

Internet of Everything (IoE)

Pertemuan 7 : Keamanan dan Privasi dalam Internet of Everything (IoE)

Alauddin Maulana Hirzan

Fakultas Teknologi Informasi dan Komunikasi
Universitas Semarang

Outline

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

- 1 Keamanan IoE
- 2 Keamanan Data IoE
- 3 Lastly

Konsep Keamanan

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

- **IoE (Internet of Everything)** mengintegrasikan manusia, proses, data, dan benda (things) ke dalam satu ekosistem digital yang saling berinteraksi.
- Tujuannya adalah menciptakan konektivitas cerdas yang memungkinkan pengambilan keputusan otomatis dan efisien di berbagai sektor: industri, kesehatan, transportasi, dan rumah tangga.
- Semakin kompleks sistem dan banyaknya perangkat yang terhubung, semakin luas pula permukaan serangan (attack surface) yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab.

Tantangan Keamanan

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Tantangan utama meliputi:

- ① Autentikasi dan otorisasi perangkat.
- ② Kerahasiaan dan integritas data.
- ③ Keamanan komunikasi antar node dan antar jaringan.
- ④ Pengelolaan patch dan pembaruan perangkat keras maupun lunak.

Kebutuhan Keamanan

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

IoE memerlukan keamanan menyeluruh (end-to-end security) yang mencakup seluruh lapisan:

- ① **Sensor/Perangkat Edge** : proteksi firmware dan identitas perangkat.
- ② **Jaringan Komunikasi** : enkripsi data dan mitigasi serangan DoS/DDoS.
- ③ **Middleware / Platform IoT** : kontrol akses dan deteksi anomali.
- ④ **Aplikasi Cloud** : perlindungan data pengguna dan kepatuhan terhadap regulasi.

Contoh Kasus: Serangan Botnet Mirai (2016)

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

- Mirai Botnet mengeksploitasi kelemahan keamanan pada kamera IP dan perangkat IoT lainnya yang menggunakan password default.
- Ratusan ribu perangkat dikompromikan dan digunakan untuk meluncurkan serangan DDoS berskala besar, termasuk terhadap Dyn DNS, yang menyebabkan gangguan akses ke situs besar seperti Twitter, Netflix, dan GitHub.
- Kasus ini menegaskan pentingnya keamanan perangkat IoE sejak tahap desain (security by design).

Lapisan Keamanan IoE

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Sensor Layer

- **Fungsi :**
 - Lapisan ini mencakup sensor, aktuator, RFID, kamera, dan perangkat pengindra lainnya yang bertugas mengumpulkan data fisik dari lingkungan
- **Tujuan Keamanan :**
 - Menjamin integritas dan keaslian data sensor.
 - Melindungi perangkat dari akses fisik tidak sah dan serangan injeksi data.
 - Mengamankan identitas perangkat (device authentication).
- **Ancaman Umum :**
 - Node capture attack (pengambilalihan sensor).
 - Fake node injection dan data tampering.
 - Side-channel attack pada sensor dan MCU.

Lapisan Keamanan IoE

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Network Layer

- **Fungsi :**
 - Menangani transmisi data antara sensor, perangkat edge, dan infrastruktur jaringan (Wi-Fi, LTE, 5G, IPv6, MQTT, CoAP, dsb).
- **Tujuan Keamanan :**
 - Menjaga kerahasiaan dan integritas data selama transmisi.
 - Menjamin autentikasi antar node jaringan.
 - Melindungi dari serangan komunikasi seperti sniffing, DoS, atau MITM.
- **Ancaman Umum :**
 - Eavesdropping dan packet injection.
 - Denial of Service (DoS).
 - Routing attack (misal sinkhole, Sybil).

Lapisan Keamanan IoE

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Middleware Layer

- **Fungsi :**
 - Lapisan ini menghubungkan perangkat IoE dengan aplikasi melalui layanan seperti manajemen data, interoperabilitas, dan orkestrasi layanan.
- **Tujuan Keamanan :**
 - Menjamin integritas proses pengelolaan data.
 - Menerapkan kontrol akses dan kebijakan privasi data.
 - Menyediakan autentikasi dan otorisasi antar entitas.
- **Ancaman Umum :**
 - API exploitation dan unauthorized service invocation.
 - Data leakage pada cloud middleware.
 - Privilege escalation.

Lapisan Keamanan IoE

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Application Layer

- **Fungsi :**
 - Menyediakan antarmuka dan layanan akhir bagi pengguna, seperti smart home apps, industrial dashboards, atau e-health systems.
- **Tujuan Keamanan :**
 - Menjamin keamanan data pengguna dan privasi informasi pribadi.
 - Menghindari akses ilegal dan eksploitasi API aplikasi.
 - Menyediakan audit, logging, dan kebijakan keamanan berbasis konteks.
- **Ancaman Umum :**
 - Malware injection, phishing, insecure API calls.
 - Weak authentication dan data privacy leakage.

Ancaman-Ancaman

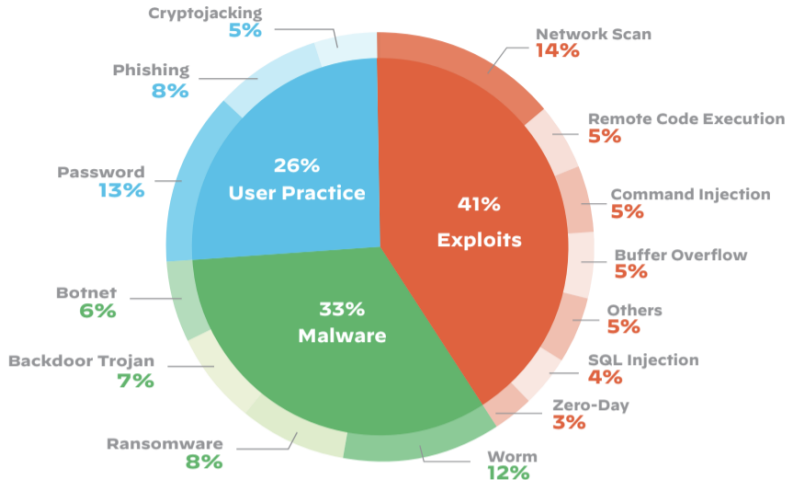
Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly



Ancaman pada Lapisan Sensor

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Jenis Ancaman

- ➊ **Physical Tampering** – Penyerang melakukan akses fisik terhadap sensor, seperti pencurian atau penggantian modul firmware. – Dampak: kehilangan data, manipulasi hasil pengukuran, atau penyusupan malware.
- ➋ **Node Capture Attack** – Penyerang menguasai node IoT untuk memperoleh kunci kriptografi atau konfigurasi sistem. – Sering terjadi pada lingkungan tanpa pengawasan fisik.
- ➌ **Side-Channel Attack** – Penyerang menganalisis konsumsi daya, waktu eksekusi, atau emisi elektromagnetik untuk menebak kunci enkripsi.

Ancaman pada Lapisan Jaringan

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Jenis Ancaman

- 1 **Eavesdropping & Man-in-the-Middle (MITM)**: – Penyadapan data pada protokol MQTT, CoAP, atau HTTP tanpa enkripsi.
- 2 **Replay Attack**: – Penyerang mengirim ulang pesan sah untuk mengacaukan sistem atau menipu perangkat target.
- 3 **Routing Attack**: – Manipulasi tabel routing dalam jaringan mesh IoT (contoh: RPL) untuk mengarahkan lalu lintas ke node jahat.

Ancaman pada Lapisan Middleware

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Jenis Ancaman

- 1 **API Injection Attack:** – Penyerang menyisipkan perintah berbahaya ke dalam API gateway IoT.
- 2 **Unauthorized Data Aggregation:** – Middleware menyimpan atau memproses data tanpa enkripsi yang memadai.
- 3 **Denial of Service (DoS):** – Serangan membanjiri broker middleware, menyebabkan penundaan atau kerusakan layanan.

Ancaman-Ancaman

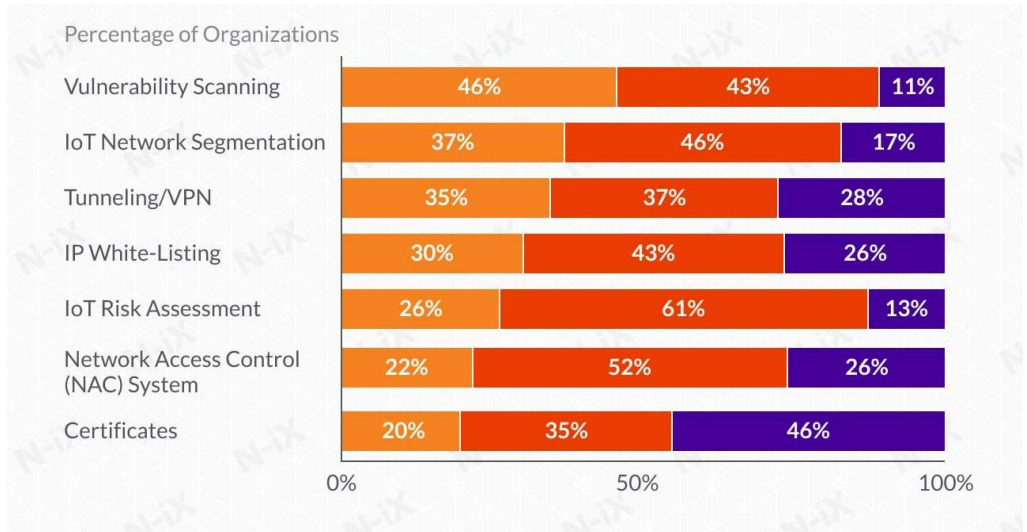
Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly



Mitigasi

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

- ➊ **Lightweight Cryptography** : penggunaan algoritma kriptografi ringan seperti SPECK, PRESENT, atau SIMON untuk perangkat berdaya rendah.
- ➋ **VPN Tunneling dan IPsec** : membangun kanal komunikasi aman untuk data IoT.
- ➌ **Audit Log & ML-based Anomaly Detection** : pencatatan aktivitas dan deteksi perilaku abnormal menggunakan pembelajaran mesin.
- ➍ **End-to-End Encryption (E2EE)** : mengenkripsi data dari sensor hingga aplikasi pengguna.

Konsep Keamanan Data

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Internet of Everything (IoE) menghubungkan berbagai entitas — manusia, proses, data, dan benda — sehingga keamanan data menjadi sangat penting untuk menjaga keandalan sistem. Konsep ini disebut CIA:

- ① *Confidentiality*
- ② *Integrity*
- ③ *Availability*

Prinsip Keamanan Data

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Prinsip CIA Triad:

① Confidentiality (Kerahasiaan)

- Tujuan: Menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang.
- Implementasi: Menggunakan mekanisme autentikasi, kontrol akses, dan enkripsi end-to-end.

② Integrity (Integritas)

- Tujuan: Mencegah perubahan, manipulasi, atau kerusakan data tanpa otorisasi.
- Implementasi: Penggunaan hash functions (misal SHA-256), tanda tangan digital, serta audit log.

③ Availability (Ketersediaan)

- Tujuan: Memastikan data dan layanan selalu tersedia bagi pengguna yang sah.
- Implementasi: Redundancy, load balancing, sistem failover, dan perlindungan terhadap serangan DDoS.

CIA Triad

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly



Pentingnya Privasi IoE

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Isu Umum Privasi

- ➊ **Pengumpulan Data Sensitif** : Perangkat IoE secara kontinu mengumpulkan data seperti lokasi geografis, biometrik, pola aktivitas, dan kebiasaan pengguna. Data ini dapat digunakan untuk analisis perilaku atau profil individu.
- ➋ **Penyimpanan Data di Cloud Lintas Negara** : Banyak layanan IoE menyimpan data pengguna pada data center global, menimbulkan persoalan yurisdiksi hukum dan keamanan lintas batas negara.

Tantangan Utama:

- ➊ **Data Ownership** : Siapa pemilik data yang dihasilkan dari sensor IoE? Pengguna, penyedia layanan, atau pihak ketiga?
- ➋ **Consent Management** : Apakah pengguna memberikan persetujuan eksplisit dan mengetahui bagaimana datanya digunakan serta dibagikan?

Regulasi GDPR (General Data Protection Regulation)

Isi Utama:

1 Hak Subjek Data :

- Akses terhadap data pribadi.

2 Prinsip Pengolahan Data :

- Data Minimization: hanya data yang relevan dan diperlukan yang boleh dikumpulkan.

3 Sanksi dan Kepatuhan :

- Pelanggaran dapat dikenakan denda hingga 4% dari total pendapatan global perusahaan.

4 Implikasi pada IoE :

- Setiap sensor atau perangkat yang mengumpulkan data pribadi wajib memperoleh user consent yang eksplisit dan terdokumentasi.
- Harus tersedia privacy by design dan privacy by default pada arsitektur sistem IoE.

UU Perlindungan Data Pribadi (UU PDP) Indonesia

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Isi Utama:

- **Prinsip Utama UU PDP :**
 - Transparansi: pengguna harus mengetahui tujuan pengumpulan dan pemrosesan datanya.
 - Akuntabilitas: pengendali data wajib menjaga keamanan dan integritas data pribadi.
 - Keamanan: data harus dilindungi dari akses, penggunaan, atau pengungkapan tanpa izin.
- **Hak Subjek Data :**
 - Akses terhadap data pribadi.
 - Koreksi atau pembaruan data.
 - Penghapusan data (right to erasure).

UU Perlindungan Data Pribadi (UU PDP) Indonesia

Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly

Isi Utama:

- **Kewajiban Pengendali Data :**
 - Wajib melaporkan insiden kebocoran data ke otoritas terkait.
 - Wajib memperoleh persetujuan eksplisit sebelum pengumpulan atau pemrosesan data.
- **Implikasi untuk IoE :**
 - Perangkat IoE harus memiliki mekanisme persetujuan eksplisit (explicit consent mechanism).
 - Penyedia layanan wajib menyediakan kebijakan privasi yang mudah diakses dan menjelaskan penggunaan data sensor.

GDPR

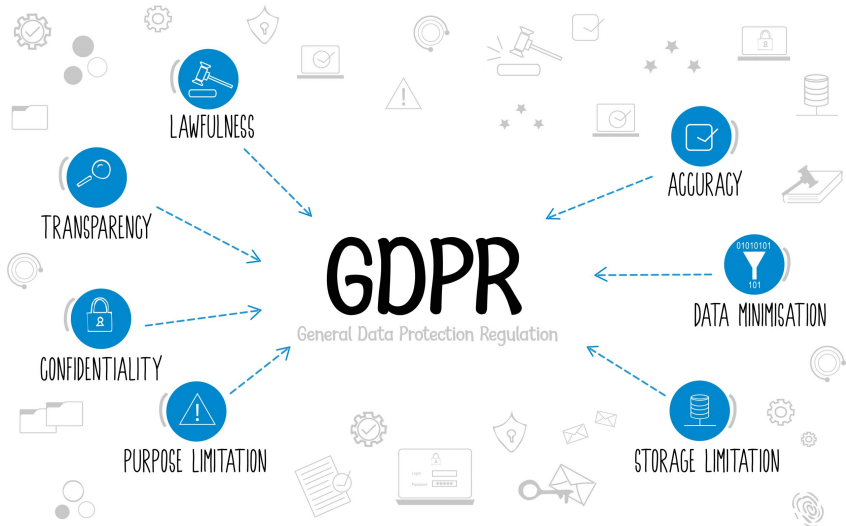
Internet of
Everything
(IoE)

Alauddin
Maulana
Hirzan

Keamanan
IoE

Keamanan
Data IoE

Lastly



Terima Kasih