KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Ekonomi Dan Manajemen
Vol.3, No.12 Desember 2025
e-ISSN: 3025-7859; p-ISSN: 3025-7972, Hal 332-341
DOI: https://doi.org/10.61722/jiem.v3i12.7507

INTERNET OF THINGS (IoT) SEBAGAI PILAR KEAMANAN DATA PADA SISTEM DISTRIBUSI DI INDONESIA

Mut'Mainna
Universitas Negeri Makassar
Andi Muhammad Rivai
Universitas Negeri Makassar
Andhi Febisatria
Universitas Negeri Makassar
Titi Sarnawiyah
Universitas Negeri Makassar
Muhammad Rafli Setiawan
Universitas Negeri Makassar
Alamat: Jalan A.P. Pettarani, Tidung, Kecamatan Rappocini, Kota Makassar, Sulawesi Selatan 90022
Korespondensi penulis: mutmainnam74@gmail.com[1], andi.rivai@unm.ac.id[2], andhi.febisatria@unm.ac.id[3], titisarnawia12@gmail.com[4], muhr55450@gmail.com[5]

Abstrak. *The Internet of Things (IoT) is an advanced technology that integrates physical objects with the internet through sensors, facilitating intellectual interaction between devices and providing increased efficiency and control in various dimensions of life and business activities. In Indonesia, the implementation of IoT has experienced significant expansion, particularly in the industrial distribution sector, although this poses substantial challenges related to data security. This study aims to explore the role of IoT as the foundation of data security in industrial distribution systems in Indonesia. The methodology applied involves a literature review of scientific journals, industry reports, and recent reliable articles. The findings indicate that IoT contributes to data security through encryption, authentication, intrusion detection, and anomaly detection systems that improve the accuracy of cyber threat identification. In addition, IoT can reduce human error, maintain product quality standards, and strengthen data integrity throughout the distribution chain. However, its effectiveness depends on technical, organizational, and regulatory factors that require further strengthening to ensure sustainable security.*
Keywords: *IoT security; data security; network security*

Abstrak. *Internet of Things (IoT) merupakan sebuah teknologi canggih yang mengintegrasikan objek fisik dengan jaringan internet melalui sensor, sehingga memfasilitasi interaksi intelektual antarperangkat serta memberikan peningkatan efisiensi dan pengendalian dalam berbagai dimensi kehidupan dan kegiatan bisnis. Di Indonesia, implementasi IoT telah mengalami ekspansi yang signifikan, khususnya dalam sektor distribusi industri, meskipun hal ini menimbulkan tantangan substansial terkait keamanan data. Penelitian ini bertujuan untuk mengeksplorasi peran IoT sebagai fondasi keamanan data dalam sistem distribusi industri di Indonesia. Metodologi yang diterapkan melibatkan tinjauan literatur terhadap jurnal ilmiah, laporan industri, serta artikel terpercaya terkini. Temuan kajian mengindikasikan bahwa IoT berkontribusi pada keamanan data melalui mekanisme enkripsi, otentikasi, deteksi intrusi, serta sistem deteksi anomali yang meningkatkan akurasi pengidentifikasian ancaman siber. Selain itu, IoT mampu mengurangi kesalahan manusiawi, menjaga standar kualitas produk, dan memperkuat integritas data sepanjang rantai distribusi. Namun demikian, efektivitasnya tergantung pada faktor-faktor teknis, organisasional, dan regulasi yang memerlukan penguatan lebih lanjut guna menjamin keamanan yang berkelanjutan.*
Kata Kunci: *Keamanan IoT; keamanan data; keamanan jaringan*

PENDAHULUAN

Menurut Kevin Ashton, *Internet of Things* (IoT) didefinisikan sebagai sistem objek fisik di dunia nyata yang terhubung ke internet melalui sensor. IoT mencakup mesin cerdas yang berinteraksi dengan mesin lainnya, objek, lingkungan, serta infrastruktur. Teknologi inovatif ini

Received Juli 30, 2023; Revised Agustus 2, 2023; September 01, 2024
* Rama Gusti Prakoso, ramagusti33@email.com

telah memberikan dampak signifikan terhadap kehidupan manusia, dengan memfasilitasi cara hidup dan bekerja yang lebih efisien serta memberikan kontrol menyeluruh atas aspek-aspek kehidupan. Di luar penyediaan perangkat cerdas untuk otomatisasi rumah tangga, IoT memiliki relevansi krusial bagi dunia bisnis. Teknologi ini menyediakan pandangan real-time mengenai operasi sistem mereka, serta menghasilkan wawasan mendalam terkait berbagai aspek, mulai dari performa mesin hingga operasi rantai pasokan dan logistik. Perangkat ini mencakup sistem rumah pintar seperti termostat dan pencahayaan, pelacak kebugaran wearable, sensor industri, kendaraan terhubung, serta monitor kesehatan. Implementasi IoT berkontribusi pada akselerasi kemajuan di berbagai sektor industri, termasuk transportasi, kesehatan, manufaktur, dan otomatisasi rumah pintar (Laghari, 2024), serta mendukung entitas bisnis dalam meningkatkan efisiensi operasional, pemantauan real-time, serta formulasi keputusan yang didasarkan pada data (Nag, 2024).

Teknologi ini telah muncul sebagai salah satu inovasi yang berkembang pesat dengan potensi signifikan untuk diadopsi di berbagai sektor, termasuk di Indonesia. Sebuah kajian menunjukkan bahwa Indonesia menempati peringkat kedua terbesar di Asia Tenggara dalam penerapan IoT, hanya di bawah Thailand. Beberapa perusahaan domestik di Indonesia, seperti Blue Bird, Pertamina Patra Niaga, dan Gojek, telah mengintegrasikan teknologi IoT ke dalam operasi bisnis mereka.

Namun, dengan proliferasi perangkat *Internet of Thing*s (IoT) yang semakin meluas, imperatif untuk implementasi keamanan yang kuat menjadi semakin mendesak. Interkonektivitas antarperangkat IoT menimbulkan kerentanan tinggi terhadap spektrum ancaman keamanan, mulai dari eksfiltrasi data hingga serangan ransomware. Meskipun teknologi IoT menawarkan transformasi revolusioner di berbagai sektor industri serta peningkatan kualitas kehidupan harian, teknologi ini juga mengandung risiko substansial bagi individu dan entitas organisasional. Perangkat IoT sering kali mengakuisisi data sensitif, seperti informasi kesehatan, preferensi personal, dan bahkan data lokasi, yang menjadikannya sasaran utama bagi aktor kejahatan siber. Tanpa protokol keamanan yang adekuat, perangkat IoT dapat dieksploitasi untuk berbagai maksud malignan, termasuk kegiatan intelijen, perampasan data, dan serangan terhadap infrastruktur vital.

Penelitian terkini menggarisbawahi insiden kegagalan keamanan dalam *Internet of Thing*s (IoT), khususnya kerentanan pada sistem rumah pintar yang memungkinkan pengguna tidak bertanggung jawab untuk menguasai perangkat terhubung (Laghari, 2024). Kemajuan pesat IoT telah merevolusi pola hidup kontemporer melalui penyediaan konektivitas tanpa batas, kecerdasan buatan, serta otomatisasi di lingkungan domestik, korporasi, sistem kesehatan, transportasi, dan infrastruktur vital. Mayoritas perangkat IoT dirancang dengan mekanisme keamanan yang minim, sering kali bergantung pada kata sandi standar atau protokol autentikasi yang tidak kuat, sehingga menjadikannya target rentan bagi penyerang yang berusaha memperoleh akses ilegal. Setelah berhasil dikompromikan, perangkat tersebut dapat dimanfaatkan untuk aktivitas berbahaya, seperti pencurian informasi, pelanggaran privasi, serta keterlibatan dalam serangan siber skala besar.

Dengan mempertimbangkan urgensi pengembangan langkah-langkah keamanan siber proaktif, hal ini bertujuan untuk menjamin integritas dan resiliensi ekosistem *Internet of Thing*s (IoT) terhadap ancaman yang muncul. Temuan penelitian ini dirancang untuk memberikan dukungan kepada produsen perangkat, pengembang, pembuat kebijakan, serta praktisi keamanan dalam membentuk ekosistem IoT yang lebih robust, mampu bertahan terhadap ancaman siber yang terus berevolusi dalam lingkungan dunia yang semakin terinterkoneksi. Perangkat IoT telah

terintegrasi secara intrinsik ke dalam kehidupan sehari-hari, dan kompromi terhadapnya tidak hanya mengakibatkan eksfiltrasi data, tetapi juga kerusakan fisik serta gangguan terhadap layanan kritis atau operasi bisnis (Xu, 2024). Oleh karena itu, penelitian ini mengkaji berbagai tantangan keamanan siber dalam ekosistem digital kontemporer. Selain itu, penelitian ini juga menyelidiki mekanisme deteksi intrusi berbasis kecerdasan buatan yang meningkatkan kapasitas untuk mengidentifikasi dan memitigasi ancaman siber secara real-time (Radanliev, 2024). Dengan menggunakan pendekatan literature review untuk mengkaji dan menganalisis berbagai sumber literatur yang relevan tentang *Internet of Thing*s (Iot) Sebagai Pilar Keamanan Data Pada Sistem Distribusi Di Indonsia. Literatur yang digunakan mencakup jurnal ilmiah, buku, laporan industri, dan artikel terpercaya yang dipublikasikan dalam rentang waktu terbaru.

KAJIAN TEORITIS

Berdasarkan hasil penelitian yang membahas mengenai keamanan data dalam sistem distribusi berbasis Industrial Internet of Things (IIoT) menunjukkan pendekatan yang beragam namun saling melengkapi. Alanazi dan Aljuhani (2023) menyoroti pentingnya sistem deteksi anomali dalam mengenali pola serangan siber di lingkungan IIoT. Temuan mereka menunjukkan bahwa teknologi ini efektif dalam meminimalisasi manipulasi data dan meningkatkan keamanan jaringan, sehingga sangat relevan untuk perlindungan data operasional industri. Sementara itu, Bobde et al. (2024) mengusulkan penggunaan teknologi blockchain sebagai solusi keamanan IIoT. Blockchain dinilai mampu meningkatkan integritas, transparansi, dan keamanan data, serta mengurangi risiko perubahan data, menjadikannya fondasi penting dalam distribusi data industri yang aman dan terverifikasi. Di sisi lain, Dhirani et al. (2021) mengidentifikasi berbagai celah keamanan pada perangkat IoT dan menekankan perlunya protokol serta standar keamanan yang lebih kuat. Kajian ini memberikan dasar penting bagi pengembangan regulasi dan kebijakan keamanan nasional dalam konteks distribusi berbasis IoT. Adapun Jurgeläne dan Batenko (2023) menekankan bahwa transformasi digital dalam rantai pasok memerlukan perlindungan data yang kuat untuk mencegah kebocoran dan serangan siber. Studi ini sangat relevan bagi Indonesia yang tengah mengembangkan sistem distribusi digital, karena menyoroti kebutuhan akan proteksi data dalam proses supply chain berbasis IoT.

Peneliti dan Tahun	Nama jurnal	Fokus peenlitian	Temuan	Relevansi
Alanazi & Aljuhani (2023)	Computers, Materials & Continua (Tech Science Press)	Deteksi anomali pada serangan siber di lingkungan IIoT	Sistem deteksi anomali mampu mengenali pola serangan, meminimalkan manipulasi data, serta meningkatkan keamanan jaringan IoT industri.	Membahas penguatan keamanan data di sistem IoT industri, yang langsung terkait dengan distribusi industri.
Bobde et al. (2024)	Electronics (MDPI)	Keamanan IIoT menggunakan teknologi blockchain	Blockchain meningkatkan integritas, transparansi, dan keamanan data dalam lingkungan	IoT perlu teknologi pendukung agar menjadi pilar keamanan data

			IIoT; meminimalkan risiko perubahan data.	pada distribusi industri.
Dhirani et al. (2021)	Sensors (Basel, Switzerland)	Analisis ancaman siber & standar keamanan IoT	Banyak celah keamanan ditemukan pada perangkat IoT; dibutuhkan protokol keamanan yang lebih kuat dan standar implementasi industri.	Tantangan keamanan yang muncul ketika IoT digunakan dalam sistem distribusi industri
Jurgelāne & Batenko (2023)	WSB Journal of Business and Finance, Volume 57(1)	Keamanan data pada rantai pasok digital	Transformasi digital dalam supply chain memerlukan perlindungan data yang kuat untuk mencegah kebocoran dan serangan.	Keamanan data dan proses distribusi industri yang berbasis digital/IoT.

Secara keseluruhan, keempat studi tersebut memperkuat pemahaman bahwa keamanan data merupakan pilar utama dalam implementasi IIoT, dan bahwa pendekatan teknologi seperti deteksi anomali, blockchain, serta penguatan standar keamanan harus diintegrasikan secara strategis dalam sistem distribusi industri.

METODE PENELITIAN

Metode penelitian ini menggunakan pendekatan literature review untuk mengkaji dan menganalisis berbagai sumber literatur yang relevan tentang *Internet of Thing*s (Iot) Sebagai Pilar Keamanan Data Pada Sistem Distribusi Di Indonsia. Literatur yang digunakan mencakup jurnal ilmiah, buku, laporan industri, dan artikel terpercaya yang dipublikasikan dalam rentang waktu terbaru. Analisis dilakukan dengan membandingkan berbagai temuan dan merangkum implikasi praktisnya bagi industri. Metode ini memberikan landasan yang kuat untuk menghasilkan kajian komprehensif dan relevan.

HASIL PENELITIAN DAN PEMBAHASAN

A. Penerapan teknologi *Internet of Thing*s (IoT) dalam mendukung keamanan data pada sistem distribusi industri

Penerapan teknologi *Internet of Thing*s (IoT) dalam mendukung keamanan data pada sistem distribusi industri, khususnya dalam konteks Industrial *Internet of Thing*s (IoT), sangat penting mengingat semakin kompleks dan terintegrasinya sistem industri modern. Beberapa komponen fundamental dari IoT mencakup perangkat seperti sistem kontrol industri dan teknologi otomatisasi, yang semuanya berkontribusi dalam menciptakan lingkungan yang efisien

namun rentan terhadap ancaman siber. Oleh karena itu, penerapan teknologi keamanan seperti deteksi intrusi, otentikasi terjamin, dan enkripsi menjadi esensial untuk menjaga integritas data dan melindungi sistem dari serangan. Pentingnya langkah keamanan ini juga ditegaskan oleh Jurgelāne & Batenko (2023), yang menyoroti bahwa peningkatan digitalisasi harus diikuti oleh penguatan keamanan data guna mengurangi risiko eksploitasi dalam ekosistem IoT.

*Internet of Thing*s (IoT) telah menjadi salah satu fondasi utama dalam peningkatan keamanan data pada sistem distribusi industri di Indonesia. IoT memungkinkan setiap komponen dalam rantai distribusi mulai dari proses produksi, pergudangan, hingga pengantaran barang terhubung dalam satu ekosistem digital melalui sensor, perangkat pintar, dan jaringan berbasis cloud. Melalui hubungan ini, keamanan data dapat dikelola secara lebih terintegrasi, real-time, dan akurat. Hal ini sejalan dengan temuan Altubaishe et al., (2024) yang menunjukkan bahwa kemampuan IoT untuk mengumpulkan dan menganalisis data secara real-time telah menjadi faktor penting dalam transformasi manajemen rantai pasokan menuju efisiensi dan fleksibilitas yang lebih tinggi.

Penerapan IoT pada sistem distribusi di Indonesia umumnya dilakukan melalui penggunaan sensor untuk memonitor kondisi barang, *GPS tracker* untuk memantau posisi kendaraan distribusi, RFID (*Radio Frequency Identification*) untuk identifikasi dan pencatatan otomatis, serta platform cloud yang menyimpan seluruh data logistik. Sistem ini tidak hanya mendukung efisiensi operasional, tetapi juga memastikan bahwa data yang tersimpan dan ditransmisikan lebih aman karena melewati proses enkripsi dan autentikasi. Dengan memanfaatkan teknik pembelajaran mendalam, data yang dihasilkan oleh berbagai sensor dapat diproses untuk mendeteksi pola aneh yang mungkin menunjukkan adanya pelanggaran keamanan (Awotunde et al., 2021). Selain itu, penggunaan teknologi kriptografi menjadi langkah penting dalam melindungi data IoT berbasis cloud, sebagaimana dijelaskan oleh Qasem et al., (2024) bahwa enkripsi yang kuat mampu memberikan perlindungan lebih baik terhadap serangan siber yang menargetkan sistem IoT.

Berdasarkan temuan beberapa penelitian, salah satu hasil utama adalah meningkatnya ketepatan dan kecepatan deteksi ancaman terhadap keamanan data. Salah satu metode yang banyak digunakan adalah deteksi anomali yang dapat membantu mengidentifikasi perilaku abnormal dalam jaringan IoT, yang sering kali merupakan indikasi adanya serangan siber. Penelitian oleh Alanazi & Aljuhani (2023) menunjukkan pentingnya penggunaan mekanisme deteksi anomali dalam mencegah serangan pada sistem kontrol industri. Hal ini mengurangi risiko manipulasi data, kehilangan data, maupun pencurian barang. Selain itu, IoT juga membantu perusahaan dalam memastikan bahwa seluruh alur distribusi berlangsung sesuai standar keamanan yang telah ditetapkan, sehingga setiap bentuk penyimpangan dapat segera diidentifikasi.

Penerapan IoT juga mendukung keamanan data melalui pengurangan campur tangan manusia (*human intervention*) dalam proses pencatatan dan pengambilan keputusan. Dengan demikian, potensi kesalahan manual yang dapat mengancam integritas data dapat diminimalisir. Pada beberapa industri seperti makanan-minuman, farmasi, dan manufaktur, sensor IoT membantu memastikan bahwa kondisi barang tetap terjaga sesuai standar, sehingga kualitas produk dapat dipertahankan selama proses distribusi.

Namun, implementasi IoT sebagai pilar keamanan data tidak terlepas dari tantangan. Dengan meningkatnya ketergantungan terhadap infrastruktur IIoT, masalah keamanan tidak bisa diabaikan. Riset oleh Gupta dan Singh (Dhirani et al., 2021) menyatakan bahwa kombinasi antara teknologi baru dan tantangan keamanan yang dihadapi sangat memerlukan perhatian ekstra untuk

mengembangkan solusi yang memastikan operasi industri tetap berjalan lancar dan aman. Salah satu temuan penting adalah adanya kerentanan terhadap serangan siber karena seluruh sistem terhubung secara online. Jika tidak terlindungi dengan protokol keamanan yang kuat seperti enkripsi, firewall, dan sistem deteksi intrusi, maka perangkat IoT dapat menjadi celah masuk bagi pelaku kejahatan siber.

Dalam konteks ini, integrasi teknologi blockchain telah menjadi salah satu solusi yang banyak diteliti. Bobde et al., (2024) menegaskan bahwa blockchain mampu meningkatkan integritas dan privasi data pada jaringan IoT industri melalui sistem yang transparan dan tidak dapat diubah. Hal ini diperkuat oleh (Din et al., 2019) yang menyatakan bahwa kombinasi IoT dan blockchain dapat mengatasi kerentanan keamanan yang sering terjadi di ekosistem IoT terpadu.

Secara keseluruhan, penerapan IoT terbukti efektif dalam mendukung keamanan data pada sistem distribusi industri di Indonesia. IoT tidak hanya memperkuat pengawasan dan pengendalian secara real-time, namun juga meningkatkan transparansi proses, akurasi pelaporan, serta mempercepat pengambilan keputusan berbasis data. Dengan pemanfaatan yang tepat dan perlindungan keamanan yang memadai, IoT akan terus menjadi pilar penting dalam pengelolaan distribusi yang aman, efisien, dan berkelanjutan di berbagai sektor industri Indonesia.

B. Tantangan Yang Dihadapi Dalam Penerapan Iot Sebagai Pilar Keamanan Data Pada Sistem Distribusi Industri

*Internet of Thing*s (IoT) menyediakan manfaat signifikan bagi para pengguna, meskipun disertai oleh sejumlah tantangan. Keamanan siber serta risiko privasi merupakan fokus utama perhatian bagi para peneliti dan ahli keamanan yang disebutkan. Kedua aspek tersebut menimbulkan masalah substansial bagi berbagai organisasi bisnis dan entitas publik. Insiden keamanan siber berskala besar yang terjadi secara teratur telah menyoroti kerentanan bawaan dari teknologi *Internet of Thing*s (IoT). Kerentanan tersebut timbul dari karakteristik interkonektivitas jaringan pada sistem IoT, yang memungkinkan akses oleh entitas anonim dan tidak terpercaya melalui internet, sehingga menuntut pengembangan langkah-langkah keamanan inovatif (Mishra, N., & Pandya, 2021).

Analisis keamanan sistem informasi dalam lingkungan *Internet of Thing*s (IoT) telah berhasil mengidentifikasi berbagai jenis ancaman yang mengintai, yang berpotensi memengaruhi kelangsungan operasi serta keamanan infrastruktur IoT (Darumaya, 2023). Volume dan penerapan perangkat *Internet of Thing*s (IoT) yang signifikan memunculkan spektrum tantangan keamanan yang kompleks. Banyak perangkat IoT dideploy di lingkungan yang tidak terkontrol atau dioperasikan dengan cara yang tidak diperkirakan selama tahap desainnya, sehingga meningkatkan kerentanannya terhadap eksploitasi. Salah satu tantangan fundamental adalah absensi standar keamanan universal untuk perangkat IoT. Berbeda dengan sistem komputasi konvensional, perangkat IoT sering kali tidak dilengkapi dengan mekanisme autentikasi yang robust, seperti autentikasi multi-faktor, dan mengadopsi protokol enkripsi yang ketinggalan zaman, yang menjadikannya rentan terhadap serangan (Bari et al., 2021). Banyak perangkat IoT memiliki kemampuan pemrosesan yang terbatas, yang membatasi penerapan langkah-langkah keamanan canggih seperti enkripsi dan otentikasi berlapis (Radanliev, 2024). Meskipun perangkat ini meningkatkan efisiensi operasional serta konektivitas, ia juga menimbulkan kerentanan yang belum pernah terjadi sebelumnya, yang dapat dieksploitasi oleh pengguna yang tidak bertanggung jawab (Doifode S. P., 2024). Melalui penerapan metodologi Pengujian Penetrasi Berbasis Ancaman, organisasi mampu mensimulasikan serangan siber yang bersifat dunia nyata guna mengidentifikasi kelemahan dalam mekanisme pertahanan mereka, serta menangani potensi

pelanggaran secara proaktif (Pourrahmani, 2023). Hal ini memungkinkan agar organisasi memperkuat regulasi ketat, seperti Undang-Undang Ketahanan Operasional Digital, yang menetapkan kerangka kerja keamanan siber yang kuat bagi entitas keuangan (Doifode S. P., 2024).

Perspektif mengenai kegunaan *Internet of Thing*s (IoT) sangat bergantung pada kemampuan teknologi tersebut untuk menjaga privasi pengguna. Kekhawatiran yang terkait dengan privasi serta risiko inheren yang melekat pada IoT berpotensi menjadi penghalang substansial bagi adopsi IoT secara menyeluruh Wibowo (2023). Oleh karena itu, diperlukan inisiatif yang terkoordinasi dari berbagai pemangku kepentingan, meliputi produsen, penyedia layanan, pengguna akhir, serta regulator, guna merancang strategi keamanan yang tangguh dan efisien dalam menanggulangi ancaman pada era *Internet of Thing*s (IoT) ini. Pendekatan ini melibatkan implementasi standar keamanan yang ketat, pengawasan berkelanjutan terhadap lalu lintas jaringan, peningkatan literasi keamanan di kalangan pengguna, serta kerja sama untuk mengatasi tantangan interoperabilitas dan ketidakkonsistenan standar keamanan. Melalui langkah-langkah tersebut, diharapkan dapat terbentuk ekosistem IoT yang lebih aman dan dapat diandalkan, sehingga menjaga integritas data serta keamanan infrastruktur di tengah era konektivitas dan kemajuan teknologi yang semakin kompleks.

Dalam ranah *Internet of Thing*s (IoT), interaksi dan komunikasi antarperangkat yang berasal dari beragam produsen merupakan suatu keharusan. Namun, adanya ketidakselarasan atau keterbatasan dalam aspek interoperabilitas berpotensi menimbulkan kerentanan serius terhadap keamanan sistem, karena kondisi tersebut dapat membuka peluang terjadinya eksploitasi maupun serangan siber yang signifikan (Widarti, 2024). Walaupun interoperabilitas penuh tidak selalu dapat diwujudkan di seluruh produk dan layanan, pengguna cenderung menolak pembelian produk dan layanan yang kurang fleksibel serta menimbulkan keprihatinan terkait ketergantungan pada penyedia layanan. Perangkat IoT yang dirancang secara tidak memadai dapat menimbulkan dampak negatif terhadap sumber daya jaringan yang terhubung dengannya (Zaldivar et al., 2020). Salah satu permasalahan krusial dalam ekosistem *Internet of Thing*s (IoT) muncul ketika perangkat tidak memiliki kemampuan untuk melakukan validasi maupun enkripsi atas data yang dikirimkan atau diterima dari perangkat lain. Kondisi tersebut berimplikasi pada meningkatnya kerentanan data sensitif yang ditransmisikan melalui jaringan IoT terhadap risiko pencurian maupun manipulasi oleh pihak yang tidak berwenang. Lebih lanjut, absennya standar interoperabilitas yang komprehensif turut membuka peluang terjadinya serangan, seperti *spoofing* dan *man-in-the-middle*, di mana aktor jahat dapat mengeksploitasi kelemahan sistem dengan menipu perangkat IoT agar berinteraksi dengan entitas palsu atau menyusup untuk memperoleh data yang sedang dipertukarkan dalam jaringan

Akuntabilitas dalam pengelolaan kepercayaan menuntut agar setiap aktivitas dapat ditelusuri secara eksplisit kepada entitas yang telah terautentikasi. Sistem pengelolaan kepercayaan dituntut memiliki kapasitas untuk mengakomodasi jumlah entitas yang besar, mendukung mekanisme delegasi akses, mengatur tindakan lintas domain organisasi, serta memastikan keberlanjutan derivasi data. Dalam konteks ini, pengelolaan kepercayaan berfungsi sebagai komponen otonom yang mampu mengendalikan aliran informasi sekaligus mencegah kebocoran data pribadi ke perangkat yang tidak sah. Para peneliti mengadopsi teori himpunan kabur dan bahasa berbasis semantik formal sebagai landasan penerapan mekanisme kepercayaan berlapis, yang kemudian dievaluasi melalui atribut spesifik pada setiap lapisan, seperti efisiensi, tingkat risiko, dan riwayat interaksi. Akses pengguna terhadap ekosistem IoT hanya dimungkinkan apabila kredensial keamanan yang dimiliki sesuai dengan kebijakan keamanan, yang ditentukan melalui fungsi pengambilan keputusan berbasis nilai kepercayaan pengguna.

Menurut Harry et al., (2025) Regulasi dalam konteks *Internet of Thing*s (IoT) memainkan peran krusial dalam menjamin operasional ekosistem IoT yang aman, reliabel, serta selaras

dengan prinsip-prinsip perlindungan data dan privasi pengguna. Mengingat IoT melibatkan jutaan perangkat yang saling terinterkoneksi melintasi berbagai sektor dan batas negara, diperlukan kerangka hukum serta standar teknis yang homogen untuk meminimalkan risiko ancaman keamanan siber, eksploitasi data, serta inkompatibilitas interoperabilitas antar perangkat. Pada dasarnya, regulasi IoT berfungsi untuk mengatur tata kelola data, keamanan perangkat, serta tanggung jawab penyedia layanan dan pengguna. Tujuan utamanya adalah membangun kepercayaan (*trust*) di antara semua aktor yang terlibat dalam ekosistem digital.

Regulasi ini mencakup berbagai dimensi, seperti privasi data personal, keamanan infrastruktur jaringan, sertifikasi perangkat, serta mitigasi terhadap ancaman serangan siber. Pemerintah memperkuat regulasi yang berkaitan dengan keamanan data dan privasi melalui sejumlah kebijakan, diantaranya: a. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang mengatur hak pengguna atas data pribadi serta kewajiban penyelenggara sistem elektronik untuk menjaga keamanan dan kerahasiaannya; b. Peraturan Menteri Kominfo No. 4 Tahun 2016 tentang Sistem Elektronik, yang mengatur penyelenggaraan dan perlindungan data dalam layanan berbasis teknologi, termasuk IoT: c. Strategi Keamanan Siber Nasional (BSSN), yang berfokus pada penguatan keamanan siber nasional melalui kolaborasi antar lembaga dan pelaku industri teknologi.

C. Faktor-faktor yang mempengaruhi efektivitas IoT dalam menjaga keamanan data pada sistem distribusi industri

Efektivitas IoT dalam menjaga keamanan data pada sistem distribusi industri dipengaruhi oleh faktor teknis, organisasi, dan regulasi. Kelemahan pada salah satu aspek ini dapat membuka celah bagi kebocoran atau serangan siber a. Kualitas Perangkat dan Infrastruktu : Keamanan data sangat bergantung pada keandalan perangkat IoT yang digunakan. Sensor atau gateway yang tidak memiliki standar keamanan tinggi dapat menjadi titik masuk bagi peretas. Perangkat dengan firmware usang atau tidak diperbarui secara berkala juga meningkatkan risiko. Selain itu, keterbatasan daya komputasi pada perangkat IoT membuatnya sulit menjalankan algoritma enkripsi yang kompleks, sehingga menurunkan efektivitas perlindungan; b. Protokol Komunikasi dan Enkripsi : Data dalam sistem distribusi industri sering berpindah antar node, server, dan cloud. Tanpa protokol komunikasi aman (misalnya TLS atau MQTT-S), data dapat disadap atau dimanipulasi. Faktor penting lainnya adalah implementasi enkripsi end-to-end. Jika enkripsi hanya dilakukan sebagian, maka data tetap rentan saat transit. Efektivitas IoT meningkat bila sistem mampu menjaga kerahasiaan, integritas, dan autentikasi data sepanjang rantai distribusi; c. Manajemen Identitas dan Akses : IoT dalam industri melibatkan ribuan perangkat yang saling terhubung. Tanpa manajemen identitas digital yang kuat, perangkat palsu dapat menyusup ke jaringan. Sistem distribusi yang efektif biasanya menerapkan multi-factor authentication (MFA) dan role-based access control (RBAC) untuk membatasi akses hanya pada pihak yang berwenang. Faktor ini menentukan apakah data tetap terlindungi dari insider threat maupun serangan eksternal; d. Ketahanan terhadap Serangan Siber : Efektivitas IoT juga dipengaruhi oleh kemampuan sistem menghadapi serangan DDoS, malware, atau man-in-the-middle attack. Sistem distribusi industri yang tidak memiliki mekanisme deteksi intrusi (IDS) atau firewall berbasis IoT akan lebih mudah lumpuh. Oleh karena itu, lapisan keamanan berlapis (defense in depth) menjadi faktor penting agar data tetap aman meski terjadi serangan; e. Kebijakan Organisasi dan Regulasi : Selain aspek teknis, budaya keamanan dalam organisasi sangat menentukan. Jika operator tidak dilatih mengenai praktik keamanan, maka human error dapat membuka celah. Regulasi industri juga berperan, misalnya standar ISO/IEC 27001 atau aturan perlindungan data nasional. Kepatuhan terhadap regulasi memastikan bahwa sistem distribusi tidak hanya aman secara teknis, tetapi juga sah secara hokum; f. Integrasi dengan Teknologi Pendukung : Efektivitas IoT meningkat bila didukung oleh cloud computing, edge computing, dan AI. Edge computing memungkinkan pemrosesan data dekat dengan sumber, sehingga mengurangi risiko kebocoran

saat data dikirim ke pusat. AI dapat digunakan untuk mendeteksi anomali dalam pola distribusi data, sehingga ancaman bisa diidentifikasi lebih cepat.

KESIMPULAN

*Internet of Thing*s (IoT) telah terbukti memainkan peran strategis sebagai pilar utama dalam menjamin keamanan data pada sistem distribusi industri di Indonesia. Melalui integrasi sensor, perangkat cerdas, serta jaringan berbasis komputasi awan, IoT tidak hanya meningkatkan efisiensi operasional, tetapi juga memperkuat integritas data melalui penerapan mekanisme keamanan seperti enkripsi, otentikasi, deteksi intrusi, dan analisis anomali. Implementasi IoT turut berkontribusi dalam meminimalisasi kesalahan manual serta memastikan konsistensi kualitas produk sepanjang rantai distribusi. Namun demikian, tingkat efektivitasnya sangat bergantung pada penguatan aspek teknis, kelembagaan, dan regulasi yang diperlukan untuk menghadapi tantangan terkait keamanan, privasi, interoperabilitas, serta manajemen kepercayaan. Dengan penguatan dimensi-dimensi tersebut, IoT berpotensi menjadi fondasi krusial dalam mendukung perlindungan data sekaligus mempercepat transformasi digital pada sektor distribusi industri di Indonesia.

DAFTAR PUSTAKA

Alanazi, R., & Aljuhani, A. (2023). *Anomaly Detection for Industrial Internet of Things Cyberattacks*. https://doi.org/10.32604/csse.2023.026712

Altubaishe, B., Zafar, S., & Bhalla, P. (2024). Revolutionizing the Supply Chain: A Comprehensive Analysis of the Impact of Industry 4.0 on Supply Chain Management. *International Journal of Religion*, *5*, 4722–4737. https://doi.org/10.61707/2p0f3e58

Awotunde, J. B., Chakraborty, C., & Adeniyi, and A. E. (2021). *Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection - Awotunde - 2021 - Wireless Communications and Mobile Computing - Wiley Online Library* (p. 17). https://onlinelibrary.wiley.com/doi/pdf/10.1155/2021/7154587

Bobde, Y., Narayanan, G., Jati, M., Raj, R., Cvitić, I., & Perakovic, D. (2024). Enhancing Industrial IoT Network Security through Blockchain Integration. *Electronics*, *13*, 687. https://doi.org/10.3390/electronics13040687

Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Sensors (Basel, Switzerland)*, *21*(11). https://doi.org/10.3390/s21113901

Din, I. U., Guizani, M., Hassan, S., Kim, B.-S., Khan, M. K., Atiquzzaman, M., & Ahmed, S. H. (2019). The *Internet of Thing*s: A Review of Enabled Technologies and Future Challenges. *IEEE Access*, *7*, 7606–7640. https://doi.org/10.1109/ACCESS.2018.2886601

Jurgelāne, I., & Batenko, A. (2023). *Assessment of Data Security Implementation in the Supply Chain Enterprises in Latvia*. *57*(1), 21–27. https://doi.org/10.2478/WSBJBF-2023-0003

Qasem, M. A., Thabit, F., Can, O., Naji, E., Alkhzaimi, H. A., Patil, P. R., & Thorat, S. B. (2024). Cryptography algorithms for improving the security of cloud-based *Internet of Thing*s. *Security and Privacy*, *7*. https://api.semanticscholar.org/CorpusID:268245073

Chen, Z. G. (2024). *Internet of Thing*s and Cyber-Physical System

Laghari, A. A. (2024). *Internet of Thing*s (IoT) applications security trends and challenges. Discover *Internet of Thing*s, 4(1), 36.

Nag, A. H. (2024). Exploring the applications and security threats of *Internet of Thing* in the cloud computing paradigm: A comprehensive study on the cloud of things. Transactions on Emerging Telecommunications Technologies, 35(4), e4897

Xu, H. L. (2024). Security risks concerns of generative AI in the IOT. IEEE *Internet of Thing*s Magazine, 7(3), 62-67.

Radanliev, P. D. (2024). AI security and cyber risk in IoT systems. Frontiers in Big Data, 7, 1402745

Bari, A., et al. (2021). Security and privacy challenges in IoT: A survey. IEEE Transactions on Industrial Informatics, 17(3), 2041–2050.

Doifode, S. P. (2024). Cybersecurity in the *Internet of Thing*s (IoT): Challenges and Solutions. International Journal of Scientific Research in Modern Science and Technology, 3(7), 17-21.

Pourrahmani, H. Y. (2023). A review of the security vulnerabilities and countermeasures in the *Internet of Thing*s solutions: A bright future for the Blockchain. *Internet of Thing*s, 23, 100888.

Wibowo, A. (2023). *Internet of Thing*s (Iot) Dalam Ekonomi Dan Bisnis Digital. Penerbit Yayasan Prima Agus Teknik, 1-94.

Zaldivar, D.; Tawalbeh, L.; Muheidat, F. Investigating the Security Threats on Networked Medical Devices. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6 January 2020; pp. 0488–0493.

Kumar, A., Gaurav, K., Akpabio, E., & Kumar, N. (2025). Security and Privacy for *Internet of Thing*s: Challenges and Solutions. *JOURNAL OF INTELLIGENT SYSTEMS AND COMPUTING*. https://doi.org/10.51682/jiscom.v6i1.68.

Mishra, N., & Pandya, S. (2021). *Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions*: A Systematic Review. IEEE Access, 9, 59353-5937. https://doi.org/10.1109/access.2021.3073408.

Widarti, E., Joosten, J., Pratiwi, P. Y., Pradnyana, G. A., Indradewi, I. G. A. A. D., Kamilah, N., & Sepriano, S. (2024). *BUKU AJAR PENGANTAR SISTEM INFORMASI*. PT. Sonpedia Publishing Indonesia.

Setya , Harry., et al (2025) *INTERNET OF THING(IOT) : PRINSIP DAN IMPLEMENTASINYA*. Bekasi: Yayasan Putra Adi Dharma