Jurnal Sistem Dan Teknologi Informasi (JSTI)

https://journalversa.com/s/index.php/jsti Vol. 07, No. 1 Februari 2025

KEAMANAN DAN KESELAMATAN IMPLEMENTANSI *INTERNET OF THINGS* (IOT): TANTANGAN PADA SEKTOR INDUSTRI DAN RUMAH TANGGA

Muhammad Tengku Sadewa[1]
Email: mtengkusadewa15@gmail.com

Dedek Kurniadi[2]
Email**:** dedekk789@gmail.com

Tata Sutabri[3]
Email**:** tata.sutabri@gmail.com

[1,2,3]Universitas Bina Darma

ABSTRAK

Perkembangan Internet of Things (IoT) membawa perubahan signifikan salam berbagai sektor kehidupan baik di industri maupun rumah tangga. IoT merujuk pada jaringan perangkat yang saling terhubung dan dapat saling bertukar data melalui internet, yang memungkinkan kontrol dan pemantauan secara otomatis. Teknologi ini menawarkan banyak potensi dalam meningkatkan efisiensi, kenyamanan, serta keamanan dan keselamatan. Namun, masih ada berbagai tantangan yang perlu diatasi, baik dari segi teknologi maupun sosial, sebelum visi IoT dapat terwujud sepenuhnya. Implementasi IoT di sektor industri dan rumah tangga menawarkan potensi besar untuk meningkatkan efisiensi dan kenyamanan. Penelitian ini merupakan penelitian fenomenologi yang bertujuan untuk memahami implementasi dan tantangan terkait teknologi informasi dan komunikasi Internet of Things (IoT) di seiring berkembangnya teknologi di dunia.

Kata Kunci: Keamanan, IoT, Tantangan, Rumah tangga, Industri.

ABSTRACT

The development of the Internet of Things (IoT) has brought significant changes in various sectors of life both in industry and household. IoT refers to a network of devices that are interconnected and can exchange data with each other over the internet, which allows for automated control and monitoring. This technology offers a lot of potential in improving efficiency, convenience, as well as security and safety. However, there are still various challenges that need to be overcome, both in terms of technology and society, before the IoT vision can be fully realized. The implementation of IoT in the industrial and household sectors offers great potential to improve efficiency and convenience. This research is a phenomenological research that aims to understand the implementation and challenges related to information and communication technology of the Internet of Things (IoT) in line with the development of technology in the world.

Keywords: *Security, IoT, Challenges, Household, Industrial.*

1. PENDAHULUAN

Beberapa tahun terakhir ini teknologi informasi dan komunikasi Internet of Things (IoT) yang dikenalkan oleh kevin ashton tahun 1998 mendapat perhatian yang semakin besar (Santucci, 2009). Perkembangan Internet of Things (IoT) membawa perubahan signifikan salam berbagai sektor kehidupan baik di industri maupun rumah tangga. IoT merujuk pada jaringan perangkat yang saling terhubung dan dapat saling bertukar data melalui internet, yang memungkinkan kontrol dan pemantauan secara otomatis. Teknologi ini menawarkan banyak potensi dalam meningkatkan efisiensi, kenyamanan, serta keamanan dan keselamatan.

Di sektor industri, IoT telah diadopsi untuk berbagai tujuan, mulai dari pemantauan mesin dan peralatan, pengelolaan rantai pasokan, hingga pengawasan keselamatan pekerja. Dengan adanya sensor dan perangkat IoT, proses pengawasan menjadi lebih akurat dan real-time, memungkinkan pengambilan keputusan yang lebih cepat dan tepat dalam mencegah kecelakaan atau kerusakan yang dapat merugikan. Di sisi lain, sektor rumah tangga juga mulai mengintegrasikan IoT dalam kehidupan sehari-hari, misalnya dengan perangkat rumah pintar yang dapat mengontrol pencahayaan, suhu, atau sistem keamanan rumah. Hal ini tidak hanya meningkatkan kenyamanan, tetapi juga memberikan tingkat perlindungan dan pengawasan yang lebih baik bagi penghuni rumah.

Meskipun demikian, implementasi IoT di kedua sektor ini tidak tanpa tantangan. Di sektor industri, tantangan terbesar adalah masalah integrasi teknologi dengan sistem yang sudah ada, serta kebutuhan akan infrastruktur yang kuat dan aman untuk mendukung komunikasi data yang terus-menerus. Selain itu, tantangan dalam pengelolaan data yang dihasilkan oleh perangkat IoT juga menjadi isu penting, karena volume data yang sangat besar memerlukan kapasitas penyimpanan dan pengolahan yang memadai. Di sektor rumah tangga, dalam Peningkatan Keamanan dan Keselamatan: Tantangan Implementasi pada Sektor Industri dan Rumah Tangga.

Kekuatan utama dari visi IoT terletak pada dampaknya yang signifikan terhadap berbagai aspek kehidupan sehari-hari dan perilaku pengguna potensial. Dari perspektif pengguna individu, pengaruh IoT yang paling jelas akan terlihat dalam bidang pekerjaan dan rumah tangga. Dalam konteks ini, beberapa contoh aplikasi yang mungkin muncul

termasuk kehidupan asistif, rumah dan kantor pintar, e-health, serta pembelajaran yang ditingkatkan, di mana paradigma baru ini akan memainkan peran penting dalam waktu dekat(Atzori, Iera and Morabito, 2010). Demikian pula, dari perspektif pengguna bisnis, konsekuensi yang paling nyata akan sama-sama terlihat di bidang-bidang seperti otomasi dan manufaktur industri, logistik, manajemen proses bisnis, transportasi orang dan barang yang cerdas.

Namun, masih ada berbagai tantangan yang perlu diatasi, baik dari segi teknologi maupun sosial, sebelum visi IoT dapat terwujud sepenuhnya. Salah satu masalah utama adalah bagaimana memastikan interoperabilitas yang lengkap antara perangkat yang terhubung, serta bagaimana memberikan kecerdasan yang tinggi dengan memungkinkan perangkat beradaptasi dan berperilaku secara otonom, sambil tetap menjamin kepercayaan, keamanan, dan privasi pengguna serta data mereka (Heuser and Woods, 2010). Selain itu, loT akan menimbulkan beberapa masalah baru mengenai isu-isu yang berkaitan dengan pemanfaatan sumber daya yang efisien objek yang memiliki keterbatasan sumber daya.

Pengertian Internet of Things (IoT)

Internet of Things (IoT) adalah sebuah jaringan perangkat yang saling terhubung dan dapat bertukar data secara otomatis dari satu perangkat ke perangkat lainnya(Prasetya, I., 2024).

Menurut Porter (1985), seorang pakar manajemen dari Harvard Business School, IoT dapat diartikan sebagai jaringan perangkat fisik yang terhubung melalui internet, yang memungkinkan pengumpulan data dan analisis untuk mengoptimalkan proses. Sementara itu, Vint Cerf, salah satu “bapak” dari internet modern, memberikan definisi yang lebih sederhana. Menurutnya, IoT adalah kemampuan perangkat dalam mengumpulkan data, mengirimkan data, dan menerima instruksi melalui internet.

Dari beberapa definisi di atas, dapat disimpulkan bahwa IoT merupakan konsep di mana segala sesuatu bisa terhubung dan saling berkomunikasi melalui internet. Mulai dari perangkat elektronik, kendaraan, peralatan rumah tangga, hingga sistem manufaktur dapat terhubung dalam satu jaringan yang sama.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian fenomenologi yang bertujuan untuk

memahami implementasi dan tantangan terkait teknologi informasi dan komunikasi Internet of Things (IoT) di seiring berkembangnya teknologi di dunia. Data yang diolah pada penelitian ini adalah data literatur dan sinkronisasi studi kasus teknologi informasi dan komunikasi Internet of Things (IoT). Secara garis besar, data yang digunakan adalah teori yang menyangkut teknologi informasi dan komunikasi Internet of Things (IoT) yang diperoleh dari berbagai sumber data seperti jurnal, artikel internet, dan sumber lainnya yang relevan dengan teori yang digunakan. Data-data tersebut kemudian dianalisis secara deskriptif guna menghasilkan gambaran implementasi dan tantangan dalam pemanfaatan teknologi informasi dan komunikasi Internet of Things (IoT) dalam sektor industri dan rumah tangga.

3. HASIL DAN PEMBAHASAN

Perkembangan IoT dalam Sistem Keamanan dan Keselamatan

Perkembangan signifikan yang terjadi dalam upaya melindungi perangkat, data, dan jaringan pada *Internet of Things* (IoT) terlihat pada kemajuan keamanan sistem dan keselamatan. Mengimplementasikan teknologi keamanan dan keselamatan yang lebih canggih, memperkuat autentikasi, meningkatkan enkripsi yang digunakan, secara real time memantau keamanan dan keselamatan sistem, dan melakukan peningkatan kesadaran terhadap risiko keamanan dan keselamatan merupakan contoh dari perkembangan IoT dalam sistem keamanan dan keselamatan(Muhana, M.F. and Fuads, E., 2024)

Keamanan perangkat IoT semakin menjadi perhatian utama bagi kalangan pengguna maupun produsen, mengingat semakin berkembangnya ekosistem perangkat yang terhubung ini. Isu-isu terkait kerentanannya terhadap serangan siber, seperti peretasan, pencurian data, atau bahkan pemanfaatan perangkat sebagai bagian dari serangan botnet, mendorong produsen untuk merancang perangkat yang lebih aman secara default. Dalam proses desain, produsen kini lebih fokus pada integrasi fitur keamanan sejak tahap awal produksi, seperti penguatan otentikasi, pembaruan perangkat lunak otomatis, serta pengenalan sistem proteksi yang lebih canggih. Hal ini bertujuan untuk meminimalkan potensi eksploitasi celah-celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Sementara itu, pengguna juga semakin disadarkan untuk lebih berhati-hati dalam mengamankan perangkat mereka. Banyak perangkat IoT yang mengumpulkan data pribadi, seperti informasi kesehatan, kebiasaan

konsumsi, hingga lokasi pengguna, yang dapat dengan mudah diekspos jika tidak dilindungi dengan baik. Untuk itu, penting bagi pengguna untuk memahami cara melindungi perangkat mereka dengan langkah-langkah seperti penggunaan kata sandi yang kuat, pengaturan jaringan yang aman, dan pembaruan perangkat lunak yang rutin (Sari, 2024).

Seiring dengan meningkatnya ancaman, banyak negara mulai mengimplementasikan regulasi yang mewajibkan perangkat IoT memenuhi standar keamanan tertentu, guna melindungi pengguna dari potensi risiko. Sebagai contoh, inisiatif seperti Cybersecurity Improvement Act di Amerika Serikat menekankan pentingnya penerapan kebijakan keamanan yang lebih ketat, termasuk pembuatan standar keamanan wajib bagi produsen perangkat IoT. Regulasi seperti ini mendorong produsen untuk mengadopsi protokol keamanan yang lebih rigor, serta mengutamakan privasi pengguna dalam desain produk mereka. Selain itu, teknologi kecerdasan buatan (AI) dan machine learning semakin banyak diterapkan untuk mendeteksi ancaman dan serangan siber pada perangkat IoT dengan lebih cepat dan akurat. AI dapat mengidentifikasi pola-pola yang mencurigakan atau perilaku anomali pada jaringan IoT dan memberikan respons otomatis atau peringatan dini, memungkinkan mitigasi ancaman sebelum menyebabkan kerusakan lebih lanjut.

Di sisi lain, enkripsi data end-to-end kini menjadi praktik umum untuk melindungi informasi yang ditransmisikan antara perangkat IoT dan server. Enkripsi memastikan bahwa data yang sensitif, seperti riwayat kesehatan atau informasi transaksi, tetap aman meskipun berada dalam perjalanan atau tersimpan di server cloud. Ini secara signifikan mengurangi risiko data disadap oleh pihak yang tidak berwenang, yang dapat menyebabkan pelanggaran privasi atau kerugian finansial. Tak kalah penting, teknologi blockchain mulai diterapkan dalam konteks keamanan IoT untuk memberikan lapisan tambahan perlindungan terhadap transaksi data antar perangkat. Dengan menggunakan buku besar terdesentralisasi dan transparan, blockchain memungkinkan verifikasi yang lebih aman dan tahan terhadap manipulasi data atau serangan siber. Selain itu, dengan sifatnya yang terdistribusi, blockchain juga dapat meningkatkan ketahanan perangkat IoT terhadap serangan terkoordinasi atau peretasan dari satu titik kelemahan.

Dengan perkembangan teknologi yang terus maju, integrasi berbagai inovasi ini diharapkan dapat memberikan solusi yang lebih komprehensif dalam menjaga keamanan

dan privasi dalam ekosistem IoT. Di masa depan, diharapkan perangkat IoT tidak hanya lebih aman, tetapi juga lebih andal dan dipercaya oleh pengguna, baik di tingkat individu maupun sektor industri. Penerapan standar keamanan yang lebih ketat, inovasi teknologi yang lebih canggih, serta kesadaran yang lebih tinggi di kalangan pengguna dan produsen akan membuka jalan bagi penerapan IoT yang lebih luas dan lebih aman, sehingga teknologi ini dapat memberikan manfaat maksimal tanpa menimbulkan risiko yang merugikan.

Penerapan IOT pada sektor industri

Pemantauan dan Pemeliharaan Mesin:

Pemantauan mesin menggunakan IoT memungkinkan pemantauan kondisi mesin secara real-time melalui sensor, seperti suhu, tekanan, getaran, dan arus listrik. Sensor ini membantu mendeteksi kerusakan potensial sebelum menjadi masalah besar, memungkinkan pemeliharaan preventif yang lebih efisien. Dengan pemeliharaan berbasis kondisi, perusahaan dapat mengurangi downtime dan biaya perawatan, serta meningkatkan produktivitas. Integrasi kecerdasan buatan (AI) memungkinkan prediksi kegagalan mesin lebih akurat, mengoptimalkan perencanaan pemeliharaan dan mengurangi gangguan produksi.

Manajemen Rantai Pasok:

IoT dan RFID memungkinkan pelacakan barang secara real-time di seluruh rantai pasok. Data yang dikumpulkan dari sensor dan label RFID meningkatkan visibilitas, memudahkan pemantauan stok, dan mendeteksi masalah seperti keterlambatan pengiriman atau kekurangan pasokan. Dengan visibilitas yang lebih tinggi, perusahaan dapat merespons lebih cepat, mengoptimalkan manajemen inventaris, dan meningkatkan efisiensi operasional, yang pada gilirannya memperkuat daya saing perusahaan.

Otomatisasi Proses Produksi:

IoT mengintegrasikan mesin dalam proses produksi, memungkinkan koordinasi otomatis antara mesin dan sistem. Data real-time mengenai kecepatan, suhu, dan tekanan membantu mengoptimalkan aliran produksi, mengurangi waktu siklus, dan mengidentifikasi bottleneck. Sistem otomatis ini juga mendukung pemeliharaan prediktif, mengurangi downtime dan memastikan produksi tetap lancar. Dengan pengelolaan produksi yang lebih efisien, perusahaan dapat meningkatkan produktivitas, mengurangi

pemborosan, dan menjaga kualitas produk.

Keselamatan Kerja:

IoT membantu memantau lingkungan kerja untuk memastikan keselamatan karyawan. Sensor gas, suhu, dan kelembaban dapat mendeteksi kondisi berbahaya seperti gas beracun atau suhu ekstrem, memberikan peringatan dini untuk menghindari risiko kecelakaan. Sensor juga dapat mendeteksi getaran atau kebisingan yang abnormal, menghindari kerusakan peralatan dan cedera fisik. Sistem ini meningkatkan keselamatan, meminimalkan kecelakaan, dan mendukung kepatuhan terhadap standar keselamatan kerja.

Analisis Data untuk Peningkatan Kualitas:

Data dari sensor IoT memungkinkan analisis kondisi operasional dan kualitas produk secara real-time. Dengan memantau variabel seperti suhu dan tekanan, perusahaan dapat mendeteksi masalah kualitas dan efisiensi lebih cepat. Analisis ini membantu memperbaiki proses produksi dan meminimalkan variabilitas produk, serta mengidentifikasi bottleneck dalam proses produksi. Dengan demikian, perusahaan dapat mengurangi biaya, mengoptimalkan sumber daya, dan meningkatkan konsistensi produk.

Penerapan IoT di Sektor Rumah Tangga

Smart Home:IoT telah merevolusi sektor rumah tangga dengan menciptakan rumah pintar yang mengintegrasikan berbagai perangkat untuk kenyamanan, efisiensi, dan keamanan. Perangkat seperti lampu otomatis, termostat pintar, dan sistem keamanan terhubung memungkinkan pengguna mengontrol dan memantau kondisi rumah secara real-time, bahkan dari jarak jauh. Lampu otomatis menghemat energi dengan menyesuaikan pencahayaan sesuai kebutuhan, sementara termostat pintar mengatur suhu secara efisien, baik secara otomatis atau melalui aplikasi. Sistem keamanan dengan kamera pengawas, sensor gerak, dan deteksi pintu atau jendela memberikan perlindungan lebih, memberi peringatan langsung dan akses video secara real-time untuk kontrol penuh.(Muallif, 2024)

Pengelolaan Energi:Perangkat IoT memungkinkan pemantauan konsumsi energi secara real-time, memberikan wawasan mendalam tentang penggunaan energi di rumah. Sensor pada perangkat seperti pemanas, pendingin udara, dan peralatan elektronik membantu melacak konsumsi energi dan mengidentifikasi pola penggunaan. Misalnya,

termostat pintar menghindari pemborosan energi dengan menyesuaikan suhu saat rumah kosong. Pengguna dapat mengatur jadwal penggunaan perangkat untuk mengoptimalkan efisiensi dan mengurangi biaya listrik. Dengan demikian, IoT membantu rumah menjadi lebih efisien dan ramah lingkungan.

Keamanan Rumah:Sistem keamanan cerdas dengan kamera pengawas, sensor gerak, dan teknologi analitik memungkinkan pemantauan rumah secara real-time dan respons otomatis terhadap ancaman. Kamera dan sensor mendeteksi gerakan mencurigakan, mengirimkan peringatan dan rekaman video langsung ke perangkat pengguna. Beberapa sistem dapat menghubungi layanan darurat secara otomatis jika terdeteksi ancaman serius, seperti perampokan atau kebakaran, meningkatkan respons cepat tanpa keterlambatan. Teknologi IoT ini memberikan kontrol penuh atas keamanan rumah dan ketenangan pikiran bagi penghuninya.

Kenyamanan dan Automasi:Perangkat IoT memungkinkan otomatisasi tugas sehari-hari, meningkatkan kenyamanan dan efisiensi energi. Lampu otomatis dan termostat pintar dapat disesuaikan berdasarkan preferensi pengguna, seperti menyesuaikan suhu saat pulang kerja atau menyalakan lampu pada waktu tertentu. Pengguna juga dapat mengatur rutinitas seperti menutup tirai atau mengaktifkan sistem penyiraman otomatis di kebun. Dengan penghematan energi yang lebih besar, rumah menjadi lebih adaptif terhadap kebutuhan penghuni, meningkatkan kenyamanan dan efisiensi tanpa interaksi manual.

Tantangan Implementasi Internet of Things (IoT) di Sektor Industri dan Rumah Tangga

Internet of Things (IoT) telah menjadi bagian integral dari transformasi digital di berbagai sektor, termasuk industri dan rumah tangga. Meskipun menawarkan banyak manfaat, implementasi IoT juga menghadapi sejumlah tantangan yang signifikan. Pada penerapan IoT di sektor industri yang membuat sistem operasional berjalan dengan lebih efisien, tantangan yang harus di hadapi seperti biaya pembelian perangkat, instalasi, pelatihan karyawan untuk menggunakan IoT cukup mahal. Regulasi terkait keamanan data, privasi, penggunaan IoT yang sering kali belum matang, dan bagi industri yang berada di Lokasi terpencil sering menghadapi keterbatasan akses jaringan internet berkualitas tinggi.

Tantangan di Sektor Industri

a. Keamanan Data dan Privasi :semakin banyaknya perangkat yang terhubung ke internet, risiko kebocoran data dan serangan siber menjadi semakin besar. Setiap interaksi digital, baik itu transaksi finansial, pertukaran informasi pribadi, maupun komunikasi bisnis, dapat menjadi sasaran potensi ancaman yang berbahaya. Oleh karena itu, penerapan protokol keamanan yang kuat, seperti enkripsi data end-to-end, otentikasi dua faktor, dan perlindungan terhadap sistem jaringan sangat penting untuk menjaga kerahasiaan dan integritas data (Hapsah and Nasution, 2024). Tanpa perlindungan yang memadai, informasi sensitif dapat dengan mudah dicuri atau disalahgunakan, yang dapat merugikan individu maupun organisasi secara finansial maupun reputasional. Keamanan data dan privasi harus menjadi prioritas utama dalam setiap inovasi teknologi untuk memastikan bahwa perkembangan ini tidak menimbulkan kerugian yang lebih besar di masa depan.
b. Skalabilitas dan Manajemen Perangkat: Pertumbuhan eksponensial dalam jumlah perangkat Internet of Things (IoT) telah menciptakan tantangan besar dalam hal pengelolaan, karena semakin banyak perangkat yang terhubung dan berfungsi secara simultan. Setiap perangkat, yang sering kali datang dari produsen yang berbeda dengan berbagai protokol dan standar teknis, memerlukan perhatian khusus dalam proses pemasangan, konfigurasi, dan pemeliharaannya. Tanpa sistem yang terintegrasi dan efisien, pengelolaan perangkat IoT dapat menjadi sangat rumit dan rawan kesalahan, yang pada gilirannya dapat menurunkan kinerja sistem secara keseluruhan. Untuk itu, diperlukan sistem manajemen IoT yang canggih dan otomatisasi yang dapat menangani berbagai aspek operasional, mulai dari penyusunan inventaris perangkat, pemantauan kondisi perangkat secara real-time, hingga pembaruan perangkat lunak dan pemecahan masalah. Dengan adanya solusi manajemen yang efisien, organisasi dapat mengoptimalkan penggunaan perangkat IoT, meminimalkan downtime, dan mengurangi biaya operasional, sekaligus memastikan perangkat tetap aman dan berfungsi dengan baik sepanjang siklus hidupnya.
c. Integrasi Sistem: Berbagai perangkat yang diproduksi oleh produsen yang berbeda sering kali tidak kompatibel satu sama lain, yang dapat menimbulkan kesulitan dalam penggunaannya, terutama dalam ekosistem yang saling terhubung. Masalah

kompatibilitas ini dapat menghambat efisiensi, meningkatkan biaya, dan membatasi fleksibilitas pengguna dalam memilih perangkat atau solusi teknologi yang sesuai dengan kebutuhan mereka. Oleh karena itu, sangat penting untuk mengembangkan dan menerapkan standar universal yang dapat memastikan interoperabilitas antar perangkat dari berbagai merek dan produsen. Dengan adanya standar tersebut, perangkat dapat saling berkomunikasi dan berfungsi secara harmonis, memungkinkan pengalaman pengguna yang lebih mulus dan mengurangi kompleksitas dalam pengelolaan sistem teknologi yang terintegrasi. Hal ini juga dapat mendorong inovasi, mempercepat adopsi teknologi baru, dan menciptakan pasar yang lebih terbuka dan inklusif.

d. Konektivitas Jaringan: Keberhasilan implementasi Internet of Things (IoT) sangat bergantung pada konektivitas yang stabil dan andal. IoT berfungsi dengan menghubungkan berbagai perangkat yang saling berkomunikasi untuk mengumpulkan dan mentransfer data secara real-time. Jika koneksi jaringan tidak konsisten atau terputus-putus, hal ini dapat menyebabkan gangguan serius dalam pengumpulan dan pertukaran data, yang pada gilirannya dapat memengaruhi akurasi dan keandalan sistem secara keseluruhan. Ketidakstabilan jaringan dapat menyebabkan kehilangan data, keterlambatan informasi, atau bahkan kegagalan sistem, yang sangat berbahaya dalam konteks aplikasi IoT yang memerlukan respons cepat dan presisi tinggi, seperti dalam sektor kesehatan, transportasi, atau industri manufaktur. Oleh karena itu, memastikan konektivitas yang kuat dan stabil adalah salah satu elemen kunci dalam keberhasilan implementasi IoT, dengan memperhatikan kualitas jaringan, pemilihan teknologi yang tepat, dan perencanaan infrastruktur yang memadai. Tanpa koneksi yang handal, manfaat potensial dari IoT tidak akan tercapai secara optimal, dan dapat menurunkan efisiensi serta merugikan berbagai pihak yang mengandalkan sistem tersebut.

e. Biaya Implementasi: Investasi awal untuk perangkat keras dan perangkat lunak IoT masih tergolong cukup tinggi, yang menjadi tantangan besar, terutama bagi usaha kecil dan menengah (UKM). Biaya untuk mengadopsi teknologi IoT mencakup pengadaan perangkat fisik, seperti sensor, aktuator, dan perangkat penghubung lainnya, serta pengembangan dan penerapan perangkat lunak yang diperlukan untuk manajemen dan analisis data. Bagi banyak UKM, biaya ini bisa menjadi beban

finansial yang signifikan, terutama jika dibandingkan dengan anggaran terbatas mereka. Selain itu, biaya tambahan seperti pelatihan staf, pemeliharaan perangkat, serta pembaruan sistem yang rutin juga turut menambah beban(Bandyopadhyay and Sen, 2011). Meskipun IoT memiliki potensi untuk meningkatkan efisiensi dan produktivitas, banyak UKM yang merasa kesulitan untuk mengakses teknologi ini tanpa dukungan finansial atau insentif yang memadai. Oleh karena itu, penting bagi penyedia solusi IoT dan pemerintah untuk mencari cara untuk menurunkan hambatan biaya, misalnya melalui model langganan atau skema pembiayaan yang lebih fleksibel, agar UKM dapat memanfaatkan potensi IoT tanpa harus menghadapi kesulitan finansial yang besar. Dengan cara ini, teknologi IoT dapat diakses oleh lebih banyak pelaku usaha kecil dan menengah, yang pada gilirannya dapat mendorong inovasi dan pertumbuhan ekonomi yang lebih merata.

f. Regulasi dan Kepatuhan: Mematuhi regulasi yang berkaitan dengan privasi data dan keamanan informasi merupakan tantangan penting dalam penerapan Internet of Things (IoT), karena perangkat yang terhubung sering kali mengumpulkan, menyimpan, dan mentransmisikan data sensitif yang melibatkan individu maupun organisasi. Setiap perangkat IoT, dari rumah pintar hingga sistem industri, dapat menjadi titik rawan yang mengancam keamanan data pribadi dan bisnis jika tidak dikelola dengan hati-hati sesuai dengan aturan yang berlaku. Banyak negara memiliki regulasi yang ketat mengenai perlindungan data pribadi, seperti GDPR di Eropa, yang mengharuskan perusahaan untuk memastikan data yang dikumpulkan dilindungi dengan langkah-langkah keamanan yang memadai dan bahwa pengguna diberi kontrol atas data mereka(Fadhlullah *et al.*, 2016). Namun, dalam praktiknya, banyak pengembang dan penyedia layanan IoT yang menghadapi kesulitan dalam memenuhi persyaratan ini karena kompleksitas teknologi yang terlibat, perbedaan kebijakan di berbagai wilayah, serta tantangan dalam mengimplementasikan protokol keamanan yang memadai di seluruh ekosistem perangkat yang saling terhubung. Selain itu, kekurangan sumber daya atau pemahaman tentang regulasi ini sering kali membuat perusahaan, terutama yang berukuran kecil, kesulitan dalam memenuhi standar yang ditetapkan. Oleh karena itu, penting untuk menciptakan solusi yang tidak hanya mendukung kepatuhan terhadap regulasi yang ada, tetapi juga memfasilitasi pengelolaan keamanan dan privasi secara lebih

efisien dan terintegrasi dalam sistem IoT, untuk melindungi data dan membangun kepercayaan pengguna.

Tantangan dalam Implementasi IoT pada Rumah Tangga

Dalam implementansi IoT di rumah tangga memang memiliki manfaat yang sangat berguna serta menciptakan rumah pintar yang lebih efisien dan sesuai dengan kebutuhan penghuninya, mengingat pada sekarang yang perkembangan teknologinya sangat berkembang pesat. Ternyata dibalik banyaknya manfaat yang diterima, masih ada tantangan yang harus dihadapi seperti kekhawatiran tentang keamanan data yang mudah untuk diretas, biaya awal yang tinggi, dan terhambatnya kinerja IoT yang disebabkan oleh konektivitas jaringan internet yang buruk, terlebih jika di daerah terpencil(Hildayanti and Sya'rani Machrizzandi, 2020).

a. Adopsi Pengguna: Banyak pengguna, baik individu maupun organisasi, yang masih belum sepenuhnya memahami manfaat dan cara kerja teknologi Internet of Things (IoT), yang menghambat adopsi dan penerimaan teknologi ini secara luas. Meskipun IoT menawarkan potensi besar untuk meningkatkan efisiensi, kenyamanan, dan produktivitas, banyak orang merasa ragu atau bingung mengenai bagaimana teknologi ini berfungsi dan apa manfaat langsung yang dapat mereka peroleh darinya. Ketidaktahuan ini sering kali muncul karena kurangnya pemahaman tentang cara perangkat IoT saling terhubung, bagaimana data dikumpulkan dan digunakan, serta bagaimana perangkat tersebut dapat memberikan nilai tambah dalam kehidupan sehari-hari atau operasional bisnis. Oleh karena itu, dibutuhkan upaya edukasi yang lebih intensif melalui berbagai saluran, seperti pelatihan, seminar, webinar, dan materi edukasi berbasis media sosial, untuk memberikan pengetahuan yang jelas dan mudah dipahami tentang IoT. Edukasi ini tidak hanya mencakup aspek teknis, tetapi juga harus menjelaskan bagaimana IoT dapat meningkatkan keamanan, efisiensi, dan kenyamanan, serta cara mengelola dan melindungi data yang dihasilkan oleh perangkat tersebut. Dengan meningkatkan pemahaman tentang manfaat dan potensi IoT, pengguna akan lebih cenderung untuk menerima dan mengimplementasikan teknologi ini dalam kehidupan mereka, yang pada akhirnya akan mempercepat transformasi digital dan membawa dampak positif dalam berbagai sektor.
b. Keamanan Perangkat: Perangkat rumah pintar, meskipun menawarkan

kenyamanan dan efisiensi, sering kali rentan terhadap serangan siber jika tidak dilindungi dengan langkah-langkah keamanan yang memadai. Karena perangkat-perangkat ini terhubung ke internet dan saling berkomunikasi, mereka dapat menjadi celah yang dimanfaatkan oleh peretas untuk mengakses jaringan rumah, mencuri data pribadi, atau bahkan mengendalikan perangkat tanpa izin. Misalnya, kamera pengawas, termostat pintar, atau asisten virtual bisa saja dieksploitasi jika tidak dilengkapi dengan protokol keamanan yang kuat, seperti enkripsi data dan kata sandi yang kompleks. Oleh karena itu, penting untuk memberikan pemahaman kepada pengguna mengenai risiko yang terkait dengan perangkat rumah pintar dan betapa krusialnya perlindungan yang tepat. Edukasi tentang pentingnya pengaturan kata sandi yang kuat, pembaruan perangkat lunak secara berkala, dan penggunaan jaringan Wi-Fi yang aman sangat diperlukan agar pengguna dapat mengoptimalkan keamanan perangkat mereka. Selain itu, pengenalan terhadap fitur keamanan tambahan, seperti autentikasi dua faktor (2FA), dan pemahaman mengenai cara mengelola dan membatasi akses aplikasi juga menjadi bagian penting dalam mencegah potensi serangan. Dengan memberikan wawasan yang cukup, pengguna tidak hanya dapat menikmati kenyamanan teknologi rumah pintar, tetapi juga dapat menjaga privasi dan data mereka agar tetap aman dari ancaman siber.

c. Keterbatasan Infrastruktur: Di beberapa daerah, terutama di luar kota besar, akses internet yang cepat dan andal masih menjadi masalah utama yang menghambat penerapan Internet of Things (IoT) secara luas. IoT memerlukan konektivitas jaringan yang stabil dan berkecepatan tinggi untuk dapat berfungsi secara optimal, terutama ketika perangkat-perangkat yang terhubung harus mentransfer data dalam jumlah besar secara real-time. Di daerah-daerah dengan infrastruktur internet yang terbatas atau tidak memadai, seperti di pedesaan atau daerah terpencil, kualitas jaringan sering kali tidak cukup untuk mendukung kebutuhan IoT, yang dapat menyebabkan keterlambatan dalam pengiriman data, kehilangan informasi, atau bahkan kegagalan sistem secara keseluruhan. Selain itu, tingginya biaya untuk membangun infrastruktur jaringan yang lebih canggih, seperti 4G atau 5G, sering kali menjadi hambatan bagi penyedia layanan di daerah-daerah dengan kepadatan penduduk rendah. Masalah ini tidak hanya menghambat pengadopsian IoT di sektor industri atau komersial, tetapi juga dapat menghalangi pemanfaatan teknologi IoT

dalam sektor-sektor penting lainnya, seperti pertanian, kesehatan, dan pendidikan. Oleh karena itu, untuk memperluas penerapan IoT, diperlukan upaya lebih dalam meningkatkan aksesibilitas dan kecepatan internet di daerah-daerah tersebut, baik melalui peningkatan infrastruktur lokal, kolaborasi antara pemerintah dan penyedia layanan telekomunikasi, maupun melalui teknologi alternatif seperti jaringan satelit atau koneksi berbasis radio. Dengan perbaikan dalam konektivitas internet, potensi IoT dapat dioptimalkan untuk meningkatkan kualitas hidup dan perekonomian di seluruh wilayah, baik di kota besar maupun di daerah terpencil.

d. Konsumsi Energi: Banyak perangkat Internet of Things (IoT) beroperasi dalam jangka waktu yang lama tanpa perlu pengisian daya yang sering, terutama perangkat yang ditempatkan di lokasi yang sulit dijangkau atau tersebar di area yang luas, seperti sensor di pertanian, alat pemantauan lingkungan, atau perangkat kesehatan yang dipakai tubuh. Untuk itu, efisiensi penggunaan energi menjadi salah satu perhatian utama, mengingat sebagian besar perangkat IoT mengandalkan baterai sebagai sumber daya utama mereka. Jika perangkat ini mengonsumsi energi secara berlebihan, maka masa pakai baterai akan berkurang drastis, yang pada gilirannya meningkatkan biaya pemeliharaan dan mengurangi efektivitas operasionalnya. Oleh karena itu, pengembangan teknologi yang dapat mengoptimalkan efisiensi baterai, seperti penggunaan chip low-power, manajemen daya yang pintar, serta algoritma yang mengatur kapan perangkat harus aktif atau dalam mode hemat daya, sangat penting untuk memastikan perangkat IoT dapat berfungsi secara mandiri untuk jangka waktu yang lama. Selain itu, tren pengembangan energi alternatif, seperti pengisian daya melalui tenaga surya atau penggunaan teknologi pengisian nirkabel, juga semakin relevan untuk mendukung perangkat IoT agar tetap efisien dan berkelanjutan. Dengan mencapai efisiensi energi yang tinggi, perangkat IoT tidak hanya akan lebih hemat biaya dan ramah lingkungan, tetapi juga dapat memperluas penerapannya di berbagai sektor, meningkatkan kinerja dan keandalan sistem IoT secara keseluruhan

4. KESIMPULAN

Perkembangan signifikan dalam keamanan dan keselamatan pada perangkat IoT telah membawa kemajuan penting untuk melindungi perangkat, data, dan jaringan. Produsen kini lebih fokus pada integrasi fitur keamanan sejak tahap desain, seperti

penguatan autentikasi dan pembaruan perangkat lunak otomatis. Di sisi pengguna, kesadaran tentang pentingnya mengamankan perangkat semakin meningkat, dengan langkah-langkah perlindungan yang lebih baik, seperti penggunaan kata sandi yang kuat dan pengaturan jaringan yang aman.

Implementasi IoT di sektor industri dan rumah tangga menawarkan potensi besar untuk meningkatkan efisiensi dan kenyamanan. Namun, tantangan seperti keamanan data, manajemen perangkat, adopsi pengguna, dan keterbatasan infrastruktur harus diatasi agar teknologi ini dapat memberikan manfaat maksimal. Dengan kolaborasi antara pengembang teknologi, regulator, dan pengguna, solusi IoT dapat berkembang dengan aman dan efektif di masa depan.

Regulasi yang semakin ketat, seperti Cybersecurity Improvement Act di AS, serta penerapan teknologi canggih seperti kecerdasan buatan (AI), machine learning, dan blockchain, juga berperan penting dalam mengidentifikasi dan mencegah ancaman siber. Enkripsi data end-to-end menjadi praktik umum untuk melindungi data sensitif yang dikirim antar perangkat, sehingga mengurangi risiko kebocoran informasi.

Seiring berkembangnya teknologi, integrasi inovasi-inovasi ini diharapkan dapat meningkatkan keamanan dan privasi perangkat IoT, menjadikannya lebih andal dan terpercaya, baik di tingkat individu maupun industri. Penerapan standar keamanan yang lebih ketat dan kesadaran yang lebih tinggi akan membuka jalan bagi adopsi IoT yang lebih luas, memberikan manfaat yang maksimal tanpa menimbulkan risiko yang merugikan.

DAFTAR PUSTAKA

Atzori, L., Iera, A. and Morabito, G. (2010) ‘The Internet of Things: A survey’, *Computer Networks*, 54(15), pp. 2787–2805. Available at: https://doi.org/10.1016/j.comnet.2010.05.010.

Bandyopadhyay, D. and Sen, J. (2011) ‘Internet of things: Applications and challenges in technology and standardization’, *Wireless Personal Communications*, 58(1), pp. 49–69. Available at: https://doi.org/10.1007/s11277-011-0288-5.

Fadhlullah, H.S.F. *et al.* (2016) ‘PENGARUH INTERNET OF THINGS (IOT) DALAM INDUSTRI THE IMPACT INTERNET OF THINGS (IOT) IN INDUSTRY Haidar’, 2(5), pp. 1–23.

Febryan, H. dkk. (2024) ' Internet of Things (IoT) Dalam Rumah Tangga' Available at :

Internet of Things (IoT) dalam Rumah Tangga - Jurusan Informatika - Fakultas Teknologi Industri - Universitas Islam Indonesia

Hapsah, Z.F. and Nasution, M.I.P. (2024) 'PENGGUNAAN SISTEM DATABASE UNTUK APLIKASI INTERNET OF THINGS (IoT): TANTANGAN DAN PELUANG BAGI PERUSAHAAN', *Kohesi: Jurnal Sains dan Teknologi*, 3(10), pp. 71–80.

Heuser, L. and Woods, D. (2010) 'Is Europe leading the way to the future internet?', *IEEE Internet Computing* [Preprint]. Available at: https://doi.org/10.1109/MIC.2010.120.

Hildayanti, A. and Sya'rani Machrizzandi, M. (2020) 'Sistem Rekayasa Internet Pada Implementasi Rumah Pintar Berbasis IoT', *Jurnal Ilmiah Ilmu Komputer*, 6(1), pp. 45–51. Available at: https://doi.org/10.35329/jiik.v6i1.143.

Muallif. (2024) 'Mengenal Internet of Things (IoT) : Cara Kerja, Manfaat, dan Tantangannya di Berbagai Sektor' Available at Mengenal Internet of Things (IoT): Cara Kerja, Manfaat, dan Tantangannya di Berbagai Sektor – Universitas Islam An Nur Lampung

Muhana, M.F. and Fuads, E. (2024) 'Keamanan dan Implementasi IOT Dalam Lingkungan Industri' *Jurnal Mahasiswa Teknik Informatika*, 8(1).

Najib, W. dkk. (2020) 'Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things' *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, 9(4).

Porter, M.E. (1985) 'Technology and competitive advantage (chapter 5 in competitive advantage book)', *Journal of Business Strategy*, 5(3), pp. 60–78.

Prasetya, I. (2024) ' Apa Itu Internet of Things?' Available at : https://docif.telkomuniversity.ac.id/apa-itu-iot/

Salwa, N.D.K. (2024) 'Mengenal IoT' Available at : https://www.cloudcomputing.id/pengetahuan-dasar/mengenal-konektivitas-iot

Santucci, G. (2009) 'From internet of data to internet of things', *International Conference on Future Trends of the Internet*, (January), pp. 1–19. Available at: http://www.ipv6council.lu/AgendaLfICT.html.

Sari, D.R. (2024) 'Analisis Keamanan Sistem Informasi dalam Era Internet of Things (IoT)', *Technologia Journal*, 1(2), pp. 1–10.