**Muhammad Fadli Mannguluang**

**1202223209**

**46-01**

**Taxonomy of IoT Security**

**Privacy**

Dengan adanya pengaplikasian perangkat menggunakan IoT, tentunya tidak mustahil jika kebocoran informasi data pengguna kerap kali terjadi. Kebocoran informasi data pengguna dapat menimbulkan masalah dan ancaman yang besar untuk seluruh jaringan dan dapat merusak data individual maupun data perusahaan. Dengan banyaknya pengguna mungkin hal tersebut merupakan tantangan utama bagi perusahaan untuk mempunyai sistem data privasi yang mendukung.

**Secara umum ada 3 cara untuk menjamin privasi, yaitu:**

1. **Manajemen Identitas**

Manajemen identitas terutama digunakan untuk mengotentikasi pengguna pada suatu sistem dan memastikan apakah pengguna itu diizinkan atau dilarang mengakses sistem tertentu. Biasanya, manajemen identitas terdiri dari berbagai fase termasuk otentikasi pengguna, tingkat otorisasi dan jenis peran yang mungkin dimiliki pengguna. Ini juga berkaitan dengan tingkat akses yang dimiliki pengguna pada sistem tertentu. Misalnya, pengguna mungkin diberikan akses ke sistem / perangkat lunak, tetapi tidak semua komponennya.

1. **Otentikasi**

Otentikasi berfungsi untuk mengikat sebuah objek dengan identitasnya (identitas akar) dan untuk menjamin properti maupun peran dari objek tersebut. Misalnya jika sebuah objek adalah pengguna, maka properti yang dijamin dapat berupa:

* berusia lebih dari 17 tahun ,
* memiliki tanda pengenal yang sah .
* memiliki sertifikasi level Z,
* dan lain-lain.

1. **Otorisasi**

Merupakan proses pemberian akses terhadap informasi maupun ke sumber daya IoT bagi sebuah objek sesuai dengan aturan akses dan jenis aksi tertentu. Untuk menjamin privasi, pengguna harus memiliki kontrol penuh terhadap aturan akses yang beruhungan dengan data personalnya.

**Trust**

Keamanan dan privasi dapat dibangun melalui hubungan kepercayaan antara penyedia layanan dan pengguna, dalam arti yang lain trust dalam IoT dapat didefinisi sebagai harapan atau ekspetasi bahwa sesuatu dilakukan tanpa merugikan pengguna.

**Contoh Studi Kasus Trust :**

1. **Smart Grid**

Smart meter memungkinkan pemantauan konsumsi listrik dan membuat penagihan berdasarkan data. Trust IoT memungkinkan penyedia energi untuk mengamankan catatan penggunaan listrik serta pendapatan.

1. **Patient Surveillance**

Menangkap, mendeteksi, dan monitoring tanda-tanda vital seperti denyut jantung, suhu tubuh, tekanan darah, dll. Trust Iot melindungi menjaga kerahasiaan informasi pasien.

1. **IP Cameras**

Kamera yang terhubung dari jarak jauh memungkinkan untuk menerima gambar secara real time. Trust IoT melindungi privasi dan memastikan gambar atau video berasal dari kamera yang telah diautentikasi dan terpecaya.

**Daftar Pustaka**

<http://snete.unsyiah.ac.id/2015/prosiding/Naskah%2015.pdf>

<https://id.theastrologypage.com/identity-management>

<https://www.qilium.com/trust-iot/>

<https://arxiv.org/pdf/1903.05362>