gateway device (Raspberry Pi).

---

#### 5. Achieving integrity check for sensor data through SHA-3 hash function

Learn the techniques to implement SHA-3 hash function in microcontroller and the techniques to provide integrity check on data communicated between sensor node and gateway device.

---

#### 6. Secure data aggregation (privacy preserving) in sensor nodes and gateway: partial homomorphic encryption

Learn the techniques to implement Paillier cryptosystem in gateway device and how to provide privacy preserving computation in IoT application

---

#### 7. Authenticating sensor node and sensor data through RSA

Learn the techniques to implement modular exponentiation for RSA encryption and the techniques to implement digital signature through RSA

---

#### 8. Implement NTRU in Microcontroller

Learn the techniques to implement NTRU public key cryptosystem in microcontroller and the technique to speed up the computation of polynomial multiplication for NTRU

---

## Problem-Based Assignments

The problem-based assignments below allow students to enhance their problem-solving skills.

#### 1. End-to-End IoT System with Secure Communication

*First part:* Develop an IoT system to monitor the heart rate (MAX30102) using MQTT and cloud solution.

*Second part:* Secure the sensor data through PRESENT lightweight block cipher.

*Third part:* Improve the encryption and hash speed through various implementation techniques.

#### 2. Optimizing the Implementation of NTRU Public Key Encryption in Sensor Node

*First Part:* Develop the firmware to monitor the heart rate (MAX30102) using MSP430 microcontroller as sensor node.

*Second Part:* Encrypt the sensor data through PRESENT lightweight block cipher. Secure the encryption key for PRESENT using RSA public key cryptography.

*Third Part:* Improve the execution speed of RSA through various implementation techniques

# Training Kit Hardware Specifications

---

## General

---

Warranty :1 year

## Ordering Information

| Description                    | Package   | Product Number                                       |
|--------------------------------|---|--|
| Teaching Slides                | 1 user license                                  | ME5100-100   |
| Training Kit                   | 1 set training kit                              | ME5100-200   |
| Teaching Slides + Training Kit | 1 user license (slides) +<br>1 set training kit | ME5100-300   |
| Instruments                    | Where applicable                                | Purchase separately from Keysight or its distributor |

Training courses related to subject matter are available on request. Visit [dreamcatcher.asia](http://dreamcatcher.asia) for details.

For more information or enquiries:

Website: [dreamcatcher.asia/cw](http://dreamcatcher.asia/cw)  
E-mail: [cw.sales@dreamcatcher.asia](mailto:cw.sales@dreamcatcher.asia)

Acehub Vista Sdn Bhd (785702-P)  
*A member of the DreamCatcher group*

70-03-79, D'Piazza Mall, Jalan Mahsuri  
11900 Bayan Lepas, Penang  
Malaysia

© 2016 Acehub Vista Sdn Bhd

We reserve the right to change or alter the information in this material without prior notice. The information provided in this material is accurate as of the print date.

Microsoft, Windows, and Office Programs are trademarks of Microsoft Corporation in the United States and/or other countries. All other copyrights and trademarks belong to their respective owners.

The logo for DreamCatcher, featuring the word "dream" in a lowercase, cursive-style font above the word "CATCHER" in a bold, uppercase, sans-serif font. The "CATCHER" text is set against a red rectangular background.

Updated on 25 Apr 2019