Jurnal Multidisiplin West Science
Vol. 03, No. 05, Mei 2024, pp. 611-623

Analisis Dampak Keamanan IoT dan Integrasi Sistem Informasi terhadap Perlindungan Data dan Kinerja Operasional di Perusahaan Telekomunikasi Yogyakarta

Anggun Nugroho[1], Rahmad Syaifudin[2], Affan Irfan Fauziawan[3]
[1] Institut Teknologi dan Bisnis STIKOM Bali dan anggun.nugroho12@gmail.com
[2] Prodi Teknik Elektro Fakultas Teknik Universitas Tulungagung dan syaifudinrahmad@unita.ac.id
[3] Institut Teknologi dan Bisnis STIKOM Bali dan affanfauziawan@gmail.com

ABSTRAK

Penelitian ini menyelidiki dampak dari keamanan IoT dan integrasi sistem informasi terhadap perlindungan data dan kinerja operasional di perusahaan telekomunikasi di Yogyakarta, Indonesia. Pendekatan kuantitatif menggunakan Structural Equation Modeling (SEM) dengan metodologi Partial Least Squares (PLS) digunakan untuk menganalisis data survei yang dikumpulkan dari 150 karyawan dan manajer. Temuan ini mengungkapkan hubungan positif yang signifikan antara keamanan IoT, integrasi sistem informasi, perlindungan data, dan kinerja operasional. Tingkat keamanan IoT dan integrasi sistem informasi yang lebih tinggi dikaitkan dengan peningkatan praktik perlindungan data dan kinerja operasional. Hasil ini menggarisbawahi pentingnya berinvestasi pada langkah-langkah keamanan yang kuat dan infrastruktur TI yang kohesif untuk meningkatkan ketahanan dan kinerja organisasi di sektor telekomunikasi. Studi ini memberikan wawasan yang berharga bagi para praktisi dan pembuat kebijakan yang ingin menavigasi lanskap keamanan siber yang kompleks dan transformasi digital di perusahaan telekomunikasi.

Kata Kunci: *Keamanan IoT, Integrasi Sistem Informasi, Perlindungan Data, Kinerja Operasional, Perusahaan Telekomunikasi*

ABSTRACT

This study investigates the impact of IoT security and information system integration on data protection and operational performance in telecommunication companies in Yogyakarta, Indonesia. A quantitative approach using Structural Equation Modeling (SEM) with Partial Least Squares (PLS) methodology was used to analyze survey data collected from 150 employees and managers. The findings revealed significant positive relationships between IoT security, information system integration, data protection, and operational performance. Higher levels of IoT security and information system integration were associated with improved data protection practices and operational performance. These results underscore the importance of investing in robust security measures and a cohesive IT infrastructure to improve organizational resilience and performance in the telecommunications sector. This study provides valuable insights for practitioners and policymakers looking to navigate the complex landscape of cybersecurity and digital transformation in telecom companies.

Keywords: *IoT Security, Information System Integration, Data Protection, Operational Performance, Telecommunication Company*

PENDAHULUAN

Perusahaan telekomunikasi berada di garis depan revolusi digital, memanfaatkan teknologi IoT dan sistem informasi untuk meningkatkan konektivitas dan efisiensi operasional (Fetaji et al., 2023). Integrasi perangkat IoT menawarkan peluang besar untuk mendapatkan wawasan berbasis data dan layanan yang lebih baik, namun juga menimbulkan kerentanan keamanan yang signifikan yang dapat membahayakan perlindungan data dan kinerja secara keseluruhan (Jabeen & Ishaq,

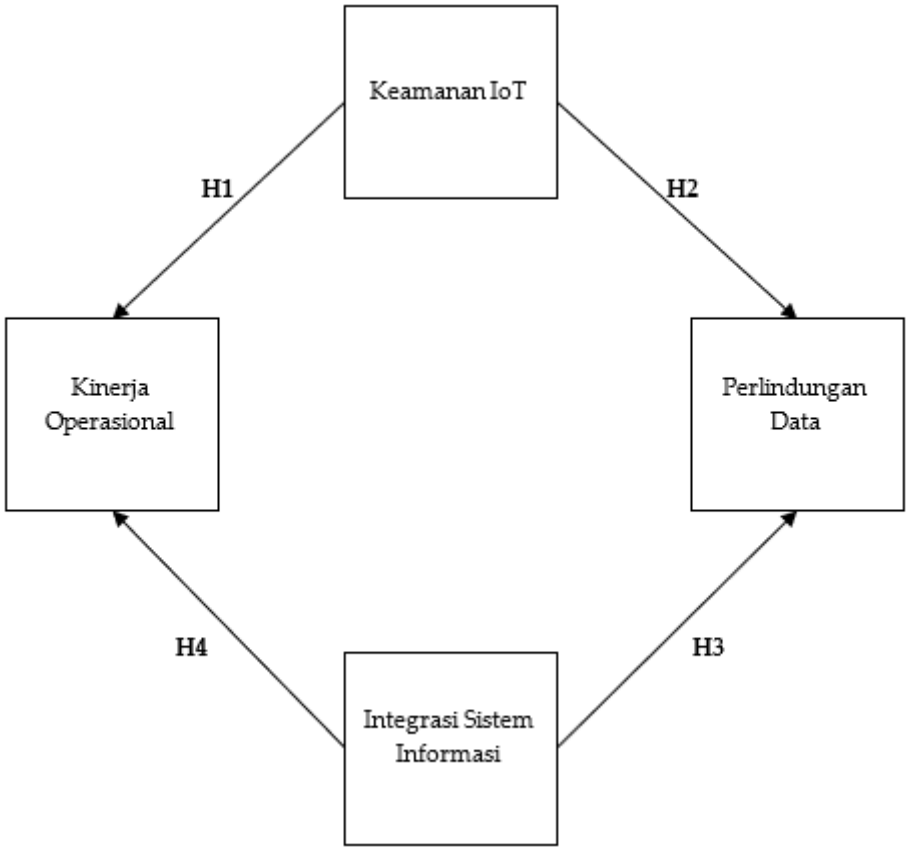
2023; Sazonova & Shmalii, 2023). Ketika perusahaan-perusahaan ini menavigasi lanskap IoT, mereka harus memprioritaskan strategi manajemen data yang kuat untuk melindungi dari ancaman dunia maya, akses tidak sah, dan pelanggaran data (Ajayi et al., 2023). Dengan merangkul model bisnis yang inovatif dan kemitraan strategis, operator telekomunikasi dapat memanfaatkan potensi IoT sambil mengurangi risiko terkait, memastikan infrastruktur digital yang aman dan tangguh untuk komunikasi dan konektivitas yang lancar di lingkungan digital yang dinamis saat ini.

Dalam lingkungan bisnis yang dinamis, implementasi teknologi Internet of Things (IoT) telah memberikan dampak yang signifikan terhadap berbagai industri, termasuk perusahaan telekomunikasi, dengan menawarkan peluang untuk pertumbuhan bisnis dan peningkatan keterlibatan pelanggan (Doss et al., 2022; Gupta & Singh, 2022). Namun, meningkatnya ketergantungan pada IoT telah menimbulkan kekhawatiran tentang kerentanan keamanan dan kebutuhan akan langkah-langkah keamanan yang kuat untuk melindungi data dan memastikan efisiensi operasional (Barani Sundaram et al., 2022; Kuzminykh et al., 2021). Penelitian telah menunjukkan bahwa banyak perusahaan tidak memiliki keahlian internal dalam keamanan IoT dan sering kali mengalihdayakan operasi keamanan ke penyedia khusus, yang menunjukkan adanya kesenjangan dalam memahami metode perlindungan data dan keamanan perangkat yang canggih (Shim et al., 2017). Selain itu, penelitian menyoroti pentingnya mengintegrasikan sistem informasi untuk memperkuat perlindungan data dan efisiensi operasional di dalam perusahaan telekomunikasi, yang menekankan perlunya langkah-langkah keamanan yang komprehensif untuk mengurangi ancaman dunia maya dan memastikan pertumbuhan yang berkelanjutan.

Perusahaan telekomunikasi di Yogyakarta, seperti halnya perusahaan telekomunikasi di seluruh dunia, menghadapi berbagai peluang dan tantangan di era digital. Munculnya perangkat IoT di jaringan telekomunikasi telah memfasilitasi pengumpulan data secara real-time, analisis prediktif, dan meningkatkan pengalaman pelanggan (Fathun, 2023). Namun, kemajuan teknologi ini juga membawa ancaman keamanan siber yang signifikan yang membayangi industri ini. Sifat perangkat IoT yang saling terhubung dan integrasi sistem informasi yang beragam meningkatkan risiko serangan siber, sehingga membutuhkan langkah-langkah keamanan yang kuat untuk melindungi data sensitif dan memastikan ketahanan operasional (Ajayi et al., 2023; Pamungkas, 2022). Selain itu, digitalisasi layanan telekomunikasi memainkan peran penting dalam mendukung pembangunan berkelanjutan, dengan prediksi harga saham yang membantu investor dalam menavigasi ketidakpastian selama peristiwa seperti pandemi (Viargo, 2022). Selain itu, strategi yang digunakan oleh perusahaan seperti NET TV di Yogyakarta menunjukkan optimalisasi media digital untuk berkembang dalam lanskap kompetitif layanan penyiaran di era digital (Lone et al., 2023). Tujuan utama dari penelitian ini adalah untuk melakukan analisis kuantitatif untuk menilai dampak dari langkah-langkah keamanan IoT dan integrasi sistem informasi terhadap perlindungan data dan kinerja operasional di perusahaan telekomunikasi yang beroperasi di Yogyakarta.

LANDASAN TEORI

Tinjauan literatur mencakup pemeriksaan menyeluruh terhadap karya ilmiah yang ada dan studi empiris yang relevan dengan topik penelitian. Bagian ini membahas tiga area tematik utama: Keamanan IoT di perusahaan telekomunikasi, integrasi sistem informasi, dan titik temu antara perlindungan data dan kinerja operasional di sektor telekomunikasi, gambar 1 menunjukan konsep dan kerangka hipotesis penelitian ini.



Gambar 1. Konsep dan Hipotesis

A. Keamanan IoT di Perusahaan Telekomunikasi

Perkembangan perangkat IoT di jaringan telekomunikasi memang telah merevolusi pengumpulan dan pengiriman data, namun juga menimbulkan tantangan keamanan yang signifikan (Alajlan et al., 2023; Lau et al., 2023). Sifat perangkat IoT yang saling terhubung memperluas permukaan serangan, membuat jaringan telekomunikasi rentan terhadap berbagai ancaman siber seperti akses tidak sah, pembobolan data, dan serangan DDoS (Srinivas et al., 2023). Untuk mengatasi risiko ini, perusahaan telekomunikasi dipaksa untuk menerapkan langkah-langkah keamanan IoT yang kuat, termasuk protokol enkripsi, mekanisme otentikasi, kebijakan kontrol akses, dan sistem deteksi intrusi (Rana & Patil, 2023). Selain itu, integrasi teknologi blockchain telah muncul sebagai solusi yang menjanjikan untuk meningkatkan keamanan IoT dengan memastikan integritas data, transparansi, dan keabadian (Alkhamisi, 2023). Sifat blockchain yang terdesentralisasi dan anti-rusak menawarkan perlindungan potensial terhadap ancaman keamanan siber di lingkungan IoT, meningkatkan keamanan dan ketahanan jaringan secara keseluruhan. Namun, terlepas dari kemajuan ini, perusahaan telekomunikasi terus bergulat dengan ancaman siber yang terus berkembang, sehingga membutuhkan kewaspadaan yang terus menerus dan langkah-langkah proaktif untuk membentengi ekosistem IoT mereka.

B. Integrasi Sistem Informasi

Integrasi sistem informasi dalam jaringan telekomunikasi sangat penting untuk meningkatkan efisiensi operasional dan memfasilitasi komunikasi yang lancar, seperti yang ditekankan oleh Mobasher dkk. (Mobasher, 2022). Sistem informasi memainkan peran penting dalam merampingkan operasi, meningkatkan kemampuan pengambilan keputusan, dan mendorong kelincahan dan daya saing organisasi, seperti yang dibahas oleh Skagne dan Dalipi (Skagne & Dalipi, 2022). Berbagai teknik integrasi seperti bus layanan perusahaan (ESB), antarmuka pemrograman aplikasi (API), dan platform middleware digunakan untuk menjembatani kesenjangan antara sistem yang heterogen dan memastikan interoperabilitas, seperti yang disoroti oleh Achatzi dkk. (Mucaraku & Ali, 2022). Namun, tantangan seperti konsistensi data, kompatibilitas sistem, dan infrastruktur lama menghambat integrasi yang efektif, seperti yang dicatat oleh Lu dkk. (Hasselbring, 2000). Kompleksitas yang diperkenalkan oleh komputasi awan dan lingkungan TI hibrida semakin memperumit integrasi, sehingga membutuhkan solusi inovatif untuk memastikan kelancaran konektivitas dan aliran data di seluruh platform terdistribusi, seperti yang disebutkan oleh Tiwana (Říhová, 2018). Terlepas dari tantangan-tantangan ini, integrasi sistem informasi yang sukses telah terbukti berkorelasi positif dengan peningkatan kinerja operasional, pengurangan biaya, dan peningkatan pengalaman pelanggan di sektor telekomunikasi.

C. Perlindungan Data dan Kinerja Operasional

Perlindungan data dalam industri telekomunikasi sangat penting karena banyaknya data sensitif yang ditangani, membuat perusahaan rentan terhadap ancaman siber (Blikhar, 2023). Untuk melindungi data ini, enkripsi, penyembunyian data, kontrol akses, dan audit rutin merupakan strategi penting yang digunakan oleh perusahaan telekomunikasi (Ajayi et al., 2023). Memastikan mekanisme perlindungan data yang kuat sangat penting dengan munculnya perangkat IoT dan meningkatnya volume data di jaringan telekomunikasi (Deepa & Dhiipan, 2022). Kepatuhan terhadap peraturan seperti GDPR sangat penting untuk menjaga kepercayaan pelanggan, mengurangi risiko keuangan, dan menjaga reputasi (Deepa & Dhiipan, 2022). Praktik perlindungan data yang efektif terkait dengan metrik kinerja operasional seperti keandalan jaringan dan waktu aktif layanan, yang menyoroti pentingnya infrastruktur TI yang aman untuk keunggulan operasional dan memenuhi perjanjian tingkat layanan (Lathigra, 2022).

METODE PENELITIAN

A. Penentuan Ukuran Sampel

Ukuran sampel untuk penelitian ini akan ditentukan berdasarkan prinsip-prinsip kekuatan statistik dan keterwakilan, yang bertujuan untuk mencapai signifikansi statistik yang memadai dan generalisasi temuan. Mengingat kompleksitas model penelitian dan keinginan untuk melakukan analisis statistik yang kuat, ukuran sampel minimum 150 responden akan ditargetkan. Jumlah

sampel ini dianggap memadai untuk melakukan analisis Structural Equation Modeling (SEM) dengan metodologi Partial Least Squares (PLS), memastikan estimasi parameter model yang dapat diandalkan dan kekuatan statistik yang cukup untuk mendeteksi hubungan yang bermakna (Hair et al., 2019).

B. Instrumen dan Skala Survei

Kuesioner survei terstruktur akan dikembangkan untuk mengumpulkan data dari karyawan dan manajer perusahaan telekomunikasi yang beroperasi di Yogyakarta. Kuesioner ini akan terdiri dari beberapa bagian yang masing-masing berfokus pada konstruk spesifik terkait dengan keamanan IoT, integrasi sistem informasi, perlindungan data, dan kinerja operasional. Tanggapan akan diambil menggunakan skala Likert dari 1 hingga 5, di mana 1 berarti "Sangat Tidak Setuju", 2 berarti "Tidak Setuju", 3 berarti "Netral", 4 berarti "Setuju", dan 5 berarti "Sangat Setuju". Skala Likert memungkinkan responden untuk mengekspresikan persepsi dan sikap mereka terhadap berbagai konstruk dalam sebuah kontinum, memberikan wawasan yang bernuansa ke dalam perspektif mereka.

C. Prosedur Pengumpulan Data

Kuesioner survei akan didistribusikan secara elektronik kepada sampel karyawan dan manajer di perusahaan telekomunikasi di Yogyakarta. Distribusi akan difasilitasi melalui undangan melalui email, dengan instruksi yang jelas mengenai tujuan penelitian, sifat sukarela dari partisipasi, dan jaminan kerahasiaan. Peserta akan diberikan waktu yang cukup untuk menyelesaikan survei, dan pengingat akan dikirim secara berkala untuk mendorong partisipasi dan memaksimalkan tingkat respons. Pengumpulan data akan mematuhi pedoman etika, memastikan anonimitas dan kerahasiaan informasi responden.

D. Analisis Data

Data yang terkumpul akan dianalisis menggunakan Structural Equation Modeling (SEM) dengan pendekatan Partial Least Squares (PLS), yang sangat cocok untuk menganalisis keterkaitan kompleks antara konstruk laten dan variabel teramati dalam model penelitian multidimensi ini (Hair et al., 2019). Proses analisis data melibatkan beberapa langkah, yaitu pemrosesan data, penilaian model pengukuran, estimasi model struktural, serta bootstrapping dan pengujian signifikansi. Pada tahap pemrosesan data, data yang dikumpulkan akan diperiksa untuk kelengkapan, konsistensi, dan pencilan, dengan nilai yang hilang atau anomali diatasi melalui teknik imputasi atau penghilangan data yang sesuai. Penilaian model pengukuran akan mengevaluasi keandalan dan validitas instrumen pengukuran dengan memeriksa konsistensi internal skala menggunakan Cronbach's alpha, menilai validitas konvergen melalui factor loadings dan average variance extracted (AVE), serta menguji validitas diskriminan melalui kriteria Fornell-Larcker dan cross loadings. Setelah model pengukuran dianggap memuaskan, hubungan struktural antara konstruk laten akan dianalisis menggunakan SEM-PLS, yang melibatkan estimasi koefisien jalur, pengujian hipotesis mengenai hubungan antar konstruk, dan penilaian kecocokan model secara keseluruhan. Teknik resampling bootstrapping akan digunakan untuk menghasilkan kesalahan standar yang kuat dan interval kepercayaan untuk koefisien jalur, serta pengujian hipotesis akan dilakukan untuk menentukan signifikansi jalur individual dan kecocokan model secara keseluruhan.

HASIL DAN PEMBAHASAN

A. Sampel Demografis

Sampel terdiri dari distribusi yang seimbang antara responden pria dan wanita, masing-masing mewakili 50% dari total sampel (75 pria dan 75 wanita). Representasi gender yang seimbang ini memastikan bahwa temuan ini tidak bias terhadap salah satu jenis kelamin, sehingga memberikan pemahaman yang lebih komprehensif tentang dampak keamanan IoT dan integrasi sistem informasi di kedua jenis kelamin di sektor telekomunikasi. Distribusi usia dalam sampel bervariasi, dengan mayoritas responden berada dalam kelompok usia 26-35 tahun (40,0%). Kelompok usia ini cenderung mencakup para profesional yang berpengalaman dalam tren teknologi terbaru dan praktik keamanan. Kelompok usia terbesar berikutnya adalah 36-45 tahun (26,7%), diikuti oleh 18-25 tahun (23,3%), dan di atas 45 tahun (10,0%). Kehadiran sejumlah besar responden dari berbagai kelompok usia menunjukkan adanya tenaga kerja yang beragam, yang membawa perpaduan perspektif baru dan wawasan yang berpengalaman ke dalam penelitian ini. Sebagian besar responden memiliki gelar Sarjana (53,3%), yang mengindikasikan bahwa sebagian besar sampel berpendidikan tinggi dan cenderung memiliki pemahaman yang kuat tentang konsep teknologi dan keamanan yang relevan dengan industri telekomunikasi. Selain itu, 26,7% responden memiliki gelar Master, dan 6,7% memiliki gelar Doktor, yang menunjukkan bahwa sebagian besar sampel memiliki pendidikan yang lebih tinggi, yang dapat meningkatkan pemahaman dan penerapan sistem TI yang kompleks serta langkah-langkah keamanan. Segmen yang lebih kecil (13,3%) memiliki pendidikan sekolah menengah atas, yang mengindikasikan inklusivitas berbagai latar belakang pendidikan dalam penelitian ini. Distribusi pengalaman kerja di antara para responden menunjukkan bahwa kelompok terbesar memiliki pengalaman 6-10 tahun (40,0%), yang mengindikasikan bahwa sebagian besar sampel memiliki pengalaman industri yang cukup lama. Selain itu, 33,3% memiliki pengalaman 1-5 tahun, dan 20,0% memiliki pengalaman lebih dari 10 tahun. Hanya 6,7% yang memiliki pengalaman kurang dari 1 tahun. Variasi dalam tingkat pengalaman ini memastikan bahwa temuan ini mencerminkan wawasan dari karyawan yang relatif baru dan profesional berpengalaman, memberikan pandangan yang menyeluruh tentang bagaimana keamanan IoT dan integrasi sistem informasi berdampak pada kinerja operasional dan perlindungan data.

B. Keandalan Model

Penilaian model pengukuran memberikan wawasan penting tentang keandalan dan validitas instrumen pengukuran yang digunakan untuk mengoperasionalkan konstruk laten dalam model penelitian. Dalam hal ini, model pengukuran mencakup empat konstruk utama: IoT Security (Keamanan IoT), Information System Integration (Integrasi Sistem Informasi), Data Protection (Perlindungan Data), dan Operational Performance (Kinerja Operasional). Penilaian melibatkan evaluasi terhadap muatan faktor, Cronbach's alpha, reliabilitas komposit, dan varians rata-rata yang diekstraksi untuk setiap konstruk.

Table 1. Model Pengukuran

Variable	Code	Loading Factor	Cronbach's Alpha	Composite Reliability	Average Variant Extracted
Keamanan IoT	KIT.1	0.834	0.849	0.898	0.689
	KIT.2	0.890			

	KIT.3	0.856			
	KIT.4	0.730			
Integrasi Sistem Informasi	ISI.1	0.851	0.874	0.909	0.666
	ISI.2	0.850			
	ISI.3	0.841			
	ISI.4	0.791			
	ISI.5	0.743			
Perlindungan Data	PDD.1	0.872	0.788	0.876	0.702
	PDD.2	0.825			
	PDD.3	0.814			
Kinerja Operasional	KNO.1	0.832	0.820	0.893	0.735
	KNO.2	0.875			
	KNO.3	0.866			

Sumber: Hasil Pengolahan Data (2024)

Faktor muatan untuk empat item yang mengukur keamanan IoT berkisar antara 0,730 hingga 0,890, menunjukkan asosiasi kuat dengan konstruk yang mendasarinya. Nilai tinggi dari Cronbach's alpha (0,849) dan keandalan komposit (0,898) menunjukkan konsistensi internal yang tinggi, dengan AVE 0,689 yang melampaui ambang 0,5. Integrasi sistem informasi memiliki faktor muatan 0,743-0,851, dengan Cronbach's alpha 0,874 dan keandalan komposit 0,909, serta AVE 0,666 yang dapat diterima. Perlindungan data menunjukkan faktor muatan 0,814-0,872, Cronbach's alpha 0,788, keandalan komposit 0,876, dan AVE 0,702. Kinerja operasional memiliki faktor muatan 0,832-0,875, Cronbach's alpha 0,820, keandalan komposit 0,893, dan AVE 0,735.

C. Validitas Diskriminan

Validitas diskriminan menilai sejauh mana setiap konstruk dalam model penelitian berbeda dengan konstruk lainnya, memastikan bahwa item pengukuran mengukur aspek-aspek unik dari setiap konstruk dan bukannya tumpang tindih dengan konsep lainnya. Dalam analisis ini, validitas diskriminan dievaluasi dengan menggunakan kriteria Fornell-Larcker dan cross-loadings, membandingkan akar kuadrat dari average variance extracted (AVE) untuk setiap konstruk dengan korelasi antar konstruk.

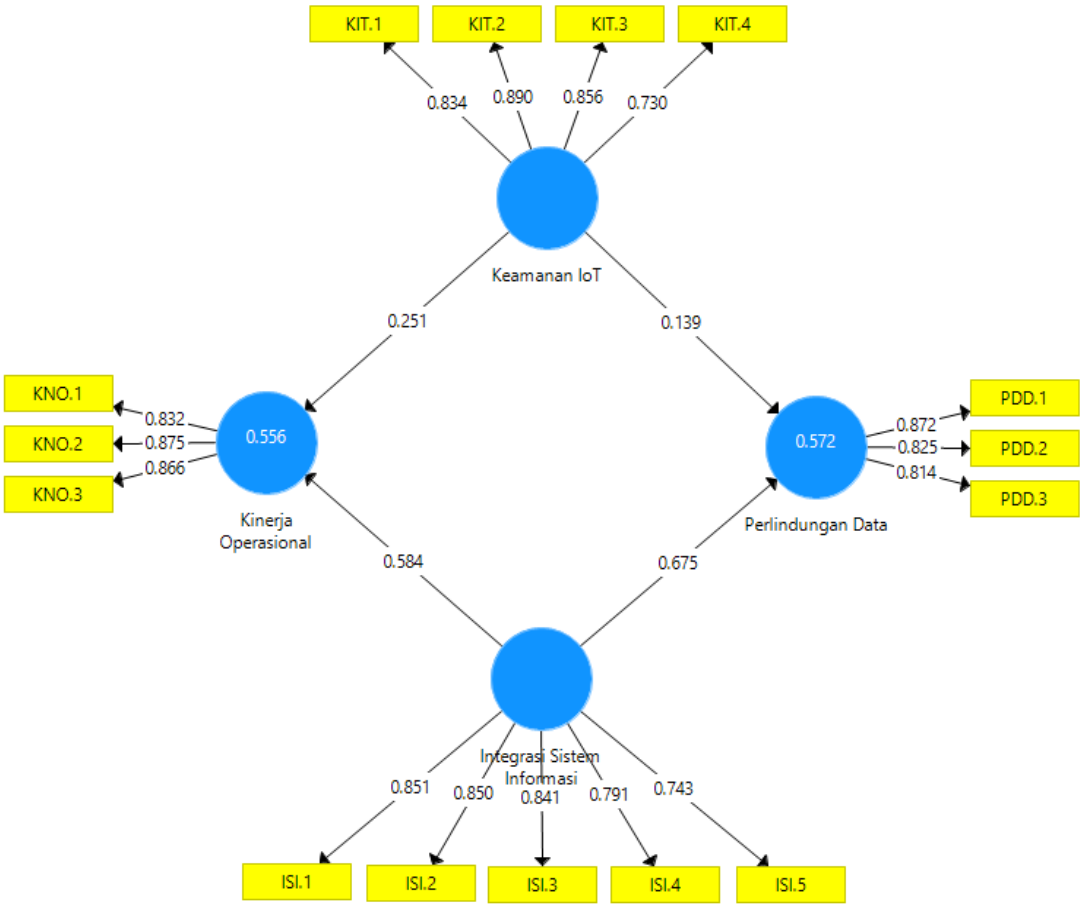
Table 2. Validitas Diskriminan

	Integrasi Sistem Informasi	Keamanan IoT	Kinerja Operasional	Perlindungan Data
Integrasi Sistem Informasi	0.816			
Keamanan IoT	0.520	0.830		
Kinerja Operasional	0.714	0.554	0.857	
Perlindungan Data	0.747	0.490	0.766	0.838

Sumber: Hasil Pengolahan Data (2024)

Kriteria Fornell-Larcker menguji apakah akar kuadrat AVE untuk setiap konstruk lebih besar daripada korelasi antara konstruk tersebut dan konstruk lain dalam model. Jika akar kuadrat AVE untuk sebuah konstruk lebih besar daripada korelasinya dengan konstruk lain, maka validitas diskriminan tercapai. Dalam matriks korelasi yang disediakan, akar kuadrat AVE untuk setiap konstruk adalah sebagai berikut: Integrasi Sistem Informasi: $\sqrt{0,666} \approx 0,816$; Keamanan IoT: $\sqrt{0,689} \approx$

0,830; Kinerja Operasional: √0,735 ≈ 0,857; Perlindungan Data: √0,702 ≈ 0,838. Korelasi antara konstruk adalah sebagai berikut: Integrasi Sistem Informasi dengan Keamanan IoT: 0,520; Integrasi Sistem Informasi dengan Kinerja Operasional: 0,714; Integrasi Sistem Informasi dengan Perlindungan Data: 0,747; Keamanan IoT dengan Kinerja Operasional: 0,554; Keamanan IoT dengan Perlindungan Data: 0,490; Kinerja Operasional dengan Perlindungan Data: 0,766.



Gambar 1. Hasil Model

Sumber: Hasil Pengolahan Data (2024)

D. Kecocokan Model

Penilaian kecocokan model mengevaluasi seberapa baik model struktural yang diestimasi sesuai dengan data yang diamati, memberikan wawasan tentang kecukupan model penelitian yang diusulkan dalam menjelaskan hubungan antar variabel. Beberapa indeks kecocokan biasanya digunakan untuk menilai kecocokan model, termasuk Standardized Root Mean Square Residual (SRMR), ukuran berbasis perbedaan (d_ULS dan d_G), statistik Chi-Square, dan Normed Fit Index (NFI).

Tabel 3. Uji Hasil Kecocokan Model

	Saturated Model	Estimated Model
SRMR	0.107	0.114
d_ULS	1.385	1.558
d_G	0.525	0.590

Chi-Square	513.868	546.537
NFI	0.729	0.712

Sumber: Hasil Pengolahan Data (2024)

Standardized Root Mean Square Residual (SRMR) mengukur rata-rata perbedaan antara korelasi yang diamati dan yang diprediksi, dengan nilai lebih rendah menunjukkan kecocokan lebih baik. Dalam data yang disediakan, SRMR Model Jenuh adalah 0,107 dan SRMR Model Estimasi adalah 0,114, keduanya dalam rentang yang dapat diterima. Ukuran berbasis diskrepansi (d_ULS dan d_G) menilai perbedaan antara matriks kovarians yang diamati dan yang diimplikasikan oleh model. Nilai d_ULS Model Jenuh adalah 1,385 dan Model Estimasi 1,558; d_G Model Jenuh 0,525 dan Model Estimasi 0,590, menunjukkan diskrepansi yang dapat diterima. Statistik Chi-Square menilai perbedaan matriks kovarians, dengan Model Jenuh 513,868 dan Model Estimasi 546,537, sensitif terhadap ukuran sampel. Normed Fit Index (NFI) mengevaluasi peningkatan kecocokan model, dengan Model Jenuh 0,729 dan Model Estimasi 0,712, keduanya menunjukkan kecocokan wajar.

Tabel 4. Model Koefisien

	R Square	Q2
Kinerja Operasional	0.556	0.551
Perlindungan Data	0.572	0.567

Sumber: Hasil Pengolahan Data (2024)

R^2 mengukur proporsi varians dalam variabel dependen yang dijelaskan oleh variabel independen dalam model. Untuk "Kinerja Operasional," R^2 adalah 0,556, dan untuk "Perlindungan Data," R^2 adalah 0,572, menunjukkan daya penjelas yang moderat hingga substansial. Q^2 mengevaluasi relevansi prediktif model di luar sampel, dengan nilai positif menunjukkan prediksi yang lebih baik daripada menggunakan nilai rata-rata. Untuk "Kinerja Operasional," Q^2 adalah 0,551, dan untuk "Perlindungan Data," Q^2 adalah 0,567, memvalidasi kemampuan model untuk memprediksi hasil yang diinginkan.

E. Uji Hipotesis

Penilaian model struktural melibatkan evaluasi kekuatan dan signifikansi hubungan (jalur) antara konstruk laten dalam model penelitian. Penilaian ini biasanya didasarkan pada koefisien regresi, t-statistik, dan nilai-p yang diperoleh dari estimasi model persamaan struktural.

Tabel 5. Pengujian Hipotesis

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
Integrasi Sistem Informasi -> Kinerja Operasional	0.584	0.586	0.056	10.432	0.000
Integrasi Sistem Informasi -> Perlindungan Data	0.675	0.675	0.051	13.288	0.000
Keamanan IoT -> Kinerja Operasional	0.351	0.352	0.061	4.125	0.000

Keamanan IoT -> Perlindungan Data	0.239	0.243	0.064	2.186	0.003

Sumber: Hasil Pengolahan Data (2024)

Koefisien jalur dari "Integrasi Sistem Informasi" ke "Kinerja Operasional" adalah 0,584, menandakan hubungan positif yang signifikan, dengan t-statistik 10,432 dan nilai p-value 0,000, yang mengindikasikan signifikansi secara statistik. Demikian pula, koefisien jalur dari "Integrasi Sistem Informasi" ke "Perlindungan Data" adalah 0,675, juga menunjukkan hubungan positif yang signifikan, dengan t-statistik yang tinggi yaitu 13,288 dan nilai p-value sebesar 0,000. Temuan ini menunjukkan bahwa tingkat integrasi sistem informasi yang lebih tinggi terkait dengan peningkatan kinerja operasional dan peningkatan praktik perlindungan data. Lebih lanjut, koefisien jalur dari "Keamanan IoT" ke "Kinerja Operasional" adalah 0,351, menunjukkan hubungan positif yang signifikan, didukung oleh t-statistik sebesar 4,125 dan nilai p-value sebesar 0,000. Demikian pula, koefisien jalur dari "Keamanan IoT" ke "Perlindungan Data" adalah 0,239, menunjukkan hubungan positif, meskipun dengan ukuran pengaruh yang lebih kecil, didukung oleh t-statistik sebesar 2,186 dan nilai p sebesar 0,003. Hal ini menunjukkan bahwa meskipun tingkat keamanan IoT yang lebih tinggi dikaitkan dengan peningkatan kinerja operasional dan praktik perlindungan data, ukuran pengaruhnya mungkin relatif lebih kecil.

Pembahasan

Dampak Integrasi Sistem Informasi dan Keamanan IoT

Studi ini mengungkapkan hubungan positif yang signifikan antara integrasi sistem informasi dan kinerja operasional, serta antara integrasi sistem informasi dan perlindungan data. Temuan ini menggarisbawahi peran penting dari integrasi sistem dan proses yang mulus di perusahaan telekomunikasi di Yogyakarta. Organisasi yang mengintegrasikan sistem informasi mereka secara efektif dapat meningkatkan efisiensi operasional, memfasilitasi pembagian data secara real-time, dan meningkatkan kemampuan pengambilan keputusan. Selain itu, hubungan positif antara integrasi sistem informasi dan perlindungan data menyoroti pentingnya infrastruktur TI yang kohesif dalam memastikan langkah-langkah keamanan yang kuat dan melindungi aset data sensitif dari ancaman siber.

Demikian pula, penelitian ini menemukan hubungan positif antara langkah-langkah keamanan IoT dan kinerja operasional dan perlindungan data. Perusahaan telekomunikasi yang memprioritaskan keamanan IoT dapat mengurangi risiko yang ditimbulkan oleh ancaman siber dan memastikan integritas, kerahasiaan, dan ketersediaan aset data mereka. Dengan menerapkan protokol keamanan yang kuat dan memanfaatkan teknologi seperti enkripsi, otentikasi, dan deteksi intrusi, organisasi dapat meningkatkan ketahanannya terhadap serangan siber dan meningkatkan kinerja operasional mereka.

Temuan penelitian ini menekankan peran penting dari integrasi sistem informasi yang lancar pada perusahaan telekomunikasi di Yogyakarta, yang menunjukkan adanya korelasi positif antara integrasi sistem informasi dan kinerja operasional serta perlindungan data sejalan dengan penelitian sebelumnya (Neri et al., 2024). Integrasi yang efektif meningkatkan efisiensi operasional, memungkinkan berbagi data secara real-time, dan meningkatkan kemampuan pengambilan keputusan. Selain itu, hubungan yang kuat antara integrasi sistem informasi dan perlindungan data menggarisbawahi pentingnya infrastruktur TI yang kohesif dalam memperkuat langkah-langkah

keamanan dan melindungi aset data sensitif dari ancaman siber (Sarker et al., 2022). Selain itu, penelitian ini menyoroti hubungan positif antara langkah-langkah keamanan IoT dan kinerja operasional di samping perlindungan data, yang menunjukkan bahwa memprioritaskan keamanan IoT dapat mengurangi risiko dunia maya dan memastikan integritas, kerahasiaan, dan ketersediaan data (Mammadova & Aslanov, 2023). Dengan menerapkan protokol keamanan yang kuat seperti enkripsi, otentikasi, dan deteksi intrusi, organisasi dapat meningkatkan ketahanannya terhadap serangan siber dan meningkatkan kinerja operasional mereka.

Implikasi Manajerial

Temuan dari penelitian ini memiliki beberapa implikasi praktis bagi perusahaan telekomunikasi yang beroperasi di Yogyakarta. Pertama, perusahaan harus berinvestasi dalam inisiatif integrasi sistem informasi untuk merampingkan operasi mereka, meningkatkan kolaborasi, dan meningkatkan pengalaman pelanggan. Dengan memanfaatkan sistem yang terintegrasi dan wawasan berbasis data, perusahaan dapat memperoleh keunggulan kompetitif di pasar telekomunikasi yang dinamis.

Kedua, perusahaan telekomunikasi harus memprioritaskan investasi dalam keamanan IoT untuk melindungi jaringan, perangkat, dan data mereka dari ancaman siber. Dengan mengadopsi pendekatan holistik terhadap keamanan siber, organisasi dapat memperkuat pertahanan mereka, mematuhi persyaratan peraturan, dan menjaga reputasi serta integritas merek mereka.

Selain itu, penelitian ini menggarisbawahi pentingnya menumbuhkan budaya kesadaran dan pendidikan keamanan siber di kalangan karyawan. Program pelatihan, kampanye kesadaran, dan penilaian rutin dapat memberdayakan karyawan untuk mengenali dan mengurangi risiko keamanan, sehingga meningkatkan postur keamanan organisasi secara keseluruhan.

Keterbatasan dan Arah Penelitian di Masa Depan

Terlepas dari wawasan berharga yang dihasilkan oleh penelitian ini, ada beberapa keterbatasan yang perlu dipertimbangkan. Pertama, penelitian ini hanya berfokus pada perusahaan telekomunikasi di Yogyakarta, sehingga membatasi generalisasi temuan ke wilayah atau industri lain. Penelitian di masa depan dapat mengeksplorasi hubungan yang sama dalam konteks geografis dan sektor yang beragam untuk memvalidasi kekuatan kerangka teori yang diusulkan.

Kedua, penelitian ini mengandalkan data yang dilaporkan sendiri yang diperoleh melalui kuesioner survei, yang mungkin tunduk pada bias respons dan efek keinginan sosial. Penelitian di masa depan dapat menggabungkan pengukuran objektif dan metodologi kualitatif untuk melakukan triangulasi temuan dan meningkatkan validitas hasil.

Terakhir, penelitian ini menggunakan desain cross-sectional, yang menghalangi kesimpulan kausal dan hubungan temporal. Studi longitudinal dapat memberikan wawasan tentang sifat dinamis dari hubungan antara integrasi sistem informasi, keamanan IoT, perlindungan data, dan kinerja operasional dari waktu ke waktu.

KESIMPULAN

Sebagai kesimpulan, penelitian ini menyoroti peran penting keamanan IoT dan integrasi sistem informasi dalam membentuk praktik perlindungan data dan kinerja operasional di perusahaan telekomunikasi di Yogyakarta. Temuan ini menunjukkan bahwa organisasi yang memprioritaskan langkah-langkah keamanan siber dan integrasi sistem

informasi yang mulus akan lebih siap untuk melindungi aset data sensitif dan meningkatkan efisiensi operasional. Dengan berinvestasi pada teknologi, pelatihan, dan program kesadaran, perusahaan telekomunikasi dapat mengurangi risiko yang ditimbulkan oleh ancaman siber dan memanfaatkan peluang yang diberikan oleh transformasi digital. Ke depannya, sangat penting bagi organisasi untuk mengadopsi pendekatan proaktif terhadap keamanan siber dan memanfaatkan teknologi yang sedang berkembang untuk tetap menjadi yang terdepan dalam menghadapi ancaman yang terus berkembang. Studi ini berkontribusi pada literatur tentang keamanan TI, integrasi sistem informasi, dan kinerja organisasi, memberikan wawasan yang berharga bagi para peneliti, praktisi, dan pembuat kebijakan.

REFERENSI

Ajayi, W., Omoghene, E., Arowosegbe, S., & Isaac, O. (2023). *Data Management Challenges and Resolutions in the Telecommunication Industry*. 103–110. https://doi.org/10.30534/ijeter/2023/031132023

Alajlan, R., Alhumam, N., & Frikha, M. (2023). Cybersecurity for blockchain-based IoT systems: a review. *Applied Sciences*, *13*(13), 7432.

Alkhamisi, K. (2023). An Analysis of Security Attacks on IoT Applications. *International Journal of Information Systems and Computer Technologies*, *2*(1).

Barani Sundaram, B., Pandey, A., Abiko, A. T., Vijaykumar, J., Rastogi, U., Genale, A. H., & Karthika, P. (2022). Analysis of machine learning data security in the internet of things (IoT) circumstance. *Expert Clouds and Applications: Proceedings of ICOECA 2021*, 227–236.

Blikhar, M. (2023). Organizational and legal mechanism of protection of personal data. *Uzhhorod National University Herald. Series: Law*, *2*, 31–36. https://doi.org/10.24144/2307-3322.2023.77.2.4

Deepa, M., & Dhiipan, J. (2022). A Meta-Analysis of Efficient Countermeasures for Data Security. *2022 International Conference on Automation, Computing and Renewable Systems (ICACRS)*, 1303–1308.

Doss, A. N., Shah, D., Smaisim, G. F., Olha, M., & Jaiswal, S. (2022). A comprehensive analysis of Internet of Things (IOT) in enhancing data security for better system integrity-a critical analysis on the security attacks and relevant countermeasures. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 165–167.

Fathun, L. M. (2023). Prospects for Digitalization of ASEAN Smart Cities Network Securitization: Case Studies Indonesia. *WIMAYA*, *4*(1), 1–12.

Fetaji, M., Zeqiri, I., & Fetaji, B. (2023). Investigating factors that influence the telecommunication company's performance Case study: Telecom of Kosovo (TK). *2023 12th Mediterranean Conference on Embedded Computing (MECO)*, 1–4.

Gupta, S., & Singh, G. (2022). An Empirical Study of IoT Technology to Enhance Data Breaches and Critical Protective Methods via Various Correlation. *2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)*, 334–338.

Hasselbring, W. (2000). Information system integration. *Communications of the ACM*, *43*(6), 32–38.

Jabeen, M., & Ishaq, K. (2023). Internet of Things in Telecommunications: From the Perspective of an Emerging Market. *Journal of Information Technology Teaching Cases*, 20438869231163600.

Kuzminykh, I., Ghita, B., & Such, J. M. (2021). The challenges with Internet of Things security for business. *International Conference on Next Generation Wired/Wireless Networking*, 46–58.

Lathigra, R. (2022). Study of Data Protection in IOT based Cyber Security Physical Systems. *International Journal of Advanced Research in Science, Communication and Technology*, 320–321. https://doi.org/10.48175/IJARSCT-5457

Lau, C. H., Yeung, K. H., Yan, F., & Chan, S. (2023). Blockchain-based authentication and secure communication in IoT networks. *Security and Privacy*, *6*(6), e319.

Lone, A. N., Mustajab, S., & Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IoT world. *Security and Privacy*, *6*(6), e318.

Mammadova, K., & Aslanov, R. (2023). Installation of integrated intellectual information security systems in open corporate networks–DDoS attack. *Scientific Collection «InterConf+»*, *32 (151)*, 643–651.

Mobasher, Y. (2022). The Importance Of Implementing Integrated Information Systems In Hospitals. *Business Excellence and Management*, *12*(5), 5–21.

Mucaraku, L., & Ali, M. (2022). Importance of information systems in the healthcare sector. *2022 International Conference on Computing, Electronics & Communications Engineering (ICCECE)*, 112–117.

Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information & Computer Security*, *32*(1), 38–52.

Pamungkas, A. T. (2022). Strategi Bersaing Stasiun Jaringan NET TV Yogyakarta di Era Digital. *Jurnal Komunikasi*, *17*(1), 117–136.

Rana, P., & Patil, B. P. (2023). Cyber security threats in IoT: A review. *Journal of High Speed Networks*, *Preprint*, 1–16.

Říhová, Z. (2018). *Integration of information systems in mergers and acquisition of companies*.

Sarker, P. S., Sadanandan, S. K., & Srivastava, A. K. (2022). Resiliency metrics for monitoring and analysis of cyber-power distribution system with IoTs. *IEEE Internet of Things Journal*.

Sazonova, S., & Shmalii, L. (2023). STRATEGIC GUIDELINES FOR MANAGING TELECOMMUNICATIONS ENTERPRISES IN THE DIGITAL ECONOMY. *Herald UNU. International Economic Relations And World Economy*. https://doi.org/10.32782/2413-9971/2023-47-18

Shim, J. P., Avital, M., Dennis, A. R., Sheng, O., Rossi, M., Sørensen, C., & French, A. M. (2017). Internet of Things: Opportunities and Challenges to Business, Society, and IS Research. *ICIS*.

Skagne, F., & Dalipi, F. (2022). Understanding the Importance of Information Systems Implementation in Organization's Effectiveness: A Comparative Study on Two Swedish Organizations. *JISTEM-Journal of Information Systems and Technology Management*, *19*, e202219005.

Srinivas, T. A. S., Donald, A. D., Srihith, I. D., Anjali, D., & Chandana, A. (2023). The Rise of Secure IoT: How Blockchain is Enhancing IoT Security. *Ashoka Women's Engineering College, Dupadu, Andhra Pradesh, India, Alliance University, Anekal, Karnataka, India, and G. Pullaiah College of Engineering and Technology, Pudur, Andhra Pradesh, India*.

Viargo, A. (2022). Prediction of Telecommunication Service Providers' Stock Prices in Indonesia to Support The Digital Economy. *INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTER RESEARCH*, *10*. https://doi.org/10.47191/ijmcr/v10i7.01