Mengamankan Data Sensor: Penerapan Kriptografi dalam Internet of Things (IoT)

Ahmad Mutawalli - 13517026
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
13517026@std.stei.itb.ac.id

***Abstract*—Perkembangan dunia teknologi sangat pesat salah satunya adalah IoT. Pada jaringan IoT akan terjadi pertukaran pesan antara beberapa perangkat. Pertukaran pesan tersebut harus dilindungi dari pihak yang tidak bertanggung jawab untuk memastikan pesan yang dikirimkan asli. Pada makalah ini akan dibahas bagaimana penerapan Kriptografi untuk mengamankan proses pertukaran pesan pada jaringan IoT**

Keywords—IoT, Pertukaran pesan, Kriptografi

I. Introduction

Perkembangan dunia teknologi sangat pesat salah satunya adalah *Internet of Things* (IoT). IoT merujuk pada suatu jaringan yang menghubungkan berbagai perangkat dalam dunia fisik dengan berbagai protokol berbeda. Berbagai perangkat saling bertukar pesan di antara satu dengan yang lain. Namun, pertukaran pesan dapat diubah ketika terjadi komunikasi oleh pihak yang tidak bertanggung jawab.

Oleh karena itu, pada makalah ini akan dibahas mengenai mengamankan data sensor pada perangkat IoT dengan Kriptografi menggunakan *digital signature*. Dengan menggunakan *digital signature*, pesan yang diterima dari perangkat IoT dapat dipastikan keasliannya.

II. LANDASAN TEORI

A. *Internet of Things* (IoT)

IoT adalah konsep dimana konektivitas internet dapat bertukar informasi satu sama lainnya dengan benda-benda yang ada disekelilingnya. IoT merupakan sebuah konsep yang bertujuan untuk memperluas manfaat dari konektivitas internet yang tersambung secara terus-menerus. IoT dapat didefinisikan kemampuan berbagai device untuk bisa saling terhubung dan saling bertukar data melalui jaringan internet. IoT merupakan sebuah teknologi yang memungkinkan adanya sebuah pengendalian, komunikasi, kerjasama dengan berbagai perangkat keras, data melalui jaringan internet. Sehingga bisa dikatakan bahwa IoT adalah ketika kita menyambungkan sesuatu (things) yang tidak dioperasikan oleh manusia ke internet Manfaatnya menggunakan teknologi IoT yaitu pekerjaan yang dilakukan oleh manusia menjadi lebih cepat, mudah dan efisien.

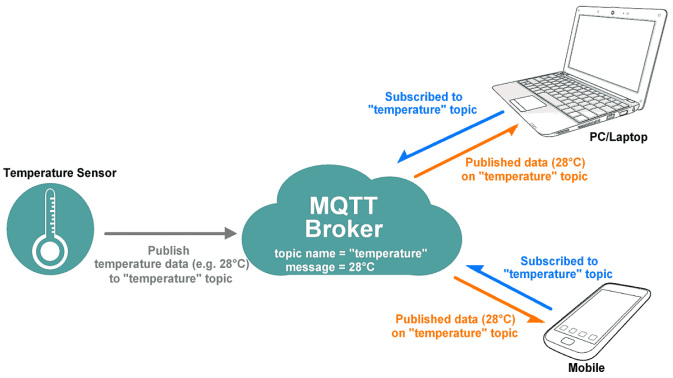
B. *MQTT*

MQTT adalah protokol pesan yang digunakan untuk komunikasi mesin ke mesin. Sensor, perangkat yang digunakan, dan perangkat IoT lainnya biasanya harus mengirim dan menerima data melalui jaringan dengan sumber daya dan bandwidth terbatas. Perangkat Iot menggunakan MQTT untuk transmisi data karena mudah diterapkan dan dapat mengkomunikasikan data IoT secara efisien. MQTT menerapkan model publikasi/berlangganan dengan menentukan klien dan broker seperti dibawah ini.

Komponen pada MQTT adalah:

- Klien MQTT: setiap perangkat dari server ke mikrokontroler yang menjalankan MQTT. Jika klien mengirim pesan, ia bertindak sebagai publisher, dan jika klien menerima pesan, ia bertindak sebagai subscriber.
- Broker MQTT: sistem backend yang mengkoordinasikan pesan antara klien yang berbeda. Tanggung jawab broker meliputi menerima dan memfilter pesan, mengidentifikasi klien yang berlangganan setiap pesan, serta mengirimi pesan kepada klien

Berikut adalah gambaran protokol MQTT



C. Kriptografi

Kriptografi berasal dari bahasa Yunani "*Kriptos*" yang artinya "yang bersembunyi" dan "*graphien*" yang berarti tulisan. Secara etimologi, kriptografi dapat diartikan sebagai

bidang ilmu tentang penyembunyian pesan. Kriptografi mempelajari berbagai teknik enkripsi. Dalam enkripsi sebuah plainteks diproses melalui sebuah algoritma enkripsi menghasilkan sebuah cipherteks. Melalui proses ini, seseorang yang tidak memiliki kunci dekripsi tidak dapat membaca data tersebut.

Kriptografi menjawab persoalan dari masalah-masalah berikut:

- *Confidentiality*: Data yang dikirimkan pengirim tidak dapat dibaca oleh pihak ketiga
- *Authentication*: Penerima dapat memastikan pesan yang diterima adalah benar pesan yang dikirimkan oleh pengirim
- *Integrity*: Penerima dapat memastikan pesan yang diterima masih asli dan tidak diubah pada saat komunikasi
- *Non-repudiation*: Penerima dapat melakukan anti-sangkalan apabila Pengirim menyangkal telah mengirimkan pesan

D. Digital Signature

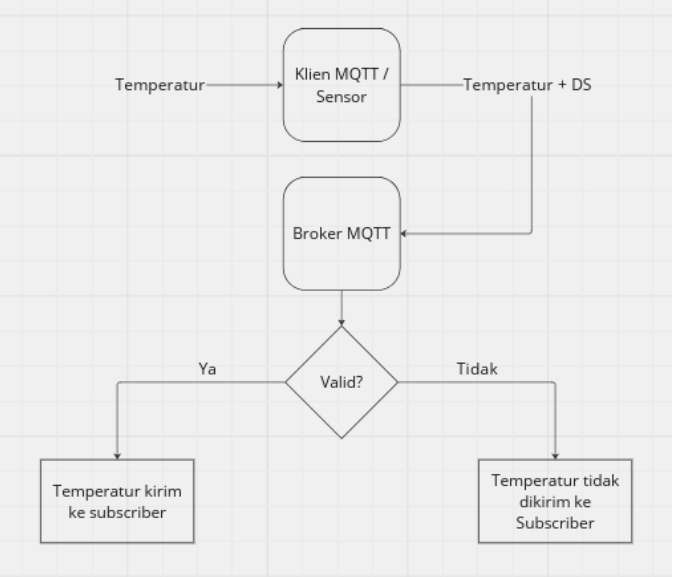
Digital Signature atau tanda tangan digital adalah sebuah nilai kriptografis yang dibuat sesuai dengan isi pesan dan kunci, dimana setiap sign atau tanda tangan yang diberikan selalu berbeda untuk antar satu pesan dengan pesan lainnya. Selain itu tanda tangan digital juga selalu berbeda untuk antar satu kunci dengan kunci lainnya. Tanda tangan digital memberikan dua dari empat layanan kriptografi yaitu *authentication* dan *non-repudiation*.

Secara garis besar, terdapat dua proses dalam tanda tangan digital, yaitu menandatangani pesan (*signing*) dan memverifikasi pesan (*verification*). Pada proses penandatangan pesan, terdapat dua metode yang umum dilakukan, yaitu dengan mengenkripsi pesan untuk pesan rahasia, serta kombinasi fungsi hash.

III. PEMBAHASAN

Peran Kriptografi dalam keamanan data sensor adalah pada saat klien MQTT ingin mengirimkan pesan kepada broker MQTT, pesan tersebut dilakukan *digital signature* terlebih dahulu. Pesan + *digital signature* dikirim kepada broker MQTT. Broker MQTT akan memverifikasi pesan + *digital signature* yang diterima sehingga dapat dipastikan pesan tersebut masih asli dan dikirim oleh klien MQTT.

Berikut adalah gambaran pengiriman data sensor menggunakan kriptografi



IV. KESIMPULAN

Kriptografi dapat menjadi solusi untuk mengamankan komunikasi antara perangkat - perangkat pada jaringan IoT menggunakan algoritma tanda tangan digital

UCAPAN TERIMAKASIH

Ucapan terimakasih penulis nyatakan kepada Tuhan Yang Maha Esa, karena karunia-Nya penulis bisa diberikan kesempatan untuk menyelesaikan dan bisa memberikan kontribusi nyata dalam memberikan ide yang dituliskan pada makalah ini.

Penulis juga mengucapkan terimakasih kepada Dr. Rinaldi Munir atas dedikasinya dalam memberikan ilmu pengetahuan tentang kriptografi kepada penulis.

REFERENSI

[1] Munir, Rinaldi "Pengantar Kriptografi". https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/01-Pengantar-Kriptografi-(2024).pdf Diakses pada 22 Juni 2024

[2] Munir, Rinaldi "Tanda Tangan Digital". https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/29-Tanda-tangan-digital-2024.pdf Diakses pada 22 Juni 2024

[3] Hergika Gusti, dkk 2021 "PERANCANGAN INTERNET OF THINGS(IOT) SEBAGAI KONTROL INFRASTUKTUR DAN PERALATAN TOLL PADA PT. ASTRA INFRATOLL ROAD" Jurnal PROSISKO

[4] AWS "What is MQTT?" https://aws.amazon.com/id/what-is/mqtt Diakses pada 22 Juni 2024

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Juni 2024

Ahmad Mutawalli 13517026