Jurnal Sistim Informasi dan Teknologi

https://jsisfotek.org/index.php

2023 Vol. 5 No. 2 Hal: 26-32 e-ISSN: 2686-3154

Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi

Fauzan Prasetyo Eka Putra[1], Selly Mellyana Dewi[2]✉, Maugfiroh[3], Amir Hamzah[4]

[1,2,3,4]Universitas Madura

sellymd19@gmail.com

Abstrak

Kevin Ashton adalah pencipta Internet of Things (IoT) pada tahun 1999. Meskipun telah diperkenalkan 15 tahun lalu, Hingga kini belum ada definisi yang jelas tentang Internet of Things (IoT). Namun, kebanyakan orang mengartikannya sebagai kemampuan untuk menghubungkan objek cerdas dan memungkinkannya berinteraksi melalui jaringan internet dengan objek lain, lingkungan, dan peralatan komputasi cerdas lainnya. Internet of Things (IoT) telah mulai diterapkan pada banyak aspek kehidupan manusia dalam berbagai bentuknya. CISCO bahkan mengantisipasi bahwa pada tahun 2020, 50 miliar objek akan terhubung ke internet. Kehidupan manusia menjadi lebih mudah karena banyaknya teknologi Internet of Things yang diadopsi. Jika dilihat dari perspektif pengguna individu, Internet of Things sangat berdampak pada sektor domestik, seperti aplikasi untuk rumah dan mobil cerdas. Jika dilihat dari perspektif penguna bisnis, IoT sangat berdampak pada kualitas dan jumlah produksi produk, pengawasan distribusi produk, pencegahan pemalsuan, manajemen rantai pasokan, dan mempersingkat waktu ketidak tersediaan produk di pasar retail. Menurut Fawzi Behmann IoT merupakan istilah dari penggunaan internet dalam skala yang lebih besar, menjadikan komputasi yang bersifat mobile dan konektifitas lalu menggabungkannya dalam kegiatan sehari-hari. Internet of Things (IoT) telah memberikan keuntungan dalam memudahkan aktivitas manusia di kehidupan sehari-hari, perkembangnya sangat pesat dan akan terus menerus berkembang lebih baik dari masa ke masa, namun penerapannya di tengah kalangan masyarakata saat ini juga memunculkan tantangan dan implikasi terkait keamanan dan privasi.

Kata kunci: Internet of Things, Keamanan, Privasi, Internet, Network.

1. Pendahuluan

IoT mengacu pada konsep yang melibatkan koneksi dan perpaduan antar berbagai perangkat fisik, objek maupun sistem dengan jaringan internet. Memungkinkan perangkat saling berkomunikasi, bertukar data, dan bertindak sesuai instruksi pengguna.

IoT melibatkan beberapa komponen penting, yakni :

a. Jaringan : Melibatkan beberapa perangkat pada jaringan dan internet, seperti ethernet, Wi-Fi, ataupun blutooth dan jaringan seluler.
b. Perangkat dan sensor : perangkat elektronik yang dilengkapi dengan perangkat sensor, perangkat pemrosesan dan kemampuan komunikasi untuk mengumpulkan data, memantau sistem dan objek fisik serta berinteraksi.
c. Data : data bisa berisi tentang informasi mengenai perangkatnya sendiri, tindakan pengguna, atau status lainnya.
d. Komputasi : Kemampuan untuk pemrosesan dan menganalisis data yang dibutuhkan.
e. Aplikasi dan layanan : memanfaatkan data yang dikumpulkan oleh perangkat itu sendiri yang melibatkan analisis,visualisasi, tindakan, dan interaksi.

IoT memiliki dampak dan implikasi yang luas dalam berbagai sektor seperti kesehatan, infrastruktur, teknologi, pertanian dan semacamnya yang dapat memberikan dampak manfaat dari berbagai sektor tersebut. Internet of things atau yang biasa di sebut dengan (IoT) ini pada masa saat ini telah berkembang sangat pesat dan akan terus menerus berkembang lebih baik lagi dimasa yang akan datang. Dan dapat di pastikan suatu saat akan ada jutaan smart device terbaru dengan segala berbagai ragam manfaatnya. Namun, semakin banyak kelebihan kelebihan ini juga akan banyak pula berbagai kekurangan.

1.1. Konsep keamanan dalam IoT

Keamanan dalam IoT adalah sebuah praktik yang menjaga sebuah sistem IoT anda agar tetap aman. Alat keamanan IoT ini juga dapat melidungi dari sebuah ancaman dan sebuah pelanggaran dan juga mengidentifikasi dan menyatukan sebuah resiko. Dan juga dapat membantu memperbaiki kerentanan. Dan keamanan IoT inilah yang dapat memastikan ketersediaan. Kerahasiaan solusi IoT anda dan juga integritas. Sedangkan pentingnya keamanan privasi dan IoT ialah IoT dan privasi harus disatukan. IoT menghubungkan segalanya, dan privasi membedakan

Diterima: 20-06-2023 | Revisi: 23-06-2023 | Diterbitkan: 08-07-2023 | doi: 10.37034/jsisfotek.v5i1.232

semuanya. Meskipun demikian, di dunia yang semakin saling berhubungan, pengembang, produsen, dan konsumen harus tetap mempertahankan privasi. Internet Data atau data yang Pribadi sering disebut sebagai Internet of Things (IoT). Data pribadi ini adalah data yang pelumas IoT jika data adalah oli baru. Perangkat yang terhubung ke internet dibanjiri data sensitif. Selain itu, di era hiperkonektivitas ini, pelanggaran privasi menanggung beban terberat dari koneksi yang tak terhindarkan antara data dan perangkat. Konsep-konsep keamanan dalam sebua IoT (internet of things) ada bentuk serangkaian langkah serta tindakan yang telah di rancang untuk mengamankan juga melindungi perangkat IoT dan data-data yang telah di kumpulkan,di terima dan juga kirim. Keamanan IoT inilah yang sangat penting dikarenakan perangkat ini sering kali terhubung dengan jaringan yang sangat rentan dan juga dapat menyebabkan sebuah kerentanan dan juga keamanan yang luas jika tidak terlindungi dengan baik dan benar. Di bawah ini adalah konsep-konsep keamanan dalam IoT yang sangat penting untuk di ketahui.

a. Indentifikasi dan otentikasi
   Hal ini sangat penting untuk memastikan bahwa pada setiap perangkat yang akan terhubung pada jaringan IoT diindentifikasi dan diauntentikasi secara tepat sebelum diberikan perizinan untuk mengakses jaringan atau juga berinteraksi dengan sebuah perangkat lainnya. Hal yan demikian ini melibatkan penggunaan sebuah protokol keamanan seperti SSL/TLS dan juga sertifikat digital guna untuk mengauntentikasi sebuah perangkat.
b. Enkripsi Data
   Data yang akan dikirim melalui jaringan IoT harus dienkripsi untuk melindungi rahasia dan integritas di dalmnya.
c. Keamanan jaringan
   Jaringan IoT harus di lindungi menggunakan firewall,deteksi intrusi dan sebuah tindakan pencegahan sebuah datangnya resiko serangan tidak baik dari luar. Selain itu segmentasi jaringan ini dapat digunakan untuk memisahkan antara perangkat data dan data yang kritis dari sebuah akses yang tidak terotorisasi.
d. Menejemen akses dan otorisasi
   Mengelola sebuah akses serta otorisasi pengguna atau juga perangkat dalam jaringan IoT sangatlah penting. Bagi Pengguna harus memiliki tingkatan akses yang sesuai dengan peran serta tanggung jawab mereka, sedangkan perangkat ini harus diberikan perizinan yang tepat untuk melakukan interaksi dengan perangkat-perangkat lain atau juga mengakses data tertentu.
e. Pemantauan keamanan
   Sistem-sistem pemantauan dan deteksi sebuah ancaman keamanan yang sangat perlu untuk diimplementasikan sebagai mendeteki serangan atau aktivitas yang mencurigakan dalam suatu jaringan IoT. Ini dapat juga melibatkan penggunaan solusi keamanan seperti Intrusion Detection System (IDS) atau Security Information and Event Management (SIEM).
f. Pembaruah perangkat lunak
   Perangkat lunak kepada perangkat IoT yang harus diperbarui secara teratur agar dapat memastikan bahwa ada celah keamanan yang diketahui telah diperbaiki. Ini juga melibatkan pembaruan pada firmware dan serta perangkat-perangkat lunak dengan versi yang lebih baru lagi , yang akan dirilis oleh produsen.
g. Keamanan fisik
   Selain keamanan perangkat lunak ini ada juga ada perangkat keras IoT yang harus dilindungi secara fisik. Tindakan seperti ini penggunaan nya slot kartu SIM yang terkunci, penempatan perangkat ini di area yang aman, serta tindakan pencegahan fisik lainnya ini pun dapat membantu mencegah pencurian perangkat atau akses fisik yang tertulis tidak sah.
h. Pengujian keamanan
   Pengujian keamanan ini yang komprehensif harus juga dilakukan pada perangkat IoT sebelum dan juga selama implementasi. Hal Ini termasuk pengujian penetrasi, pengujian kekuatan, dan juga termasuk skenario ancaman lainnya untuk mengidentifikasi kelemahan potensi.

1.2. Tantangan privasi IoT yang perlu di perhatikan

Meskipun IoT menawarkan banyak manfaat dan kemudahan, ada beberapa tantangan privasi yang perlu diperhatikan:

a. Pengumpulan data yang luas: IoT ini menghasilkan sejumlah data yang berukuran besar dari berbagai sumber-sumber. Pada Setiap perangkat IoT ini juga dapat mengumpulkan data tentang aktivitas-aktivitas pengguna, preferensi, lokasi, dan lainnya. Tantangan privasi ini akan terkait dengan pengumpulan, penggunaan, dan penyimpanan data ini penting untuk dipahami serta bisa teratasi.
b. Keamanan data: Karena pada perangkat IoT ini bisa terhubung pada internet, mereka rentan terhadap berbagai serangan-serangan siber. Jika perangkat tidak memiliki langkah-langkah keamanan yang memadai, dalam data-data pribadi yang dikumpulkan oleh perangkat IoT dapat terakses oleh pihak yang tidak bertanggung jawab. Perlindungan dat ini a harus menjadi prioritas untuk menjaga keamanan privasi pengguna.

c. Identifikasi individu: Dalam beberapa study kasus, data yang dikumpulkan oleh perangkat IoT dapat mengungkap identitas individu secara langsung atau bahkan tidak langsung. Seperti, melalui berbagai pola aktivitas sehari-hari atau informasi geografis yang dikumpulkan oleh perangkat pintar di rumah, manusia dapat dengan mudah mengidentifikasi kebiasaan dan rutinitas individu tersebut. Ini bahkan dapat mengancam privasi serta keamanan individu jika data ini jatuh kepada tangan-tangan yang salah.
d. Kontrol pengguna: Penggunaan perangkat IoT bisa mengarahkan pada kehilangan kontrol pengguna atas data-data pribadi mereka. Pengguna harus bisa memahami dan mengendalikan penggunaan data mereka oleh perangkat IoT serta pihak lain yang terlibat dalam ekosistem IoT. Kejelasan dan transparansi dalam kebijakan privasi serta opsi untuk mengontrol bagaimana data dikumpulkan juga digunakan adalah bernilai penting.
e. Akses data oleh pihak ketiga: Dalam banyaknya study kasus, data yang dikumpulkan oleh perangkat IoT dapat dibagikan dengan pihak ketiga seperti penyedia layanan, pengiklan, atau mitra bisnis. Ketika data pribadi ini dikirimkan atau dibagikan kepada pihak ketiga, risiko nya akan membuat privasi meningkat. Dan diperlukan kebijakan serta persyaratan yang jelas tentang bagaimana data akan digunakan dan dengan siapa data-data ini dapat dibagikan.

Untuk mengatasi tantangan privasi dalam IoT, beberapa langkah dapat diambil, seperti:
Mengenkripsi data untuk melindungi kerahasiaan dan integritasnya saat data berpindah di jaringan.
Mengembangkan kebijakan privasi yang jelas dan transparan yang menjelaskan pengumpulan, penggunaan, dan penyimpanan data.Memastikan keamanan perangkat IoT dengan menerapkan langkah-langkah keamanan yang memadai, seperti autentikasi yang kuat dan pembaruan perangkat lunak teratur.
Mengembangkan persyaratan hukum dan regulasi yang memperhatikan privasi pengguna dan memberikan perlindungan yang memadai.Memberikan kesadaran dan edukasi kepada pengguna tentang risiko privasi yang terkait

1.3. Framework dan standar keamanan privasi

Dalam konteks Internet of Things (IoT), ada beberapa framework dan standar yang digunakan untuk menjaga keamanan dan privasi data. Beberapa di antaranya adalah:

a. NIST Cybersecurity Framework: Framework ini dikembangkan oleh National Institute of Standards and Technology (NIST) di Amerika Serikat. Framework ini memberikan panduan tentang cara menyusun, mengimplementasikan, dan meningkatkan program keamanan cyber. NIST Cybersecurity Framework terdiri dari lima komponen inti, yaitu Identifikasi (Identify), Melindungi (Protect), Mendeteksi (Detect), Menanggapi (Respond), dan Memulihkan (Recover). Framework ini membantu organisasi mengidentifikasi risiko keamanan dan mengembangkan strategi mitigasi yang efektif.
b. ISO/IEC 27001: Standar ini adalah standar internasional untuk manajemen keamanan informasi. ISO/IEC 27001 memberikan kerangka kerja yang komprehensif untuk mendesain, mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan sistem manajemen keamanan informasi (ISMS). Standar ini memberikan panduan tentang bagaimana organisasi dapat mengelola keamanan informasi mereka secara efektif, termasuk dalam konteks IoT.
c. General Data Protection Regulation (GDPR): GDPR adalah regulasi privasi data yang berlaku di Uni Eropa. Regulasi ini memberikan kerangka kerja yang ketat untuk melindungi privasi data individu. GDPR memberikan hak kepada individu untuk mengontrol penggunaan dan pemrosesan data pribadi mereka oleh organisasi. Dalam konteks IoT, GDPR mengharuskan organisasi untuk mengumpulkan dan mengelola data pribadi secara sah, memberikan transparansi kepada individu tentang penggunaan data, dan melindungi data dari pelanggaran keamanan.

Selain framework dan standar tersebut, ada juga beberapa inisiatif dan standar lain yang relevan untuk keamanan dan privasi dalam IoT, seperti:

a. OWASP IoT Top 10: Inisiatif ini menyusun daftar sepuluh risiko keamanan teratas yang berkaitan dengan perangkat IoT, dan memberikan saran tentang bagaimana mengurangi risiko tersebut.
b. IEC 62443: Standar ini dikembangkan oleh International Electrotechnical Commission (IEC) dan menyediakan panduan dan spesifikasi untuk keamanan sistem kontrol industri termasuk dalam konteks IoT.
c. ENISA IoT Security Baseline: European Union Agency for Cybersecurity (ENISA) menyediakan pedoman dan prinsip dasar untuk keamanan IoT yang meliputi identifikasi risiko, keamanan jaringan, dan perlindungan data.

Penting untuk dicatat bahwa keamanan dan privasi dalam konteks IoT adalah bidang yang terus berkembang, dan selalu ada upaya untuk mengembangkan kerangka kerja dan standar baru yang lebih sesuai dengan tantangan dan tren terkini dalam keamanan dan privasi data IoT.

1.4. Metode keamanan

Berikut adalah beberapa teknik keamanan Internet of Things yang umum digunakan.:

a. Enkripsi data: Protokol enkripsi yang kuat seperti SSL/TLS dapat mencegah pencegatan dan penyusupan data saat data dikirim dan diterima antara perangkat IoT dan jaringan.
b. Otorisasi dan otentikasi: Menggunakan mekanisme otorisasi dan otentikasi untuk memastikan bahwa hanya perangkat yang sah dan pengguna yang memiliki hak akses dapat berinteraksi dengan sistem IoT. Mekanisme ini dapat mencakup penggunaan sertifikat digital, kata sandi, atau teknologi biometrik untuk memverifikasi identitas pengguna atau perangkat.
c. Perbarui perangkat lunak rutin: Pembaruan keamanan dari produsen dapat memastikan bahwa perangkat IoT memiliki perangkat lunak terbaru. Pembaruan ini dapat memperbaiki kerentanan yang ditemukan dan meningkatkan keamanan sistem secara keseluruhan.
d. Segregasi jaringan: Membuat jaringan Internet of Things terpisah dari jaringan utama atau jaringan pribadi yang lebih sensitif. Dengan melakukan ini, serangan pada perangkat Internet of Things tidak akan langsung mengancam jaringan inti atau data penting lainnya.
e. Pengawasan lalu lintas jaringan: Solusi pengawasan jaringan seperti analisis lalu lintas jaringan, pemantauan aktivitas perangkat, dan deteksi serangan berbasis perilaku memungkinkan identifikasi dan deteksi aktivitas yang mencurigakan atau serangan potensial.
f. Pengelolaan akses dan izin: Mengontrol akses dan izin perangkat IoT terhadap data dan sumber daya sistem. Hanya memberikan izin yang diperlukan untuk operasi tertentu dan memastikan bahwa perangkat tidak memiliki akses yang berlebihan.
g. Keamanan fisik: Mengamankan perangkat IoT secara fisik untuk mencegah orang yang tidak berhak mengaksesnya atau mencurinya. Ini dapat mencakup penggunaan kunci fisik, pengamanan perangkat keras, atau penggunaan tempat penyimpanan yang aman.
h. Deteksi dan respons terhadap ancaman: Menggunakan sistem deteksi ancaman yang efektif dan merespons serangan atau insiden keamanan dengan cepat. Ini dapat mencakup penggunaan sistem deteksi intrusi, pemantauan aktivitas perangkat, atau teknologi kecerdasan buatan (AI) untuk mengenali pola serangan.
i. Pemisahan data sensitif: sangat penting untuk memisahkan dan mengenkripsi data sensitif yang diproses oleh perangkat IoT. Ini memastikan bahwa data sensitif tetap terlindungi bahkan jika perangkat IoT terinfeksi atau dikompromikan.
j. Pendidikan dan kesadaran pengguna: Mengajarkan pengguna tentang pentingnya keamanan IoT, termasuk cara terbaik untuk mengelola perangkat IoT dan menjaga keamanan data. Ini termasuk menggunakan kata sandi yang kuat, menggunakan perangkat lunak terbaru, dan menghindari terhubung ke jaringan yang tidak aman.

Selain teknik di atas, bidang keamanan IoT terus berkembang, seperti penggunaan blockchain untuk menciptakan catatan transaksi yang aman dan auditabilitas dalam jaringan IoT. Perlindungan dan metode keamanan yang kuat harus diperbarui secara teratur untuk melindungi sistem IoT dari serangan dan pelanggaran keamanan.

1.5. Implikasi hukum dan etika

Ada beberapa konsekuensi hukum dan etika yang perlu dipertimbangkan saat IoT dikembangkan dan digunakan.

a. Privasi dan Keamanan Data: IoT mengumpulkan dan mengirimkan banyak data antara berbagai perangkat yang terhubung, jadi penting untuk melindungi data pribadi pengguna dari penyalahgunaan atau akses oleh pihak yang tidak berwenang.
b. Pengumpulan dan Penggunaan Data: Internet of Things mengumpulkan banyak data tentang kebiasaan, preferensi, dan perilaku pengguna. Ada konsekuensi etika terkait dengan cara data dikumpulkan, digunakan, dan dikelola. Sangat penting untuk membuat peraturan yang jelas tentang penggunaan data dan memastikan bahwa pengguna tahu apa yang dilakukan dengan data mereka.
c. Tanggung Jawab Produk dan Keamanan: Internet of Things (IoT) mencakup penggunaan perangkat yang terhubung ke internet. Tanggung jawab hukum dan etika terkait dengan tanggung jawab produsen dalam memastikan keamanan perangkat dan perlindungan terhadap serangan siber. Untuk melindungi pengguna dari potensi ancaman keamanan, produsen harus secara teratur memperbarui keamanan perangkat dan perangkat lunak.
d. Ketergantungan Teknologi: Implikasi etika terkait dengan ketergantungan pengguna pada teknologi IoT. Kegagalan sistem atau kelalaian dapat memiliki konsekuensi yang signifikan dalam beberapa kasus, jadi penting untuk mempertimbangkan implikasi etika dan memastikan bahwa ada alternatif atau solusi backup tersedia jika terjadi kegagalan sistem.
e. Pematuhan Regulasi dan Standar: Produsen dan pengguna IoT harus memastikan bahwa mereka mematuhi peraturan dan standar yang berlaku saat mengembangkan dan menggunakan IoT. Ini termasuk mematuhi peraturan tentang privasi data, keamanan jaringan, dan standar keselamatan.

f. Dampak Lingkungan: Implikasi etika dari penggunaan Internet of Things juga mencakup dampak lingkungan. Perlu diperhatikan penggunaan energi yang efisien, manajemen limbah elektronik, dan siklus hidup produk IoT untuk mengurangi dampak negatif pada lingkungan. Ini penting untuk mendorong praktik yang berkelanjutan untuk mengurangi dampak negatif tersebut.

Ketika mengembangkan dan menggunakan teknologi Internet of Things (IoT), sangat penting untuk mempertimbangkan konsekuensi hukum dan etika ini. Pengguna, produsen, dan bisnis harus bertanggung jawab atas perlindungan privasi, keamanan data, dan keselamatan dan keberlanjutan lingkungan. Untuk mengatasi masalah ini dan mendorong penggunaan IoT yang bertanggung jawab, juga diperlukan regulasi yang tepat.

1.6. Metode yang di gunakan dalam IoT

Ada beberapa metode yang umum digunakan dalam Internet of Things (IoT). Berikut ini beberapa metode yang sering digunakan dalam pengembangan solusi IoT:

a. Sensor dan Perangkat Terhubung: Internet of Things menggunakan sensor dan perangkat terhubung untuk mengumpulkan data dari lingkungan fisik. Sensor dapat berupa suhu, kelembaban, cahaya, gerak, tekanan, atau jenis lainnya. Perangkat terhubung dapat berupa perangkat mobile, mikrokontroler, atau perangkat pintar yang terhubung ke internet.
b. Komunikasi Jaringan: Internet of Things menggunakan protokol jaringan seluler seperti 3G, 4G, dan 5G, serta Wi-Fi, Bluetooth, Zigbee, Z-Wave, dan NFC (Komunikasi Daerah Dekat).
c. Komputer awan: Internet of Things sering kali menggunakan layanan cloud untuk pemrosesan, penyimpanan, dan analisis data. Data yang dikumpulkan dari perangkat IoT dikirim ke cloud untuk disimpan dan dianalisis, dan layanan cloud juga memungkinkan penggunaan sumber daya komputasi yang fleksibel dan skalabilitas untuk menangani beban kerja yang besar dari Internet of Things.
d. Analisis Data: Teknik analisis data seperti pemrosesan real-time, pemrosesan streaming, analisis prediktif, dan pembelajaran mesin dapat digunakan dalam pendekatan ini untuk mendapatkan informasi bermanfaat dari banyak data yang dihasilkan oleh perangkat Internet of Things (IoT).
e. Keamanan: Keamanan merupakan komponen penting dalam pengoperasian Internet of Things. Teknik keamanan seperti enkripsi data, otentikasi perangkat, otorisasi akses, pemantauan ancaman, dan perlindungan privasi sangat penting untuk melindungi data yang dikirim melalui jaringan dan memastikan bahwa hanya orang yang berwenang yang dapat menghubungi perangkat Internet of Things.
f. Protokol Komunikasi: Internet of Things menggunakan protokol khusus untuk memungkinkan perangkat berkomunikasi satu sama lain dan dengan sistem lainnya. Contoh protokol komunikasi yang umum digunakan dalam Internet of Things adalah MQTT (Pengiriman Pesan Telemetri), CoAP (Protokol Penggunaan Terbatas), dan HTTP (Protokol Pengiriman Hypertext).
g. Pemrosesan tepi: Teknik ini memproses data di perangkat tepi (edge device) atau gateway secara lokal sebelum dikirim ke cloud. Memproses data di tepi jaringan dapat mengurangi latensi dan menghemat bandwidth jaringan. Aplikasi yang membutuhkan pemrosesan real-time atau respons cepat sering menggunakan edge computing.

Setiap metode ini dapat digunakan untuk membuat solusi IoT. Setiap metode dapat disesuaikan dengan kebutuhan dan kondisi aplikasi IoT tertentu.

2. Metode Penelitian

a. Observasi: Dilakukan beberapa tahap observasi terhadap penelitian yang dilakukan agar mendapatkan hasil penelitian.
b. Wawancara: Dilakukan juga sesi wawancara dari beberapa sumber terkait tentang penelitian yang dilakukan.

3. Hasil dan Pembahasan

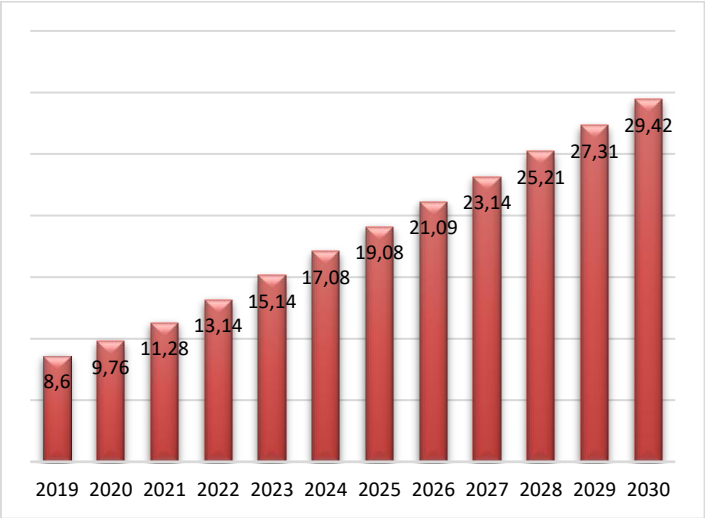
Rangkaian hasil penelitian berdasarkan urutan/susunan logis untuk membentuk sebuah cerita. Isinya menunjukan fakta/data dan jangan diskusikan hasilnya. Dapat menggunakan Tabel dan Angka tetapi tidak menguraikan secara berulang terhadap data yang sama dalam gambar, tabel dan teks. Untuk lebih memperjelas uraian, dapat mengunakan sub judul.

Pembahasan adalah penjelasan dasar, hubungan dan generalisasi yang ditunjukkan oleh hasil. Uraiannya menjawab pertanyaan penelitian. Jika ada hasil yang meragukan maka tampilkan secara objektif.

3.1. Spesifikasi

Terdapat implikasi dan tantang terhadap IoT dalam pengembangan sehari-hari karena terdapat beberapa elemen didalamnya yang terdukung teknologi.

Menurut Lionel Sujay Vailshery selaku pakar riset di bidang industri elektronik konsumen, penggunaan konsumen terhadap perangkat yang terhubung dengan IoT di prediksi meningkat pesat bahkan sampai pada tahun 2030. Bahkan penggunaan perangkat yang terhubung pada IoT meningkat pesat daripada barang non elektronik.



Gambar 1. Data penggunaan barang IoT

Penggunaan barang IoT pada tahun 2023 hampir dua kali lipat meningkat dibandingkan pada tahun 2019. Tak dapat dipungkiri, penggunaan IoT banyak digunakan di berbagai sektor.
Kasus penggunaan perangkat IoT di segmen konsumen adalah smartphone yang merupakan perangkat internet yang diperkirakan akan meningkat pesat menjadi 17miliar pada tahun 2030.

Di Indonesia, maraknya penggunaan IoT berkembang sejak tahun 2018 dengan berbagai perangkat seperti smartwatch.
"Mengenai perkembangan IoT, pada tahun 2014 diperkirakan 16 miliar perangkat yang terkoneksi dan pada tahun 2021 diperkirakan menjadi 28 miliar. Pada tahun 2020 meningkat menjadi 31 miliar." Anton.
Anton megatakan bahwasannya perkembangan IoT di Indonesia sudah termasuk jauh dan memperkirakan tahun berikutnya semakin meningkat dibandingkan penggunaan smartphone sendiri.

4. Kesimpulan

Studi menganalisis dampak kemanan dan privasi yang muncul tentang IoT yang memberikan banyak manfaat yang signifikan begitupun dengan konsekuensi yangdigunakan. Tantangan privasi dalam penerapan IoT meliputi pengimputan data yang lebih luas, kebocoran data, dan penggunaan data tanpa persetujuan penggunaan yang bisa meningkatkan terjadinya pelanggaran privasi, sehingga pentinguntuk implementasi perangkat antar pengguna.
Tak hanya itu, serangan cyber menjadi dapat menyebabkan kerugian yang mana contoh kasus seperti pencurian data.
Implikasi dari hal ini yakni perlunya mengembangkan keamanan dan privasi data pada pengguna yang memanfaatkan IoTseperti autentikasi, enkripsi data dan semacamnya.

Daftar Rujukan

[1]. Nahdi F., Dhika H., 2021, Analisis Dampak Internet of Things (IoT) Pada Perkembangan Teknologi di Masa Yang Akan Datang, Vol 6, No 1, Mei 2021: 33-42.1, Universitas Indraprasta PGRI INTEGER: Journal of Information Technology, Teknik informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Indraprasta PGRI 2.Teknik informatika, Fakultas Teknik dan Ilmu Komputer.
[2]. Amiruddin A., Rohmani F.M., 2019, Perancangan Spesifikasi Keamanan Untuk Pengembangan Aplikasi secure Chat Berdasarkan Common Criteria for It Scurity Evalution, Vol. 8, No. 6, Desember 2021, hlm. 1215-1226, Politeknik Siber dan Sandi Negara, Bogor 2Badan Siber dan Sandi Negara, Jakarta Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), hlm. 1215-1226.
[3]. Zubaidi A., Sardi I.R., Jatmika h.a., 2021, Pengamanan Internet of Things Berbasis NodeMCU Menggunakan Algoritma AES pada Arsitektur Web Service REST, Universitas Mataram e-ISSN 2549-7472 Edumatic: Jurnal Pendidikan Informatika Vol. 5 No. 2 Desember 2021, Program Studi Teknik Informatika, Hal. 252-260.
[4]. Zein A., Eriana S. E., 2021, Perancang Internet Of Things (IOT) Smart Home, Vol.31, No.2 (2021): 48-53.
[5]. Indrawan J. A., 2023, IoT dan Blockchain: Tinjauan Tantangan Solusi Keamanan dan Privasi, Universitas Komputer Indonesia, Bandung, Indonesia IoT dan Blockchain: Tinjauan Tantangan Solusi Keamanan dan Privasi hlm 1-12, diakses pada 15 juni 2023,

https://www.researchgate.net/publication/370074287
[6]. Ayu G.M, 2020, Perkembangan dan Penggunaan IoT di Indonesia Tahun 2021 Diprediksi Meningkat, Diakses pada 15 juni 2023, https://www.cloudcomputing.id/berita/perkembangan-dan-penggunaan-iot-di-indonesiav
[7]. Vailshery Lionel Sujay, 2022, Number of Internet of Things (IoT) connected devices world wide from 2019 to 2021, with forecasts from 2022 to 2030, diakses pada 15 juni 2023, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/#statisticContainerv