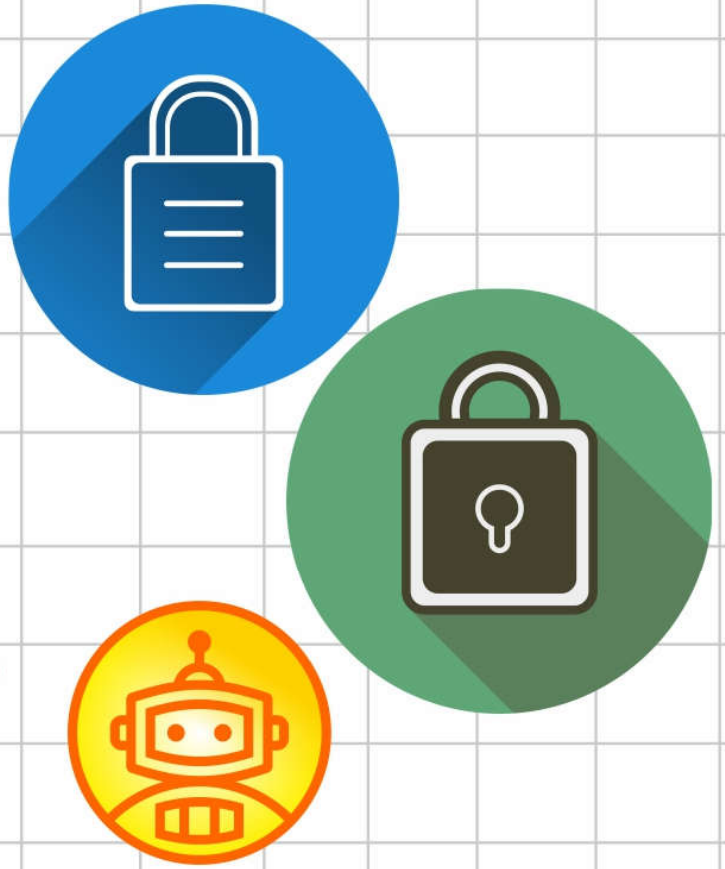
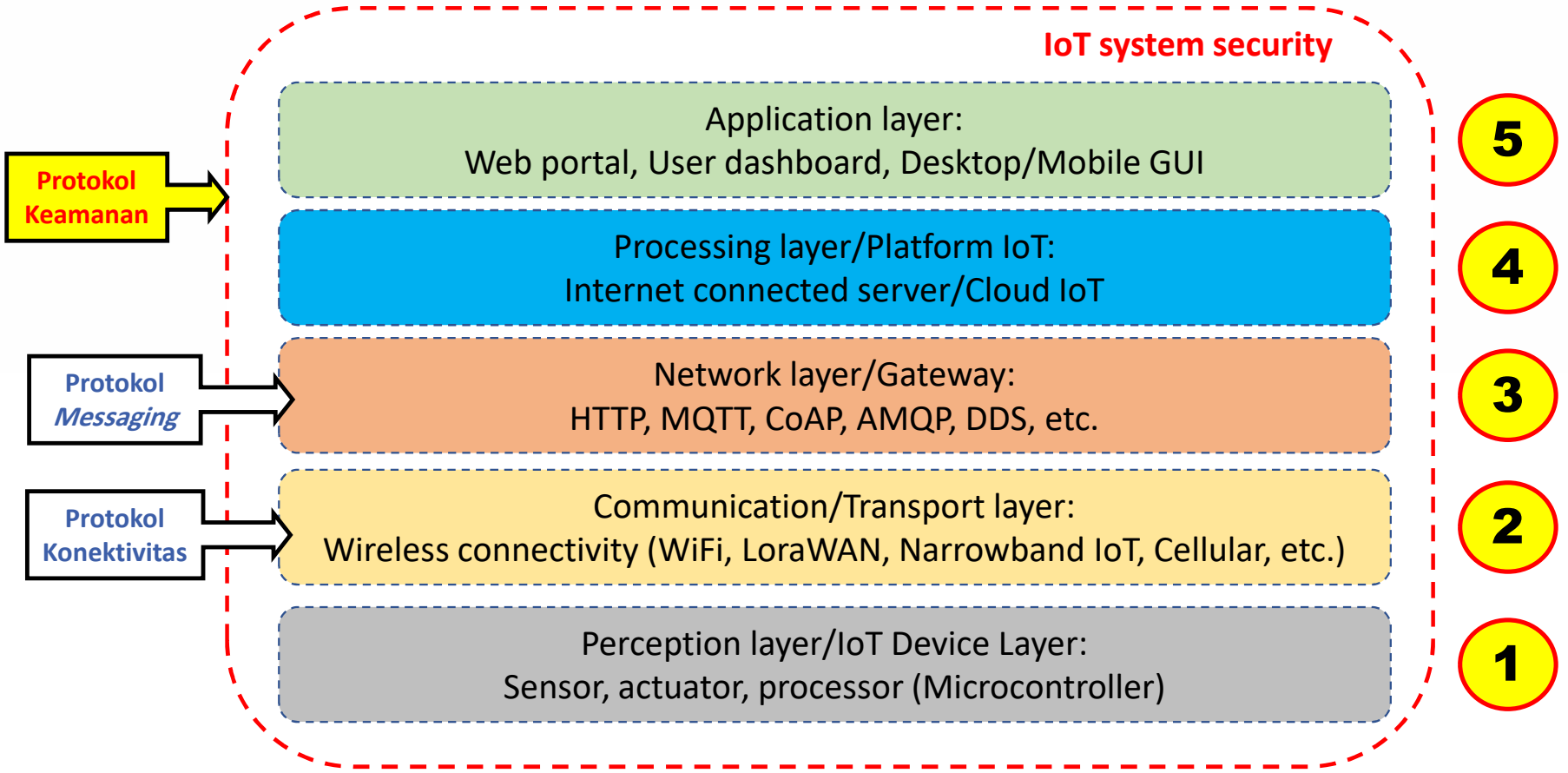
Protokol Keamanan untuk IoT



Jenis Protokol untuk Sistem IoT



Arsitektur Sistem IoT

Jenis Protokol untuk Sistem IoT

Dalam teknologi *internet of things* (IoT) terdapat 4 jenis protokol:

No.	Protokol	Keterangan	
1	Konektivitas	Didiskusikan pada video yang lain	✗
2	*Messaging* (Komunikasi)	Tema diskusi pada video ini	✗
3	Keamanan (*Security*)	Didiskusikan pada video yang lain	✓
4	Manajemen perangkat IoT	Didiskusikan pada video yang lain	✗

✓ : Topik yang didiskusikan pada video ini

✗ : Topik yang tidak didiskusikan pada video ini

Protokol Keamanan untuk Sistem IoT

Definisi

Protokol keamanan untuk sistem IoT (Internet of Things) adalah serangkaian aturan, protokol, dan teknik yang digunakan untuk melindungi perangkat IoT, data yang dikirim dan diterima oleh perangkat IoT, serta infrastruktur jaringan yang digunakan dalam ekosistem IoT.

Catatan:

- Protokol keamanan yang kuat dan implementasi yang benar sangat penting untuk menjaga keamanan dan privasi dalam ekosistem IoT yang semakin kompleks. Setiap komponen dalam jaringan IoT, mulai dari perangkat hingga server dan infrastruktur jaringan, harus dilindungi secara efektif melalui protokol keamanan yang sesuai.
- Pemilihan protokol keamanan tergantung pada kebutuhan dan karakteristik aplikasi IoT tertentu, seperti tingkat keamanan yang diperlukan, konsumsi daya, latensi, dan infrastruktur komunikasi yang digunakan. Kombinasi beberapa protokol keamanan juga sering digunakan untuk memastikan keamanan yang kuat dalam aplikasi IoT yang kompleks.

Protokol Keamanan untuk Sistem IoT

Tujuan

Tujuan utama protokol keamanan adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan data serta untuk mencegah akses yang tidak sah atau serangan terhadap perangkat IoT dan jaringan.

Protokol Keamanan untuk Sistem IoT

Komponen Utama Protokol Keamanan (1)

1. **Enkripsi**: Protokol keamanan menggunakan teknik enkripsi untuk mengamankan data yang dikirimkan antara perangkat IoT dan server atau perangkat lain dalam jaringan. Enkripsi mengubah data menjadi format yang hanya dapat dibaca oleh penerima yang sah dengan menggunakan kunci enkripsi yang sesuai.
2. **Otentikasi**: Otentikasi adalah proses verifikasi identitas perangkat IoT dan server sebelum mereka diperbolehkan untuk berkomunikasi. Ini memastikan bahwa hanya perangkat yang sah yang dapat terhubung dan berinteraksi dengan jaringan.
3. **Otorisasi**: Otorisasi mengontrol hak akses perangkat IoT terhadap sumber daya dan layanan dalam jaringan. Ini menentukan apa yang dapat dilakukan oleh perangkat berdasarkan identitasnya dan peran yang telah ditentukan.
4. **Manajemen Kunci**: Protokol keamanan menyertakan manajemen kunci yang memadai untuk menghasilkan, mendistribusikan, dan mengelola kunci enkripsi. Manajemen kunci yang kuat adalah kunci untuk menjaga keamanan data.
5. **Audit dan Pemantauan**: Protokol keamanan mencakup fitur audit dan pemantauan yang memungkinkan administrator jaringan untuk melacak dan memeriksa aktivitas perangkat IoT dan mendeteksi aktivitas yang mencurigakan.

Protokol Keamanan untuk Sistem IoT

Komponen Utama Protokol Keamanan (2)

6. **Perlindungan Terhadap Ancaman**: Protokol keamanan mengidentifikasi dan melindungi terhadap berbagai jenis ancaman keamanan, termasuk serangan seperti serangan jaringan, serangan *denial of service* (DoS), serangan berbasis malware, dan lainnya.
7. **Pembaruan Keamanan**: Sistem IoT harus mampu menerima pembaruan keamanan secara teratur untuk mengatasi kerentanannya yang ditemukan seiring waktu. Protokol keamanan mendukung pembaruan ini.
8. **Ketahanan Terhadap Serangan Fisik**: Protokol keamanan juga mempertimbangkan ketahanan terhadap serangan fisik terhadap perangkat IoT, seperti upaya untuk mencuri data atau merusak perangkat.
9. **Kepatuhan Standar**: Protokol keamanan sering harus mematuhi standar keamanan yang telah ditetapkan, seperti TLS/SSL, OAuth, atau protokol keamanan industri lainnya.
10. **Edukasi dan Kesadaran**: Pengguna dan pemilik perangkat IoT harus diberikan pemahaman tentang praktik keamanan yang baik untuk melindungi perangkat dan data mereka.

Jenis Protokol Keamanan untuk Sistem IoT

Protokol Keamanan untuk Sistem IoT

Jenis Protokol Keamanan (1)

1. **TLS/SSL (Transport Layer Security/Secure Sockets Layer)**: TLS dan SSL adalah protokol keamanan standar yang digunakan untuk mengenkripsi lalu lintas data antara perangkat IoT dan server, serta antara perangkat IoT yang berkomunikasi satu sama lain. Ini membantu melindungi data dari pihak yang tidak berwenang.
2. **DTLS (Datagram Transport Layer Security)**: DTLS adalah varian dari TLS yang dirancang khusus untuk digunakan dalam komunikasi UDP, yang sering digunakan dalam lingkungan IoT yang lebih ringan. DTLS menyediakan enkripsi dan otentikasi untuk lalu lintas UDP.
3. **OAuth (Open Authorization)**: OAuth adalah protokol otorisasi yang digunakan untuk mengontrol akses ke sumber daya IoT. Ini memungkinkan perangkat atau aplikasi untuk meminta izin akses terhadap sumber daya yang dilindungi, seringkali melalui mekanisme token.
4. **JWT (JSON Web Tokens)**: JWT adalah format token yang sering digunakan dalam otentikasi dan otorisasi perangkat IoT. Mereka mengandung klaim yang memuat informasi otentikasi dan otorisasi, dan biasanya digunakan dalam kombinasi dengan OAuth.
5. **PSK (Pre-Shared Key)**: PSK adalah metode keamanan yang melibatkan pertukaran kunci sebelumnya antara perangkat IoT dan server. Kunci ini digunakan untuk mengenkripsi dan mendekripsi data.
6. **EAP (Extensible Authentication Protocol)**: EAP adalah kerangka kerja otentikasi yang mendukung berbagai metode otentikasi yang berbeda, seperti EAP-TLS dan EAP-TTLS, yang dapat digunakan dalam komunikasi IoT yang aman.

Protokol Keamanan untuk Sistem IoT

Jenis Protokol Keamanan (2)

7. **SRP (Secure Remote Password)**: SRP adalah protokol otentikasi yang memungkinkan perangkat IoT dan server untuk melakukan otentikasi tanpa perlu mengirimkan kata sandi melalui jaringan.
8. **CoAP (Constrained Application Protocol) with DTLS**: CoAP adalah protokol messaging yang dioptimalkan untuk perangkat IoT dengan sumber daya terbatas. Ketika digunakan bersama DTLS, ini memberikan lapisan keamanan tambahan untuk komunikasi IoT.
9. **IPSec (Internet Protocol Security)**: IPSec adalah protokol keamanan yang digunakan dalam jaringan IP untuk mengenkripsi dan mengamankan komunikasi antara perangkat IoT dan server.
10. **WPA3 (Wi-Fi Protected Access 3)**: WPA3 adalah protokol keamanan yang digunakan dalam jaringan Wi-Fi yang lebih baru untuk melindungi perangkat IoT yang terhubung ke jaringan nirkabel.
11. **Blockchain**: Teknologi ***blockchain*** dapat digunakan untuk memastikan integritas dan keamanan data IoT dengan mengamankan catatan transaksi dalam rantai blok yang terdesentralisasi.


ROBONESIA
more than robotics learning