UNIVERSITAS
GADJAH MADA

LOCALLY ROOTED,
GLOBALLY RESPECTED

Keamanan Siber di Ekosistem Digital Twin

Integrasi IoT, CPS, dan Cybersecurity pada Pembangkit Listrik Modern

Guntur Dharma Putra, PhD
gdputra@ugm.ac.id
Dosen Departemen T Elektro dan T Informasi (DTETI)
Fakultas Teknik UGM

Rakor Satuan *Technology Development & Asset Management* PLN Indonesia Power
16 Desember 2025

ugm.ac.id

Who am I?

Guntur Dharma Putra, PhD

- Dosen Teknologi Informasi, Fakultas Teknik UGM
- Head of Systems Research Group
- Deputi Koordinator Program Magister IT
- Asesor Badan Nasional Sertifikasi Profesi (BNSP)
- Anggota Tim Pokja Blockchain - Metamesta DIKTI
- Anggota IEEE, ACM, PII

Education

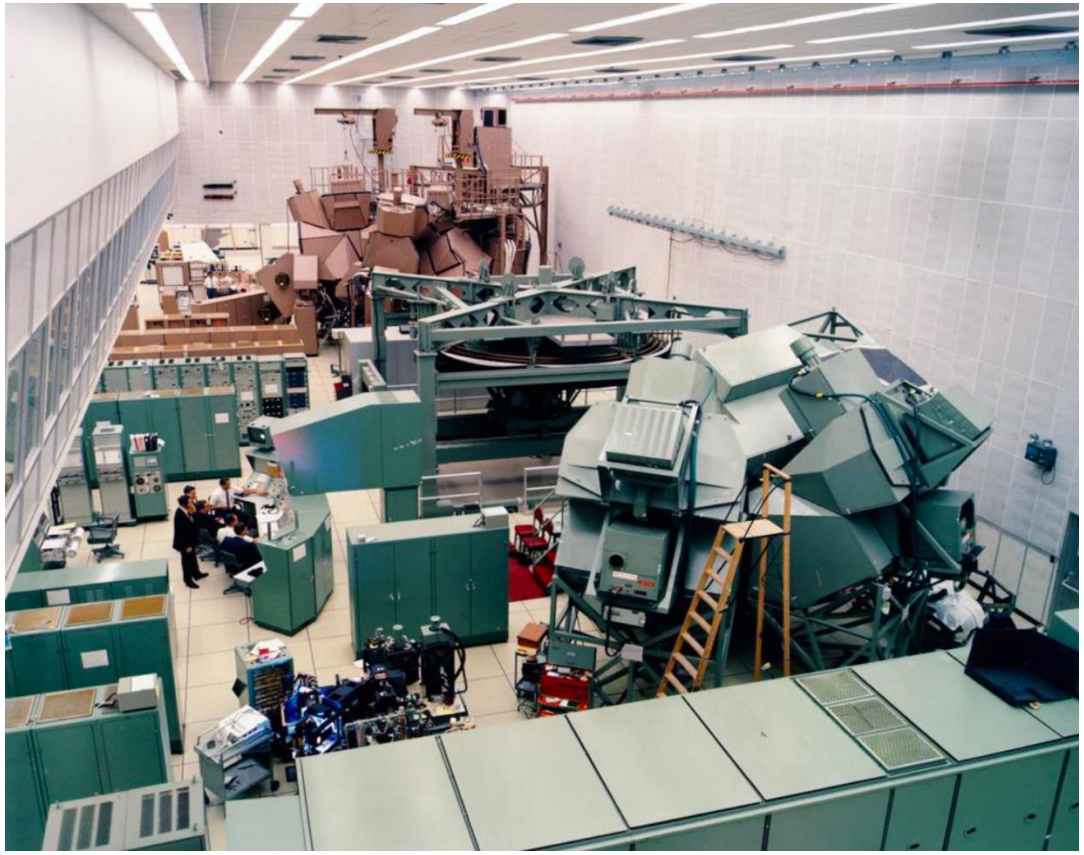
- Sarjana Teknik Elektro UGM ID
- Master's in Computing Science
  University of Groningen, the Netherlands NL
- PhD in Computer Science and Engineering UNSW
  Sydney, Australia AU

Research Area

- Security and privacy
- Blockchain
- Internet of things
- Distributed systems
- Cyber-physical systems

Ide Awal Digital Twin

- Gagasan tentang “digital twin” pertama kali lahir di NASA pada tahun 1960-an
- Sebuah “model hidup” dari misi Apollo 13
- NASA menggunakan berbagai simulator untuk mengevaluasi kegagalan, serta memperluas model fisik wahana dengan memasukkan komponen digital



Apa itu Digital Twin?

Definisi

Digital Twin bukan sekadar simulasi statis. Ia adalah ***representasi digital dinamis*** dari aset fisik yang ***terhubung secara real-time***. Menggunakan gabungan data historis dan live stream untuk mendukung simulasi akurat dan prediksi masa depan.

Lapisan Utama

- **Physical Asset:** Turbin, generator, dan sensor fisik.
- **Data Acquisition:** Jaringan IoT dan telemetri.
- **Digital Model:** Replika virtual presisi tinggi.
- **Analytics & AI:** Pemrosesan data cerdas.
- **Decision Support:** Sistem pendukung keputusan bagi operator.

Simulator vs Digital Twin: Perbedaan Inti

Aspek	Simulator	Digital Twin
Koneksi Aset	✗ Tidak Ada (Offline)	✓ Real-time (IoT)
Data Input	Parameter Asumsi	Sensor Riil & Data Historis
Adaptasi	Statis (Tidak ikut degradasi)	Dinamis (Ikut kondisi aset)
Feedback	Tidak Langsung	Loop Tertutup (CPS)
Risiko Siber	Rendah (Terisolasi)	! Tinggi (Terhubung IT/OT)

Konteks Penggunaan & Miskonsepsi

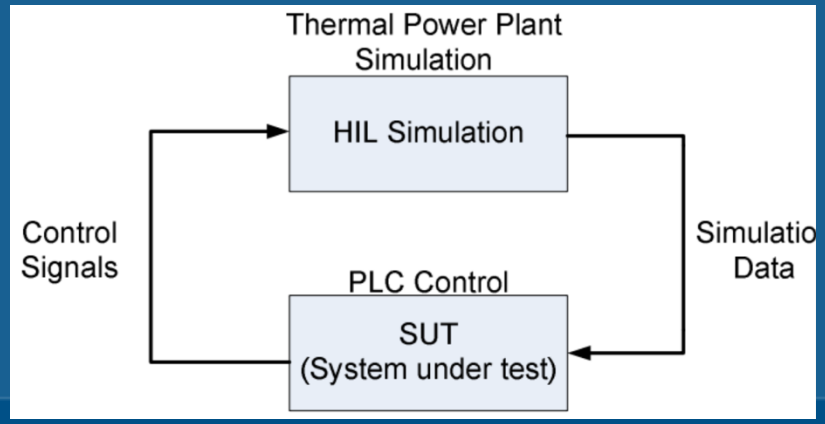
Kapan Menggunakan?

Simulator:

- Tahap desain & prototipe.
- Edukasi & pelatihan operator baru.
- Eksperimen skenario tanpa risiko.

Digital Twin:

- Operasi harian (Monitoring).
- Manajemen aset bernilai tinggi / kritis.
- Keputusan berbasis data *real-time*.



Kesalahan Umum

Menyebut sistem sebagai "Digital Twin" padahal:

- ✗ Tidak terhubung ke aset fisik.
- ✗ Tidak ada update otomatis.
- ✗ Tidak mempengaruhi keputusan operasional.

Simulator:

"What-if" system

Digital Twin:

"As-is" system

IoT sebagai Indra Digital Twin

Sensor & Data

Mengumpulkan parameter vital seperti suhu, tekanan, getaran, dan arus listrik. Data bersifat *high frequency* dan *time-series*.

Protokol

Menggunakan standar industri seperti MQTT, OPC-UA, dan Modbus untuk komunikasi data yang efisien dan interoperabilitas tinggi.

Tantangan

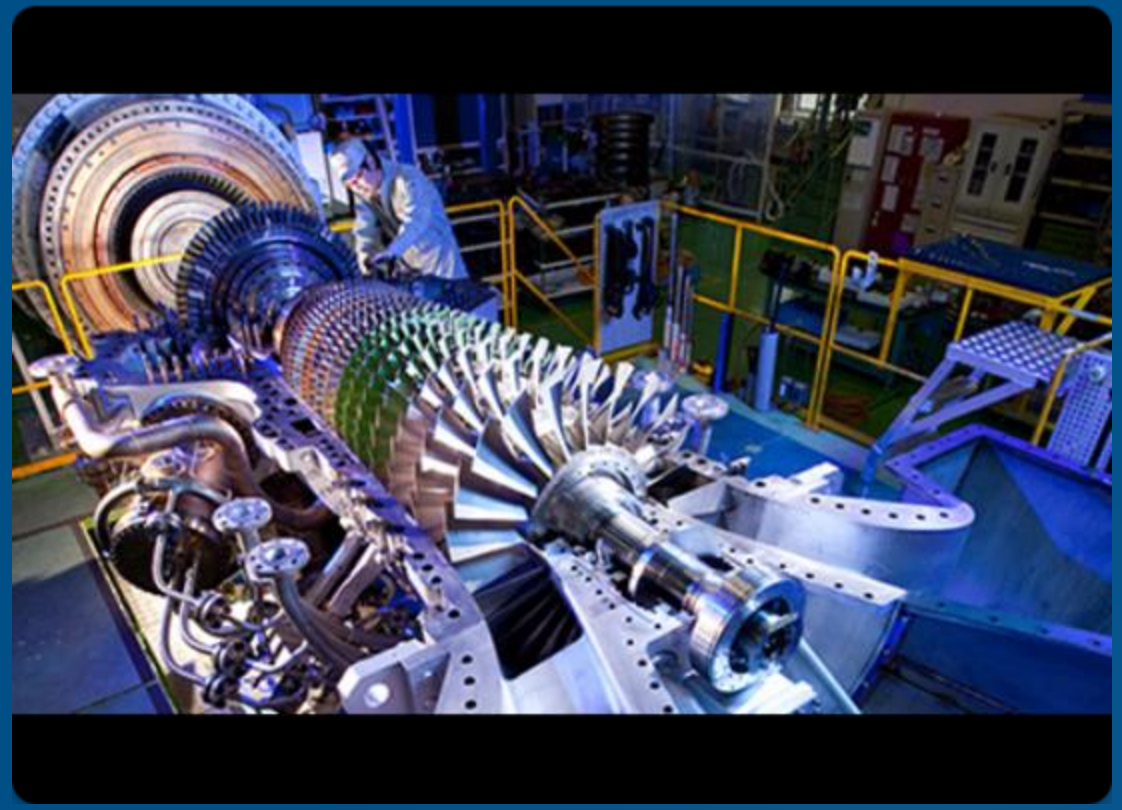
Menghadapi isu keamanan perangkat *endpoint*, skalabilitas jaringan masif, serta tuntutan latensi ultra-rendah.

Digital Twin dalam Cyber-Physical System (CPS)

CPS merupakan integrasi erat antara komputasi, jaringan, dan proses fisik. Digital Twin berfungsi sebagai otak digital dalam loop ini.

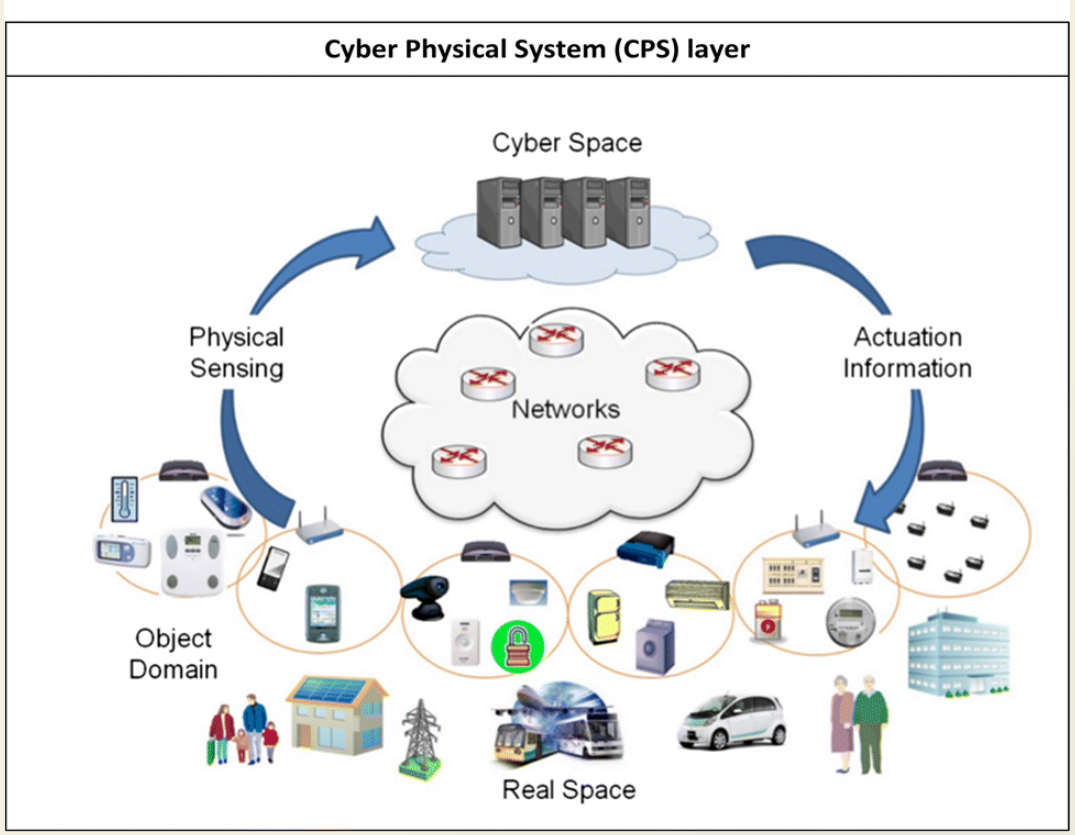
Implementasi Nyata

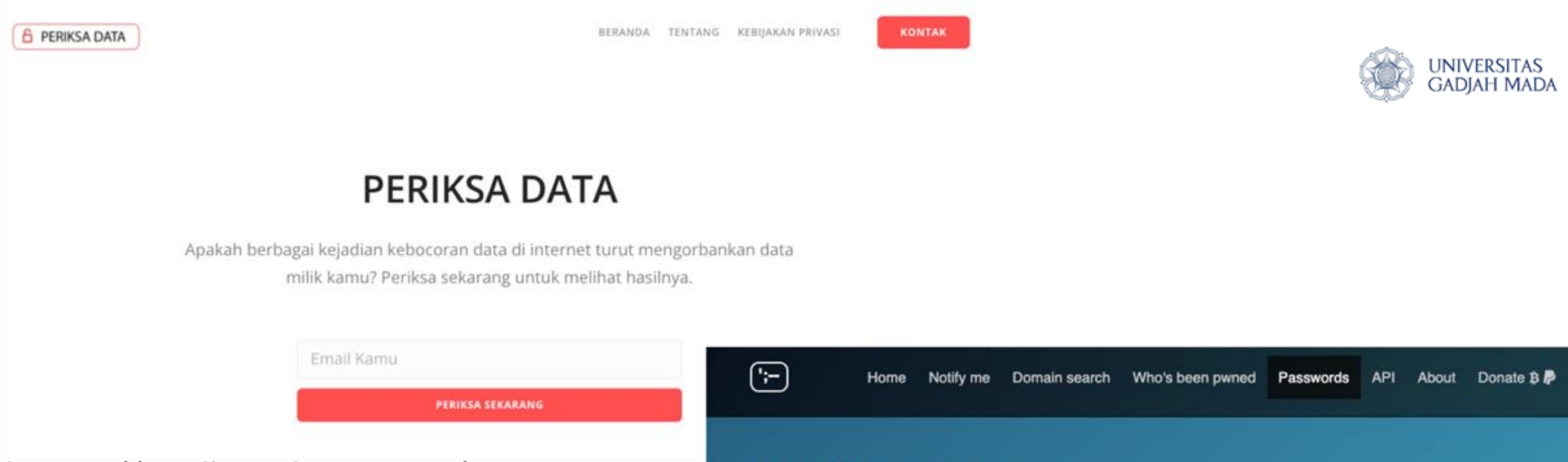
- **Kontrol Beban Otomatis:** Penyesuaian output generator secara real-time berdasarkan fluktuasi permintaan grid.
- **Operasi Berbasis Prediksi:** Penyesuaian parameter turbin sebelum terjadinya anomali, berbasis data sensor preventif.



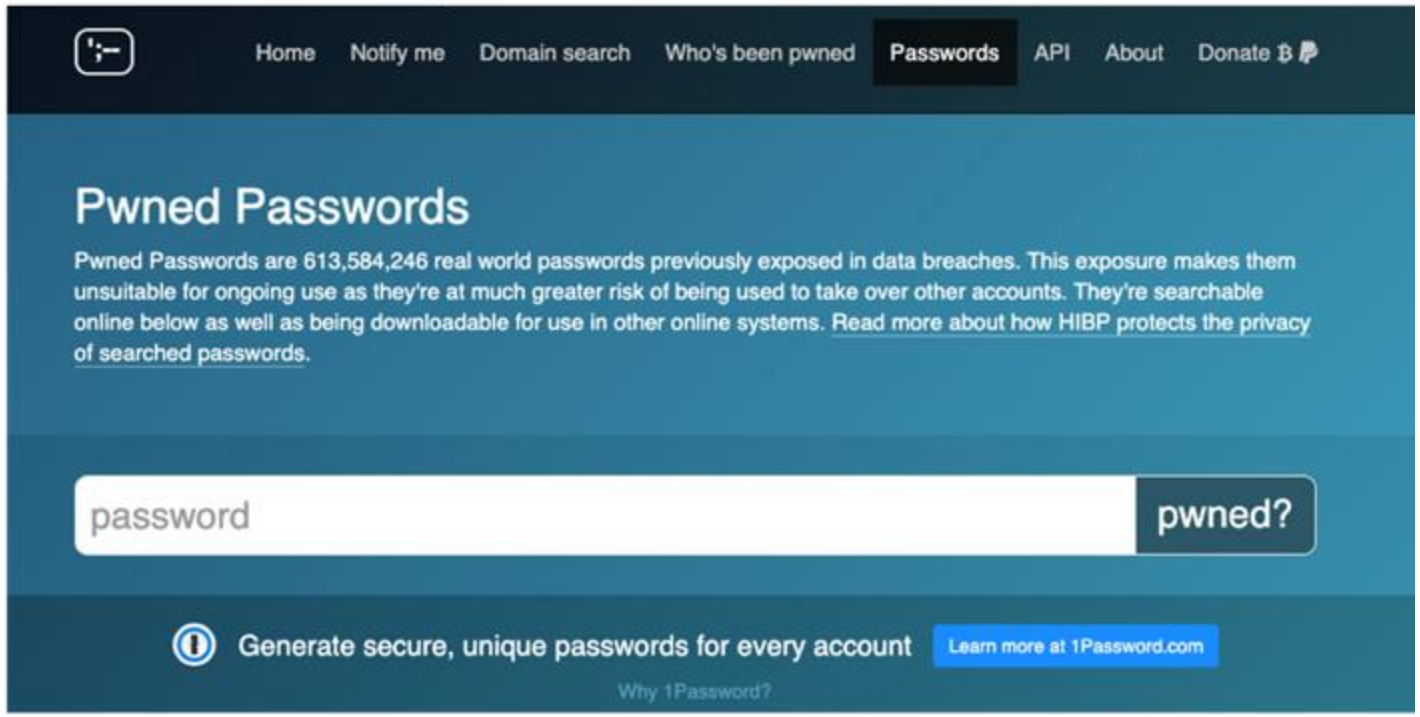
Arsitektur End-to-End

- **Edge Layer:** Titik awal data dari Sensor, PLC, dan RTU yang beroperasi di lapangan.
- **Communication Layer:** Jaringan industri yang aman (Industrial Network) dengan *secure gateways*.
- **Platform Layer:** Mesin inti Digital Twin, Data Lake untuk penyimpanan masif.
- **Application Layer:** Antarmuka untuk Monitoring, Simulasi Skenario, dan Optimalisasi Aset.

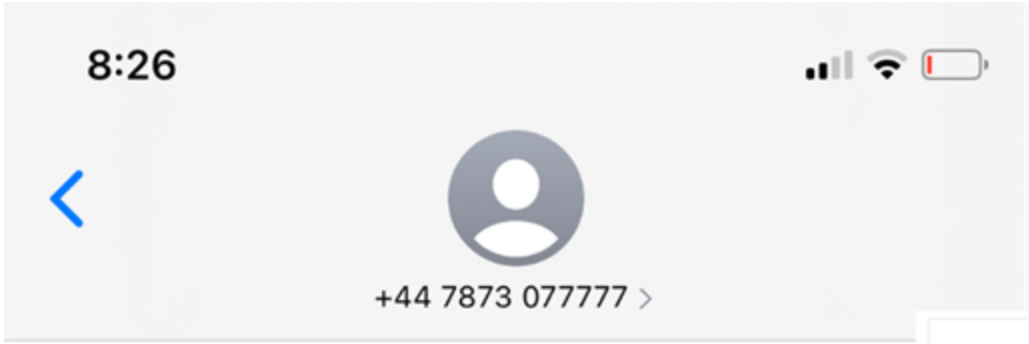




https://periksadata.com/



https://haveibeenpwned.com/Passwords



Text Message
Thu, 14 Oct, 2:47 pm

Your Evernote verification code for guntur.dharma@gmail.com is: 714314

eBay - 52,99 $
14 October 2021
Payment

Paid with
Standard Debit Mastercard 75,39 $ AUD
MasterCard Debit Card x-5639
You'll see "PAYPAL *EBAY US" on your card statement.

on 14 October 2021

Exchange rate
75,39 $ AUD = 52,99 $ USD
1 AUD = 0,7029 USD

Ship to
try AALE
7 Marlboro Rd Unit# 6
Troy, NH 03465-2639
United States

Transaction ID
3717814017718830U

Seller info
eBay
866-540-3229
http://eBay.com/help
https://eBay.com/help

Invoice ID
v2_7fde93c3-d986-4788-811a-e32e6e7ef143_2_12

Note
Order Number : 17-07729-03857

Purchase details
Purchase amount 52,99 $

Total 52,99 $

Threat Landscape: Ancaman Digital Twin

Vektor Serangan

- **IoT Devices:** Serangan fisik langsung atau manipulasi firmware.
- **Data Integrity:** *Data poisoning* yang menyesatkan model analisis.
- **Model Manipulation:** Mengubah algoritma prediksi.
- **Command Injection:** Mengirim perintah berbahaya ke sistem fisik.

Risiko Kritis

- Pengambilan keputusan strategis berbasis data palsu.
- Gangguan operasi pembangkit yang menyebabkan inefisiensi.
- Dampak sistemik katastropik seperti *blackout* total pada jaringan listrik.

Some “Big” Cybersecurity Incident

Malware caused blackouts!

Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world

May 17, 2024
By Emily Cerf

SHARE THIS STORY:

On a cold winter night in 2016, Ukrainians experienced the first-ever known blackout caused by malicious code (malware) designed to autonomously attack the power grid. One-fifth of Kyiv’s citizens were plunged into darkness as attackers used malware to target the capital city’s power grid. Six years later, in the early months of the ongoing Russia-Ukraine war, a second attack attempted to combine kinetic and cyber attacks to take down Ukraine’s power grid.

Power lines in Ukraine. Photo credit: Mny-Jhee, iStock.

Malware attacks against physical infrastructure have long been a looming threat in the realm of cybersecurity, but these two in Ukraine were the first attacks of their kind, and have received little attention from the academic community. Carried out by a Russian intelligence agency against Ukraine, they warn of the evolution of cyber attacks to the built world, and highlight the need to better understand and defend against this type of malware.

Prinsip Cybersecurity by Design

- **Core Philosophy:** Menerapkan pendekatan *Security-by-design* dan *Zero Trust*. Tidak ada perangkat atau user yang dipercaya secara implisit.
- **Defense in Depth:** Perlindungan berlapis mulai dari *Device Security* (TPM, Secure Boot) hingga *Network Security* (Segmentasi, IDS).
- **Data Protection:** Enkripsi end-to-end dan pengecekan integritas data yang ketat untuk mencegah manipulasi.
- **Model Security:** Validasi model secara berkala dan audit trail lengkap untuk setiap perubahan algoritma.

UNIVERSITAS GADJAH MADA

Secure Digital Twin Architecture

Digital Twin memiliki peran ganda: sebagai konsumen data sensitif dan sebagai objek kritis yang harus diamankan.

Pendekatan Keamanan:

- **Trusted Data Pipeline:** Menjamin keaslian data dari sensor hingga cloud.
- **Anomaly Detection:** Menggunakan twin untuk mendeteksi perilaku abnormal pada aset fisik.
- **Secure Update:** Manajemen versi model yang aman dan terenkripsi.

Tantangan Implementasi Nyata

- **Integrasi Sistem Legacy:** Menggabungkan mesin tua dengan sensor IoT modern adalah tantangan teknis utama.
- **Kualitas Data:** "Garbage in, garbage out". Data yang buruk menghasilkan prediksi yang salah.
- **SDM Lintas Disiplin:** Kebutuhan akan talenta yang memahami OT (Operational Technology) sekaligus IT Security.
- **Biaya & ROI:** Investasi awal yang besar membutuhkan justifikasi ROI yang jelas.

Kesimpulan Utama

- Digital Twin adalah **jantung operasi** pembangkit modern, bukan sekadar pelengkap.
- Integrasi **IoT & CPS** membuka pintu untuk wawasan real-time yang sebelumnya mustahil.
- **Cybersecurity** adalah prasyarat mutlak. Tanpa keamanan, Digital Twin adalah celah risiko.
- Ekosistem yang aman menjamin operasi yang **andal, efisien, dan berkelanjutan**.

UNIVERSITAS
GADJAH MADA

Matur nuwun.

Guntur Dharma Putra, PhD
gdputra@ugm.ac.id