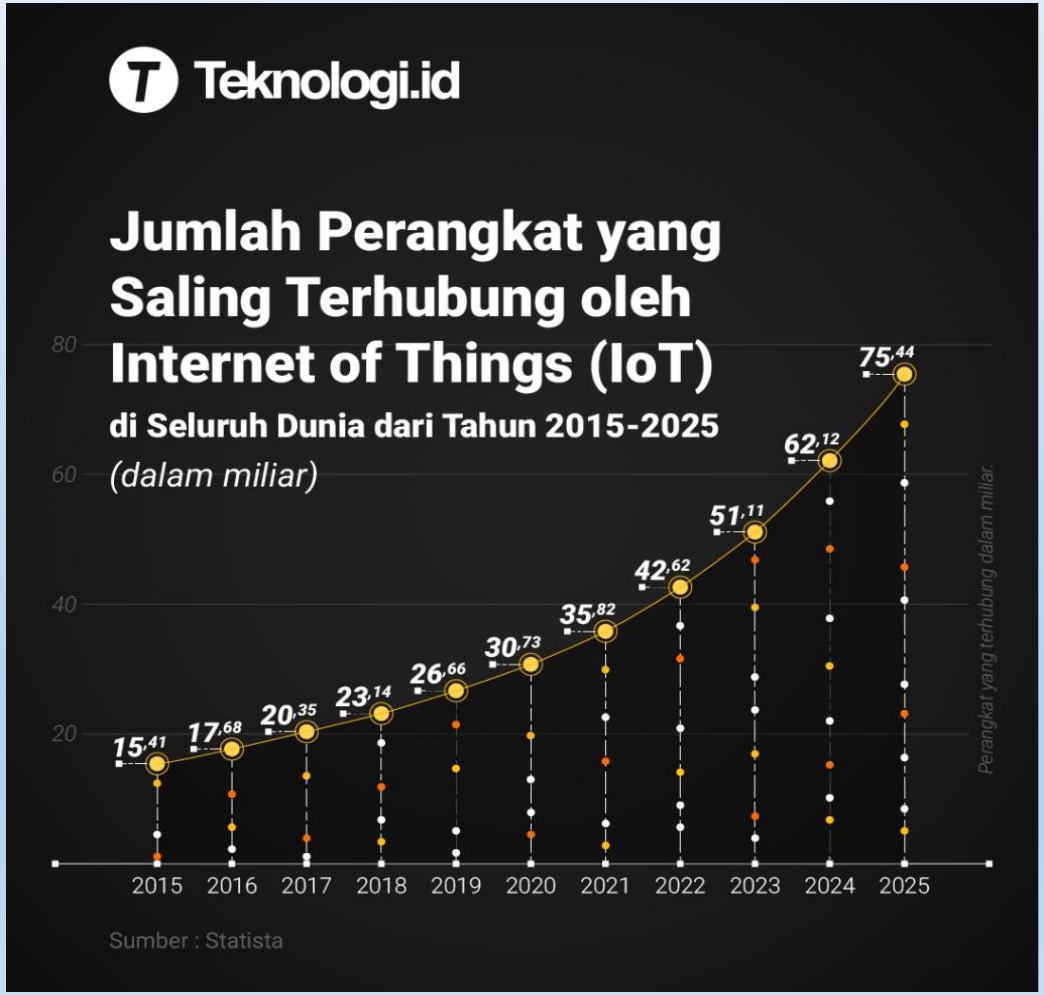
UNIVERSITAS Dinamika

Keamanan Jaringan IoT

By Harianto, SKom, M.Eng

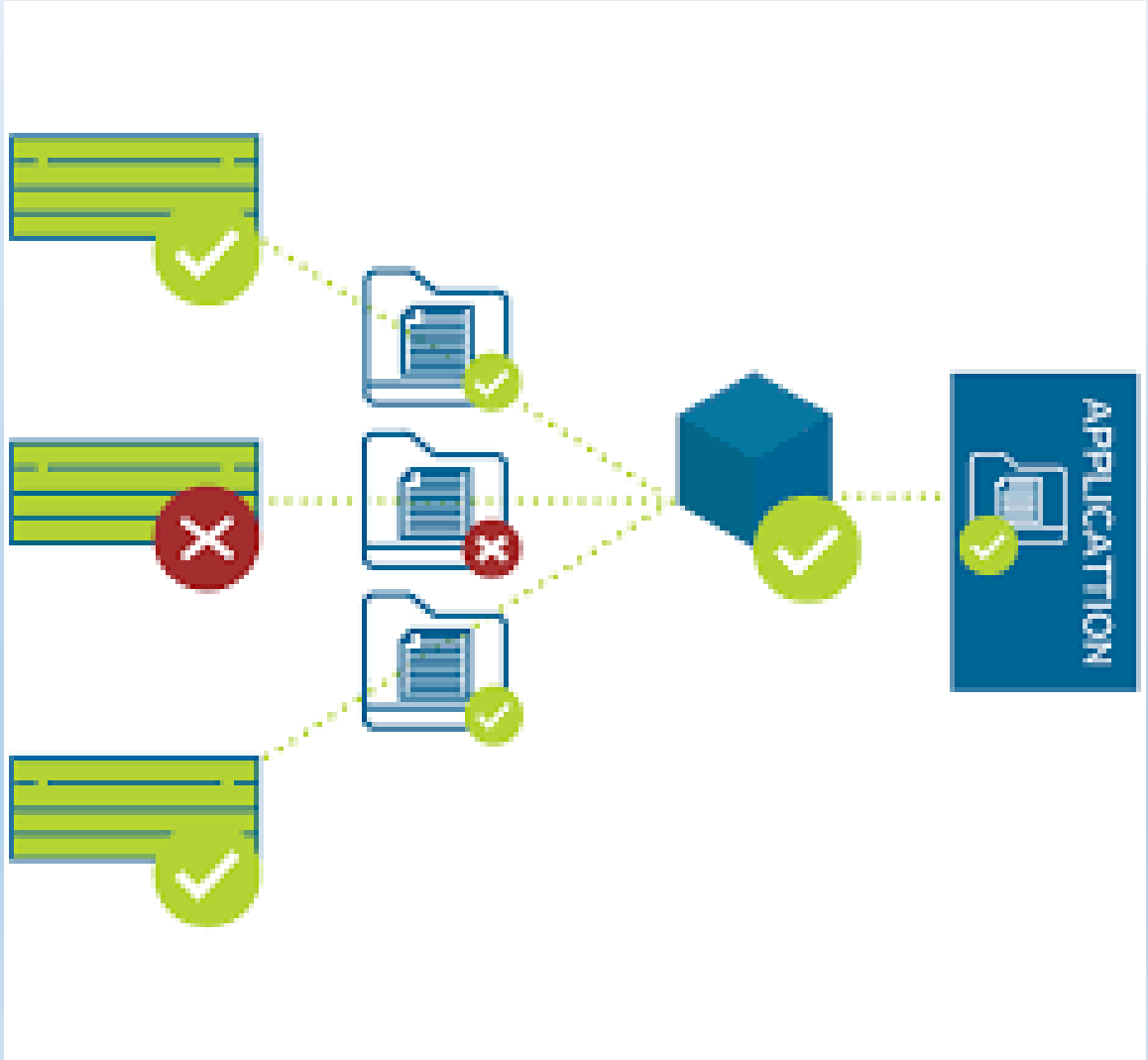
Latar belakang



UNIVERSITAS Dinamika

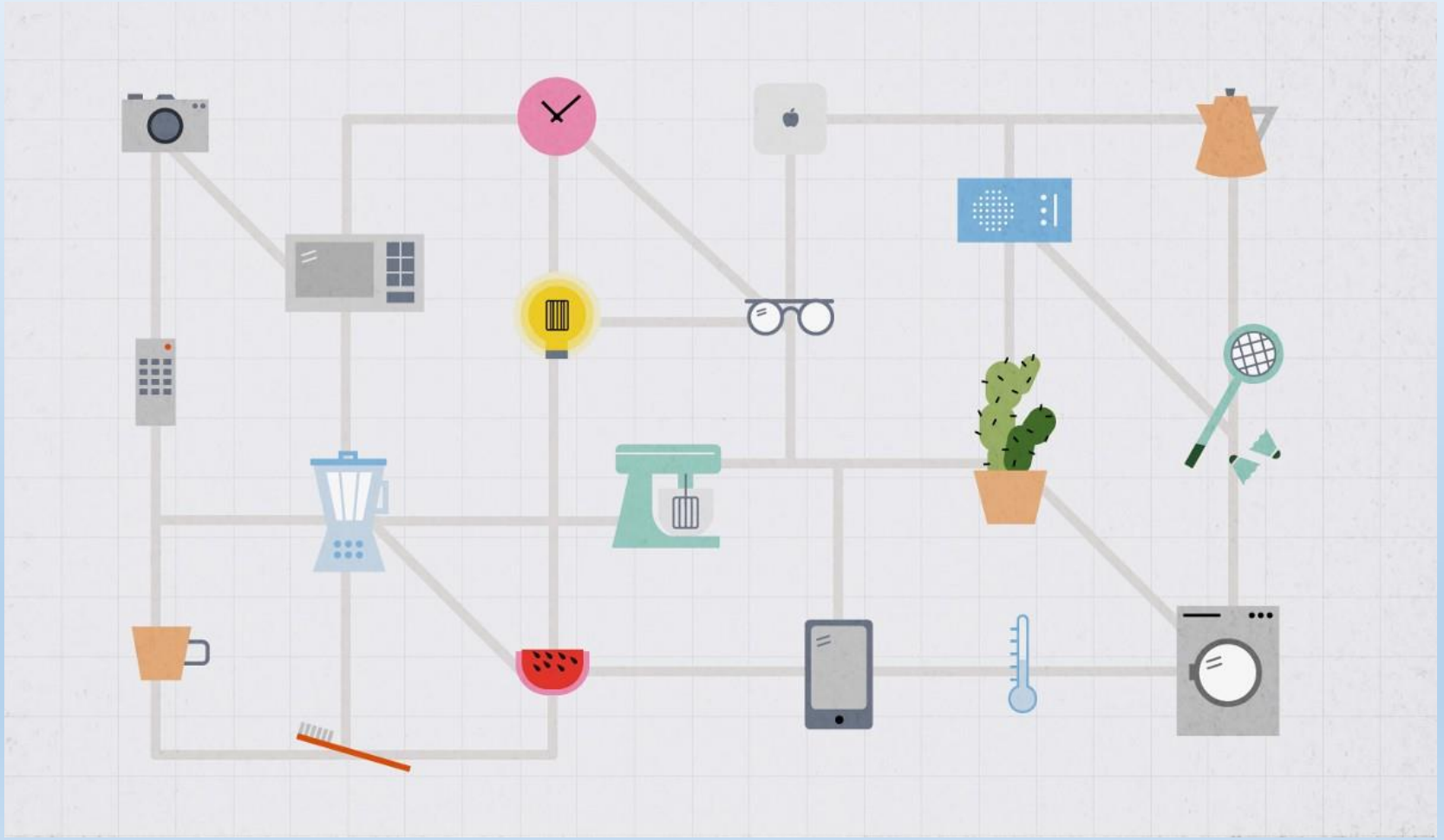
Latar belakang

Latar belakang



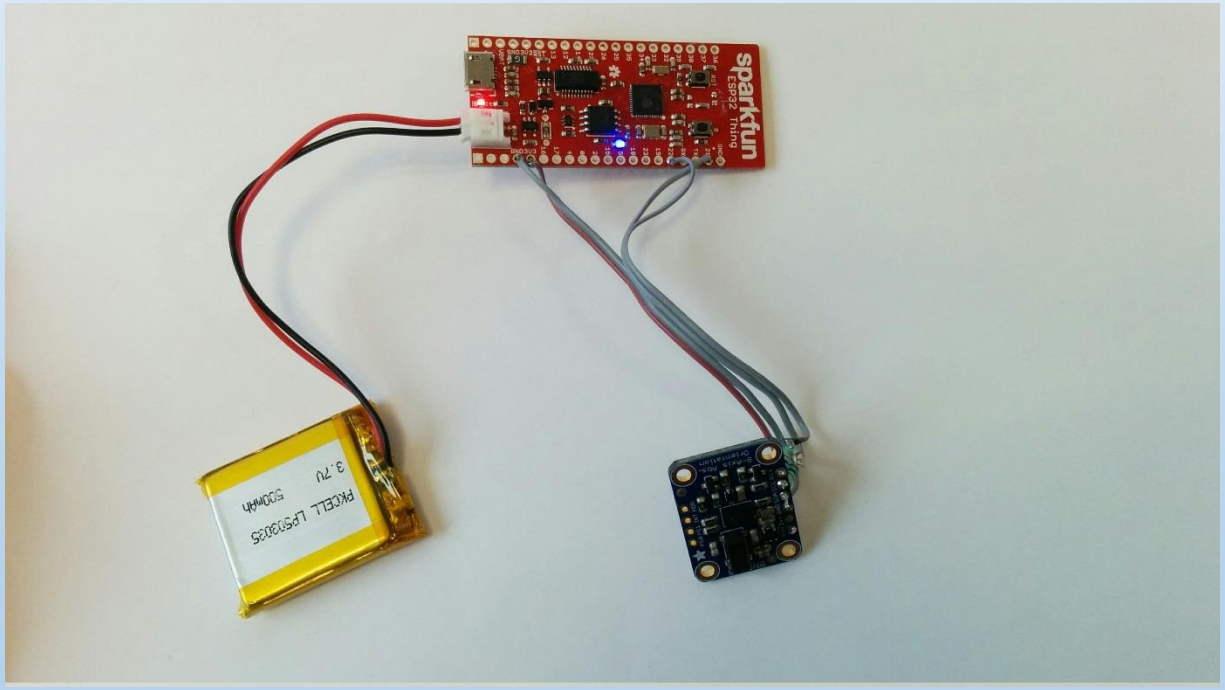
UNIVERSITAS Dinamika

Latar belakang



Pertimbangan pemilihan Protokol IoT

- Keterbatasan perangkat IoT



Pertimbangan pemilihan Protokol IoT

- Berbagai macam jenis perangkat IoT

UNIVERSITAS Dinamika

Pertimbangan pemilihan Protokol IoT

- Jalur Komunikasi yang tidak sempurna
- Keamanan Informasi

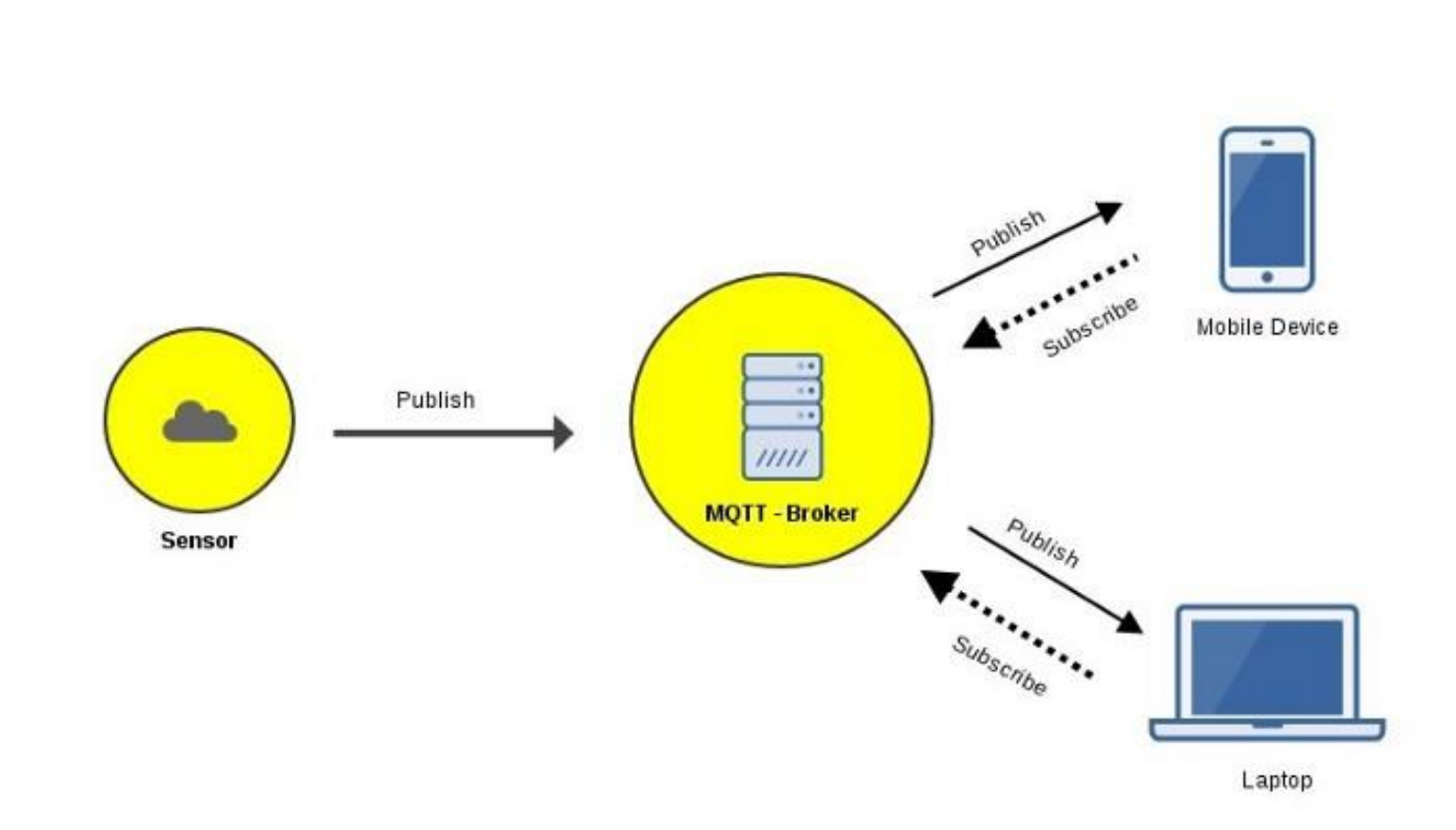
UNIVERSITAS Dinamika

Bebarapa protokol IoT :

- HTTP (Hypertext Transfer Protocol)
- XMPP (Extensible Messaging and Presence Protocol)
- CoAPP (Constrained Application Protocol)
- AMQP (Advanced Message Queuing Protocol)
- MQTT (Message Queuing Telemetry transport)

Arsitektur MQTT

- Publisher
- Subscriber
- Broker



UNIVERSITAS Dinamika

Mekanisme keamanan MQTT

- Membatasi akses ke broker
- Melindungi data dengan berbagai mekanisme keamanan
- Mekanisme keamanan dimulai dari broker
- Pertimbangan kapabilitas klient MQTT

UNIVERSITAS Dinamika

Client Authentication

- Client ids
- Usernames dan password
- Client certificates

Client Ids

- Semua client harus memberikan Ids
- Ids bersifat Unix

UNIVERSITAS Dinamika

Implemetasi pada kontroler (Publisher /Subscriber)

```
Serial.print("Use this URL to connect: ");
Serial.print("http://");
Serial.print(WiFi.localIP());
Serial.println("/");

// Connect to Server IoT (CloudMQTT)

client.setServer(mqttServer, mqttPort);
client.setCallback(receivedCallback);

while (!client.connected()) {
  Serial.println("Connecting to CLoudMQTT...");

  if (client.connect("ESP32Client", mqttUser, mqttPassword )) {

    Serial.println("connected");
      Serial.print("Message received: ");


  } else {
    Serial.print("failed with state ");
    Serial.print(client.state());
    delay(2000);
```

Client Ids

UNIVERSITAS Dinamika

Username dan Password

- Broker meminta Username dan pasword yang valid dari klien sebelum koneksi diizinkan.
- Kombinasi Username dan password dikirimkan dalam bentuk teks
- Username dapat digunakan untuk membatasi akses ke broker
- Userneme juga dapat digunakan untuk membatasi akses ke topik

UNIVERSITAS Dinamika

Implementasi pada kontroler

```
int outputpin = A0;   // sensor LM35
int analogValue;
float millivolts,celsius;


#define mqttServer "i-ot.net"
#define mqttPort 1883
#define mqttUser "upnmqtt"
#define mqttPassword "20upnmqtt"

WiFiServer server(80);
WiFiClient espClient;
PubSubClient client(espClient);
```

Username dan Password

```
client.setServer(mqttServer, mqttPort);
client.setCallback(receivedCallback);

while (!client.connected()) {
  Serial.println("Connecting to CLoudMQTT...");

  if (client.connect("ESP32Client", mqttUser, mqttPassword )) {

    Serial.println("connected");
      Serial.print("Message received: ");


  } else {
    Serial.print("failed with state ");
    Serial.print(client.state());
    delay(2000);
  }
  client.subscribe("kipas");
}
```

UNIVERSITAS Dinamika

Client Certificates

- Metode yang paling aman pada MQTT
- Broker memberikan certificate pada client
- Cukup baik digunakan untuk perangkat yang mempunyai sumberdaya yang besar.

UNIVERSITAS Dinamika

Implementasi pada kontroler

```
/* Certificate Authority info */
/* CA Cert in PEM format */
const char caCert[] PROGMEM = R"EOF(
-----BEGIN CERTIFICATE-----
MIHcAgEBBEIATXmkkoaxsd7d6QvaLYOFBpVWIKkpZiIVifjWyEvG7KORzlGXuWzA
67CkiTbUMscnzM7kn/YrwmITRDaYQ2eF0jagBwYFK4EEACOhgYkDgYYABAFzgTPk
co/CM1hNYyRm8Tnlq0l+rnFSst74VHqoj2wD9XOz7W8iFX1C0J4KsQy2N6FAccym
72tTstwCruZmuc91mgC+RyRm9TxcwvztEOFDkWeKpVCrheILGH03zBqb93p9nTIa
bUMscnzM7kn/YrwmITRDaYQ2eF0jagBwYFK4EEACOhgYkDgYYABAFzgTPkco/CM1
Rm8Tnlq0l+rnFSst74VHqoj2wD9XOz7W8iFX1C0J4KsQy2N6FAccymFSst74VHqF
zBqb93p9nTIa72tTstwCruZmuc91mgC+RyRm9TxcwvztEOFDkWeKpVCrheILGH03
zM7kn/YrwmITRDaYQ2eF0jag67CkiTbUMscnBwYFK4EEACOhgYkDgYYABAFzgTPk
qoj2wD9XOzco/CM1hNYJ4KsQy2N6FAccymyRm8Tnlq0l+7W8iFX1C0rnFSst74VH
rheILGH03zBqb93p9nTIa72tTc91mgC+RyRm9TxcwvztEOFDkWeKpVCstwCruZmu
qoj2wD9XOzco/CM1hGbPfS2UEKITVxTth9OZ+4rplg==
-----END CERTIFICATE-----
)EOF";
```

Certificate dari broker

```
/* MQTT broker cert SHA1 fingerprint, used to validate connection to right server */
const uint8_t mqttCertFingerprint[] = {0xFF,0x69,0xBB,0xAD,0xF0,0xDE,0x5F,0x89,0x23,0xF6,0x96,0xC1,0x03,0x04,0x23,0xB4,0xD3,0xD5,0x53,0x94};

/* Other globals */
```

UNIVERSITAS Dinamika

Terimakasih &

Semoga Bermanfaat