CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 8, No. 2, November 2025, hlm. 160-169

Validasi Cybersecurity Scale (CS-S) pada Konteks Industri di Batam sebagai Langkah Awal Menuju Penilaian Kesiapan Adopsi Zero Trust Architecture

Eryc[1], Vincent Claudius Santoso[2], Indasari Deu[3]

[1,2,3] Sistem Informasi, Fakultas Ilmu Komputer, Universitas International Batam
Email: [1]eryc@uib.ac.id, [2]2231007.vincent@uib.edu, [3]indasari@uib.ac.id

Abstrak

Studi ini bertujuan untuk menguji keabsahan Cybersecurity Scale (CS-S) sebagai alat ukur kesiapan sumber daya manusia (SDM) dalam menerapkan Zero Trust Architecture (ZTA) di sektor industri Batam. Validasi ini dilakukan untuk mengevaluasi sejauh mana dimensi kemanusiaan—seperti kesadaran autentikasi, pengendalian akses, dan manajemen data—dapat berfungsi sebagai tiang utama dalam penilaian kesiapan ZTA yang lebih mendalam. Dengan menggunakan pendekatan kuantitatif, data diperoleh melalui survei yang melibatkan 391 responden dari berbagai tingkatan organisasi industri manufaktur dan logistik di Batam. Hasil Analisis Faktor Konfirmatori (CFA) menunjukkan bahwa model enam faktor CS-S (Kerahasiaan, Integritas, Ketersediaan, Kontrol/Kepemilikan, Keaslian, dan Manfaat) memiliki kecocokan yang sangat baik (CFI = 0.980; TLI = 0.977; RMSEA = 0.051) dan reliabilitas yang tinggi (Cronbach's Alpha 0.913–0.946). Temuan ini menunjukkan bahwa dimensi Authenticity dan Control/Possession memiliki kontribusi terbesar, menegaskan pentingnya kesadaran terhadap verifikasi identitas dan kepemilikan data sebagai dasar penerapan ZTA. Sementara itu, dimensi Confidentiality, Integrity, dan Availability merefleksikan kesiapan teknis yang baik di kalangan perusahaan Batam. Penelitian ini menegaskan bahwa kesiapan SDM adalah fondasi krusial dalam adopsi ZTA dan bahwa CS-S dapat berfungsi sebagai instrumen awal untuk menilai kesiapan keamanan siber nasional di era regulasi UU Perlindungan Data Pribadi.

Kata kunci: *zero trust architecture, cybersecurity scale, validasi instrumen, keamanan siber, kesiapan SDM, UU PDP*

Validation of the Cybersecurity Scale (CS-S) in the Industrial Context of Batam as an Initial Step Toward Assessing Zero Trust Architecture Adoption Readiness

Abstract

This study aims to validate the Cybersecurity Scale (CS-S) as a measurement instrument for assessing human resource (HR) readiness in adopting the Zero Trust Architecture (ZTA) within Batam's industrial context. The validation focuses on the human dimension—such as authentication awareness, access control, and data management—as a fundamental pillar in comprehensive ZTA readiness assessment. Using a quantitative approach, data were collected from 391 respondents representing multiple organizational levels in Batam's manufacturing and logistics sectors. Confirmatory Factor Analysis (CFA) confirmed that the six-factor CS-S model (Confidentiality, Integrity, Availability, Control/Possession, Authenticity, and Utility) demonstrated excellent model fit (CFI = 0.980; TLI = 0.977; RMSEA = 0.051) and strong reliability (Cronbach's Alpha 0.913–0.946). The findings revealed that Authenticity and Control/Possession had the highest factor loadings, emphasizing respondents' awareness of identity verification and data ownership—two critical components of ZTA's Identity and Access Management pillar. Meanwhile, Confidentiality, Integrity, and Availability reflected strong technical readiness among Batam-based firms. The study highlights that human readiness is a foundational element in successful ZTA adoption and that the validated CS-S serves as an essential tool for evaluating national cybersecurity readiness amid the enforcement of Indonesia's Personal Data Protection Law (PDP Law).

Keywords: *zero trust architecture, cybersecurity scale, instrument validation, cybersecurity, human readiness, personal data protection law*

CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 8, No. 2, November 2025, hlm. 161-169

1. PENDAHULUAN

Kemajuan teknologi digital mendorong organisasi di seluruh dunia untuk mengadopsi sistem informasi dalam hampir semua proses bisnis. Namun, peningkatan dalam transformasi digital juga disertai dengan peningkatan ancaman siber yang semakin rumit dan menuntut perusahaan untuk mengadopsi strategi teknologi informasi yang tepat (Jeffry et al. 2024). (Alexander et al. 2023) menekankan bahwa serangan modern tidak hanya menyasar sistem teknologi informasi (IT), tetapi juga teknologi operasional (OT) yang mendukung rantai pasokan industri. Ini menunjukkan bahwa serangan siber saat ini berpotensi mengganggu sektor manufaktur, logistik, dan layanan publik.

Secara keseluruhan, Indonesia merupakan salah satu negara dengan risiko ancaman siber yang tinggi. Laporan dari Badan Siber dan Sandi Negara (BSSN) mencatat jutaan serangan siber setiap tahunnya, termasuk kebocoran data pribadi yang dialami oleh instansi pemerintah maupun swasta. Kasus kebocoran data konsumen e-commerce, perbankan, dan layanan kesehatan menunjukkan bahwa sistem keamanan siber masih belum optimal.

Di level lokal, Batam sebagai pusat industri dan perdagangan global sangat bergantung pada infrastruktur digital. Perusahaan di Batam tidak hanya menangani data internal, tetapi juga terhubung dengan jaringan pasokan global. Kebocoran data atau serangan siber di Batam dapat menimbulkan dampak ekonomi yang besar, termasuk berkurangnya kepercayaan dari mitra internasional. Fenomena ini menunjukkan bahwa urgensi untuk mengadopsi arsitektur keamanan modern seperti Zero Trust Architecture (ZTA) semakin tinggi.

Batam dipilih karena karakteristik uniknya sebagai zona industri strategis dan pusat manufaktur ekspor terbesar di Indonesia dengan konektivitas langsung ke Singapura dan rantai pasok global. Wilayah ini menghadapi ancaman siber dominan berupa serangan phishing terhadap rantai pasok, pencurian data industri, serta upaya intrusi terhadap sistem kontrol produksi (OT). Faktor ini menjadikan Batam konteks ideal untuk menguji kesiapan sumber daya manusia dalam menghadapi risiko keamanan siber melalui pendekatan ZTA.

ZTA menekankan prinsip "tidak pernah percaya, selalu verifikasi", di mana setiap akses harus selalu dicek tanpa bergantung pada batasan jaringan konvensional. Studi (Corallo et al. 2023) dalam kerangka industri 4.0 menekankan bahwa perlindungan data mesti melibatkan IT dan OT, sehingga implementasi ZTA menjadi semakin penting untuk daerah industri seperti Batam.

Di samping itu, pemerintah Indonesia sudah menyetujui Undang-Undang Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi (UU PDP) yang memberikan dasar hukum terkait pengelolaan data pribadi. (Prastyanti et al. 2022) menunjukkan bahwa regulasi ini menciptakan tantangan besar bagi banyak organisasi karena tingkat kesiapan infrastruktur dan budaya keamanan siber yang masih rendah. Dengan UU PDP yang ada, perusahaan di Batam diwajibkan untuk tidak hanya melindungi data secara teknis, tetapi juga memastikan kepatuhan terhadap hukum.

Penelitian ini secara khusus berfokus pada validasi instrumen Cybersecurity Scale (CS-S) sebagai alat ukur untuk menilai dimensi kesiapan sumber daya manusia (SDM) terhadap penerapan Zero Trust Architecture (ZTA). Dimensi SDM dipandang sebagai pilar fundamental dalam asesmen kesiapan ZTA secara menyeluruh, karena keberhasilan implementasi arsitektur ini sangat bergantung pada kesadaran, perilaku, dan praktik keamanan dari individu dalam organisasi.

Dalam menilai kesiapan organisasi dalam menghadapi ancaman dan regulasi tersebut, studi ini mengaplikasikan Cybersecurity Scale (CS-S) yang dirancang oleh (Arpaci and Sevinc 2022). Alat ini terdiri dari enam dimensi utama: kerahasiaan, integritas, ketersediaan, kontrol/kepemilikan, keaslian, dan kegunaan. Walaupun alat ini telah diuji secara global, sampai saat ini belum pernah divalidasi dalam konteks Indonesia, terutama di Batam. Inilah celah penelitian yang ingin diungkap: bagaimana tingkat kesiapan perusahaan di Batam dalam menerapkan ZTA dapat dievaluasi menggunakan instrumen CS-S dalam konteks kepatuhan UU PDP.

1.1. Rumusan Masalah

Rumusan masalah dari penelitian ini adalah kombinasi dari rumusan masalah deskriptif dan analisis, berikut adalah rumusan yang diajukan dalam penelitian ini :

1. Apakah model enam faktor Cybersecurity Scale (CS-S) sesuai dengan data empiris perusahaan di Batam melalui analisis *Confirmatory Factor Analysis (CFA)*?
2. Bagaimana tingkat validitas dan reliabilitas instrumen CS-S dalam konteks perusahaan di Batam?
3. Apa dampak hasil pengukuran CS-S terhadap kesiapan penerapan Zero Trust Architecture (ZTA) di perusahaan Batam dalam konteks regulasi UU PDP

1.2. Tujuan Penelitian

Penelitian ini bertujuan untuk :

1. Menguji kesesuaian model enam faktor CS-S melalui *Confirmatory Factor Analysis* (CFA).
2. Menganalisis validitas dan reliabilitas instrumen CS-S dalam konteks perusahaan di Batam.

1.3. Manfaat Penelitian

a. Manfaat Teoritis

- Memberikan kontribusi pada literatur keamanan siber dengan menguji validitas CS-S di Indonesia.
- Menghubungkan teori CS-S dengan konsep ZTA dalam konteks regulasi UU PDP.

b. Manfaat Praktis

- Memberikan gambaran kesiapan perusahaan di Batam dalam mengadopsi ZTA.
- Menawarkan rekomendasi langkah konkret seperti penerapan *multi-factor authentication*, pelatihan kesadaran siber, audit kepatuhan UU PDP, dan penyusunan roadmap ZTA

c. Manfaat Kebijakan

- Menjadi masukan bagi regulator dalam menilai kesiapan industri di Batam terhadap UU PDP.
- Memberikan dasar empiris bagi pemerintah untuk menyusun kebijakan dan dukungan terhadap implementasi keamanan siber nasional.

2. TINJAUAN PUSTAKA

Dalam suatu penelitian diperlukan dukungan dari hasil-hasil penelitian yang telah ada sebelumnya yang berhubungan dengan penelitian tersebut.

2.1. Konsep Keamanan Siber

Keamanan siber adalah tindakan untuk melindungi sistem informasi, jaringan, dan data dari akses yang tidak diizinkan, modifikasi, serta kerusakan. (Cremer et al. 2022) menegaskan bahwa ZTA krusial di era industri 4.0 karena keterhubungan IT dan OT. Namun, penelitian tersebut belum mengaitkan kerangka ZTA dengan konteks regulasi lokal. Konsep Triad CIA (Kerahasiaan, Integritas, Ketersediaan) merupakan dasar klasik dalam keamanan informasi. Namun, di zaman digital yang ditandai dengan kerja remote, penerapan cloud, dan Internet of Things (IoT), ancaman semakin rumit dan memerlukan pendekatan keamanan yang lebih fleksibel.

2.2. Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) adalah model baru dalam keamanan siber yang menolak anggapan kepercayaan otomatis pada pengguna atau perangkat, baik yang berasal dari dalam maupun luar jaringan. Prinsip utamanya adalah "jangan pernah percaya, selalu verifikasi", dengan kontrol akses yang bergantung pada identitas, perangkat, dan konteks (Kerman et al. 2020). Studi (Corallo et al. 2023) dalam lingkungan industri 4.0 mengindikasikan bahwa keamanan berbasis ZTA menjadi krusial karena penggabungan IT dan OT menciptakan peluang serangan yang lebih besar.

Aspek kontrol data pribadi menjadi sangat penting mengingat regulasi UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penelitian (Eryc and Santoso 2024) menegaskan bahwa perlindungan data digital bukan hanya aspek teknis, tetapi juga berkaitan dengan kepatuhan hukum dan hak privasi individu.

Bagi perusahaan di Batam yang berfokus pada manufaktur dan perdagangan internasional, ZTA penting untuk menjamin keamanan rantai pasok digital. Akan tetapi, penerapan ZTA memerlukan kesiapan organisasi, mulai dari aspek teknologi, kebijakan, hingga budaya keamanan.

2.3. Regulasi Perlindungan Data Pribadi (UU PDP)

Pengesahan Undang-Undang Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi merupakan langkah krusial dalam regulasi keamanan siber di Indonesia. UU PDP mengatur tanggung jawab pengendali dan pengolah data, hak-hak subjek data, serta hukuman administratif dan pidana untuk pelanggaran. (Prastyanti et al. 2022) membawa tantangan kepatuhan di Indonesia, tetapi belum dihubungkan dengan kesiapan teknis organisasi.

Dalam konteks Batam, pemenuhan UU PDP sangat penting mengingat posisinya sebagai daerah industri yang terhubung dengan mitra internasional. Perusahaan dituntut bukan hanya untuk melindungi data internal, tetapi juga untuk menunjukkan tanggung jawab hukum dalam pengelolaan data pelanggan dan mitra bisnis.

2.4. Cybersecurity Scale (CS-S) dan Dimensinya

(Arpaci and Sevinc 2022) membuat Skala Keamanan Siber (CS-S) untuk mengukur bagaimana orang maupun organisasi melihat dan menerapkan keamanan siber. Instrumen ini memiliki enam dimensi utama, yaitu confidentiality, integrity, availability, control/possession, authenticity, dan utility. CS-S inilah yang akan menjadi alat pengukuran untuk melihat seberapa jauh kesiapan penerapan ZTA di Batam.

- **Confidentiality (kerahasiaan)** berfokus pada untuk melindungi informasi sensitif dari akses dan pengungkapan yang tidak sah (Abrahams et al. 2023).
- **Integrity (integritas)** menekankan konsistensi dan keakuratan data sepanjang siklus hidupnya. Sementara integritas sering dijaga dengan menggunakan checksum, hash functions, atau digital signatures, tetap rentan terhadap serangan seperti pelecehan racun dan serangan backdoor (Alexander et al. 2023).
- **Availability (ketersediaan)** memastikan data dan sistem dapat diakses pihak berwenang kapanpun dibutuhkan. Data tentang risiko siber masih terbatas, menurut penelitian (Cremer et al. 2022) meskipun elemen ketersediaan telah berkembang.
- **Control/Possession (kontrol/kepemilikan)** mewakili tingkat kontrol yang dimiliki seseorang atau organisasi atas data pribadi. (Pant et al. 2023) menekankan bahwa elemen ini sangat penting untuk peraturan

perlindungan data dan privasi terutama seiring meningkatnya digitalisasi seperti yang ditekankan juga oleh (Eryc et al. 2024).

- **Authenticity (keaslian)** memastikan bahwa individu yang mengakses sistem adalah yang benar. (Sasada et al. 2024) menunjukkan bahwa metode autentikasi tradisional masih memiliki kekurangan, terutama dalam hal pekerjaan yang dilakukan secara jarak jauh.
- **Utility (utilitas)** berhubungan dengan bagaimana data dapat digunakan untuk proses pengambilan keputusan. (Bartol et al., n.d.) memperingatkan bahwa memiliki lebih banyak perangkat terhubung meningkatkan kemungkinan serangan siber, meskipun data semakin digunakan secara strategis.

Dengan demikian, penelitian ini menempatkan diri sebagai studi validasi instrumen untuk mengukur kesiapan SDM sebagai salah satu pilar kunci asesmen kesiapan ZTA, bersama dengan pilar teknologi dan kebijakan organisasi.

2.5. Pemetaan Teoretis antara Dimensi CS-S dan Pilar ZTA

Setiap dimensi pada CS-S memiliki keterkaitan langsung dengan prinsip Zero Trust Architecture.

- **Confidentiality** → mendukung pilar *data protection* dalam ZTA.
- **Integrity** → berhubungan dengan *monitoring and validation* data serta proses autentikasi berlapis.
- **Availability** → selaras dengan pilar *resiliency and recovery* yang memastikan kelangsungan layanan.
- **Control/Possession** → mencerminkan pilar *identity and access management*, yakni kontrol penuh terhadap kepemilikan data dan akses pengguna.
- **Authenticity** → berperan penting dalam *verification and continuous authentication*, sesuai prinsip "never trust, always verify".
- **Utility** → menghubungkan aspek pemanfaatan data secara aman dalam *policy enforcement and visibility*.

2.6. Penelitian Terdahulu tentang Zero Trust Security Model

Penelitian lainnya oleh (Corallo et al. 2023) juga meneliti tentang keamanan siber tetapi dalam konteks industri 4.0 dalam sistem manufaktur dimana mereka menemukan bahwa keamanan siber dalam industri 4.0 tidak hanya mempengaruhi sistem teknologi informasi tetapi juga mencakup teknologi operasional. Penelitian ini menggunakan metodologi *business impact assessment* untuk menilai dampak potensial dari serangan siber terhadap sistem manufaktur yang saling terhubung. Hasil dari penelitian ini adalah berhasil dalam mengidentifikasi data-data kritis yang harus dilindungi dari serangan siber dalam sistem manufaktur berbasis teknologi subtractive dan additive. Adapun penelitian terdahulu lebih lanjut dapat dilihat pada Tabel 1

Tabel 1. Penelitian Terdahulu

Peneliti & Tahun	Konteks	Metode	Temuan Utama	Relevansi bagi Penelitian ini
Arpaci & Sevinc (2022)	Validasi CS-S (internasional)	EFA & CFA	CS-S valid, reliabel, enam faktor	Perlu diuji dalam konteks Batam
Corallo et al. (2023)	Industri 4.0, manufaktur	Business Impact Assessment	Keamanan siber memengaruhi IT & OT	Menunjukkan urgensi ZTA di industri
Cremer et al. (2022)	Manajemen risiko siber	Studi empiris	Ketersediaan data masih terbatas	Tantangan *availability* di Batam
Prastyanti et al. (2022)	Regulasi di Indonesia	Studi regulasi	UU PDP jadi tantangan besar	Relevansi regulasi di Batam

Mayoritas studi CS-S lebih menekankan pada konteks global. Validasi dalam konteks lokal Indonesia, terutama Batam yang memiliki posisi strategis dalam industri, belum diteliti. Situasi ini mengakibatkan adanya kesenjangan akademik dan praktis untuk penelitian ini.

2.7. Gap Penelitian

Berbagai penelitian internasional telah menunjukkan bahwa **Cybersecurity Scale (CS-S)** merupakan instrumen yang valid dan reliabel dalam mengukur persepsi serta praktik keamanan siber (Arpaci and Sevinc 2022). Studi lain, seperti (Corallo et al. 2023), menekankan bahwa strategi keamanan berbasis Zero Trust sangat penting untuk menghadapi risiko siber di era industri 4.0. Namun, penelitian ini sebagian besar dilakukan di luar Indonesia, sehingga tidak memperhitungkan elemen peraturan lokal. seperti UU PDP, dan keadaan infrastruktur digital yang siap di Indonesia.

Misalnya, penelitian lokal oleh (Prastyanti et al. 2022) berfokus pada elemen regulasi dan kesiapan organisasi untuk menanggapi UU PDP. Penelitian ini penting, tetapi belum menguji instrumen pengukuran kesiapan siber yang diakui secara internasional. Oleh karena itu, kurangnya penelitian pada domain empiris, terutama mengenai validasi CS-S di Indonesia.

Selain itu, meskipun Batam adalah wilayah industri strategis yang sangat bergantung pada infrastruktur digital, belum ada penelitian yang secara khusus menyelidiki kesiapan organisasi kota tersebut. Hal ini membuat penelitian tentang validitas dan reliabilitas CS-S di Batam sangat penting karena tidak hanya akan mengisi kekosongan akademis tetapi juga akan membantu

perusahaan mengikuti peraturan UU PDP dan Zero Trust Architecture.

Adapun Hipotesis pada penelitian ini adalah sebagai berikut :

- **H1:** Model enam faktor CS-S sesuai dengan data empiris perusahaan di Batam melalui CFA.
- **H2:** Instrumen CS-S memiliki validitas dan reliabilitas yang baik dalam konteks perusahaan di Batam.
- **H3:** Kesiapan perusahaan di Batam dalam mengadopsi ZTA dapat dijelaskan melalui hasil pengukuran CS-S dalam kerangka UU PDP, dengan prediksi teoritis bahwa dimensi non-teknis (kontrol data, autentikasi) menjadi faktor penentu keberhasilan penerapan ZTA.

3. METODE PENELITIAN

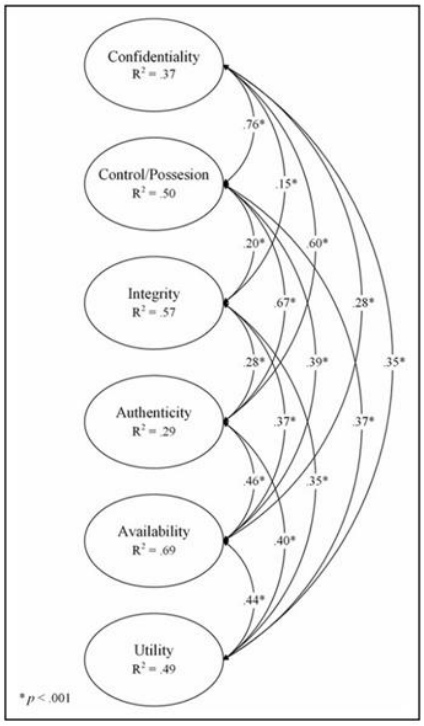
Penelitian ini adalah penelitian kuantitatif dengan pendekatan survei dan orang-orang yang telah bekerja di perusahaan-perusahaan Batam sebagai target penelitian ataupun respondennya, terutama di perusahaan yang menyimpan data-data penting ataupun data privasi seperti perusahaan jasa, manufaktur, dan lain sebagainya sebagai target penelitian ini. Penelitian ini akan mengevaluasi kesiapan dalam adopsi ZTA menggunakan metode yang telah dibahas sebelumnya. Penelitian ini bertujuan untuk menganalisis kesiapan dalam penerapan model keamanan Zero Trust di lingkungan kerja mereka, serta mengidentifikasi faktor-faktor yang mempengaruhi keberhasilan implementasi dalam konteks lokal. Penelitian ini akan menggunakan Google Form sebagai instrumen penelitian, dan di isi oleh sampel populasi dengan skala ordinal. Penggunaan Google Form pada survei kuantitatif ini dilakukan untuk kemudahan distribusi, adapun alur pada penelitian ini dapat dilihat pada gambar 1.

Gambar 1. Alur Penelitian

Sampel penelitian ini ditentukan menggunakan rumus Zikmund yang menentukan sampel populasi dengan jumlah populasi yang tidak pasti dimana menurut data dari Tingkat Partisipasi Angkatan Kerja (TPAK) Pada Agustus 2024 ada sekitar 150.630 pekerja di Batam, dengan tingkat kepercayaan 95% dan margin of error 5% maka perhitungan dari rumus tersebut didapatkan sebanyak 385 individu yang akan berpartisipasi dalam penelitian ini.

Metode Cluster Disproportional Stratified Sampling akan digunakan untuk analisis sampling, dimana sampel yang telah dikumpulkan akan diambil dan dibedakan menjadi tiga kelompok sebagai disproportional atau tidak sebanding, dan sampelnya akan diambil secara acak. Untuk kelompok disproportional nya dibagi sebagai berikut, dari golongan CEO, CTO, Direktur keamanan IT dan setingkatnya sebanyak 10 orang; golongan Manajer IT, Manajer Keamanan Informasi, Manajer Infrastruktur IT dan setingkatnya sebanyak 130 orang; dari golongan Spesialis Keamanan Siber, Staff IT, Administrator Jaringan, dan setingkatnya sebanyak 246 orang.

Metode Cluster Disproportional Stratified Sampling digunakan karena populasi penelitian terdiri dari berbagai level jabatan yang jumlahnya tidak seimbang, di mana kelompok eksekutif relatif lebih sedikit dibandingkan manajerial maupun staf teknis. Jika menggunakan *proportional sampling*, kelompok eksekutif hanya akan terwakili dalam jumlah yang sangat kecil sehingga kurang memadai untuk dianalisis. Dengan menggunakan *disproportional stratified sampling*, setiap strata memperoleh jumlah sampel yang cukup untuk dibandingkan, sementara pendekatan *cluster* memudahkan pengelompokan responden berdasarkan perusahaan. Pendekatan ini dipandang paling tepat untuk memastikan keterwakilan setiap level jabatan sekaligus mendukung tujuan penelitian dalam menganalisis perbedaan kesiapan penerapan *Zero Trust Architecture (ZTA)* di Batam.Adapun model pengukuran ini dapat dilihat pada gambar 2.



Gambar 2. Model Pengukuran

Model penelitian ini menggunakan pendekatan multi-tahap untuk mengembangkan dan memvalidasi Cybersecurity Scale (CS-S). Variabel penelitian ini adalah Confidentiality, Control/Possession, Integrity, Authenticity, Availability, dan Utility. Definisi operasional

variabel yang digunakan untuk mengembangkan instrumen penelitian ini akan ditunjukkan pada Tabel 3.1 Kuesioner akan disusun dengan skala ordinal 1-5 dari sangat tidak setuju hingga sangat setuju dan diuji validitas serta reliabilitasnya sebelum disebarkan. Pengujian reliabilitas akan menggunakan Cronbach's Alpha dengan nilai > 0,7 sebagai indikator instrumen penelitian telah reliabel. Faktor dan Indikator penelitian yang diadaptasi dari (Arpaci and Sevinc 2022), ini dapat dilihat pada Tabel 2

Tabel 2. Faktor dan Indikator Penelitian

Faktor	Indikator
Confidentiality	1. Saya berhati-hati dengan informasi pribadi yang saya bagikan di internet.
	2. Saya tidak membagikan informasi dan dokumen di internet yang tidak ingin saya bagikan dengan pihak ketiga dalam kehidupan nyata.
	3. Saya memastikan bahwa data yang saya bagikan di dunia maya hanya dapat dilihat oleh orang-orang yang memang membutuhkannya.
	4. Saya tidak keberatan membagikan informasi kontak saya di internet.
Control/Possession	5. Saya berhati-hati dengan keamanan kata sandi akun-akun saya.
	6. Saat membuat kata sandi, saya memilih kata sandi yang sulit ditebak terdiri dari simbol, angka, dan huruf kapital.
	7. Saya menggunakan layanan verifikasi telepon untuk keamanan kata sandi email saya.
	8. Saya memastikan untuk memilih pertanyaan keamanan dengan jawaban yang akan saya ingat.
	9. Saya memastikan informasi kartu kredit saya tidak disimpan.
Integrity	10. Saya merasa menyimpan data di dunia maya tidaklah aman.
	11. Informasi dan dokumen yang saya simpan di internet dapat hilang atau terhapus.
	12. Berbagi data di internet tidak melibatkan risiko apapun.
	13. Pihak ketiga mungkin dapat mengakses informasi dan dokumen yang disimpan di internet.
Authenticity	14. Saya membuka link dan lampiran dalam e-mail dari orang yang tidak saya kenal.
	15. Saya tetap mengakses web meskipun menerima pemberitahuan bahwa situs web yang saya masuki tidak memiliki sertifikat keamanan.
	16. Saya telah membuka email spam yang dikirim ke alamat email saya.
	17. Saya telah membuka email yang bertujuan untuk rekayasa sosial/phishing.
	18. Saya telah membuka tautan dan lampiran dari sumber yang tidak pasti.
Availability	19. Saya memiliki program antivirus yang terbaru di perangkat saya.
	20. Saya secara teratur memindai perangkat saya dengan program antivirus.
	21. Firewall yang terpasang di perangkat saya dalam keadaan menyala.
	22. Saya membuka file yang saya unduh dari internet meskipun saya tidak memiliki program antivirus yang terpasang di perangkat saya.
Utility	23. Saya menggunakan aplikasi media sosial untuk berbagi informasi di dunia maya.
	24. Saya secara luas menggunakan lingkungan cyber untuk memecahkan masalah yang saya temui dalam kehidupan sehari-hari.
	25. Saya menggunakan layanan yang disediakan di dunia maya untuk manajemen informasi (perolehan informasi, penyimpanan, berbagi, dan penerapan).

Penelitian ini dimulai dengan tinjauan pustaka dengan meninjau referensi-referensi yang berkaitan dengan topik penelitian. Referensi yang ditinjau dikumpulkan untuk memberikan solusi dan jawaban yang tepat terhadap permasalahan yang telah dibahas. Metode analisis yang digunakan dalam penelitian ini menggunakan aplikasi SPSS Statistics untuk melakukan uji validitas dan reliabilitas berdasarkan Cronbach's Alpha dan SPSS AMOS digunakan untuk melakukan analisis Confirmatory Factor Analysis (CFA).

4. HASIL & PEMBAHASAN

Survei ini mendapatkan data kuesioner sebanyak 630 responden, tetapi hanya 390 data responden yang valid dan akan dipakai untuk penelitian. Data dari survei ini diperoleh setelah responden mengisi 25 pertanyaan yang mewakili 6 variabel yaitu **Confidentiality** (C1–C4), **Control/Possession** (CP1–CP4), **Integrity** (I1–I4), **Authenticity** (A1–A5), **Availability** (AV1–AV5), dan **Utility** (U1–U3). Data yang diperoleh akan diuji test outlier dengan metode Z-Score dimana nilai dari Z-Score tidak boleh melebihi 3 dan kurang dari -3. Juga ditemukan ada delapan pertanyaan yang diidentifikasi sebagai reverse item dan telah dilakukan proses reverse coding sebelum dianalisis lebih lanjut. Setelah outlier dihilangkan dan dilakukan reverse coding barulah muncul 391 data yang dapat dipakai untuk penelitian ini, item yang telah di reverse adalah C4, 14, A1 sampai A5, dan AV5. Adapun data deskriptif tentang jabatan pekerjaan dari responden dapat dilihat pada tabel 3.

Tabel 3. Deskriptif Responden

Jabatan Pekerjaan	Frekuensi	Persentase
CEO, CTO, Direktur Keamanan IT,Jabatan Setingkat Eksekutif lainnya	11	2,8%
Manajer IT, Manajer Keamanan Informasi, Manajer Infrastruktur IT,Jabatan Setingkat Manajerial lainnya	131	33,6%
Spesialis Keamanan Cyber, Staff IT,Administrator Jaringan, Jabatan Teknis/Operasional Setingkat lainnya	248	63,6%

4.1. Uji Validitas

Berdasarkan uji validitas yang telah dilakukan terhadap semua instrumen pada masing-masing variabel dengan metode korelasi bivariate Pearson (Pearson Correlation). Hasil nya menunjukkan bahwa seluruh item dalam keenam variabel tersebut memiliki korelasi yang tinggi ($r = 0.884 – 0.937$; $p < 0.01$). Dengan demikian dapat dikatakan seluruh pertanyaan tersebut dinyatakan valid dan dapat dilihat pada Tabel 4.

Tabel 4 Hasil Uji Validitas Instrumen

Variabel	Item	Korelasi Item-Total	Keterangan
Confidentiality	C1-C4	r > 0.88	Valid
Control/Possession	CP1-CP4	r > 0.88	Valid
Integrity	I1-14	r > 0.88	Valid
Authenticity	A1-A5	r > 0.88	Valid
Availability	AV1-AV5	r > 0.88	Valid
Utility	U1-U3	r > 0.88	Valid

4.2. Uji Realibilitas

Reliabilitas diuji menggunakan Cronbach's Alpha pada masing-masing konstruk. Suatu konstruk dianggap reliabel apabila nilai $\alpha \geq 0.70$ seperti yang dapat dilihat pada tabel 5.

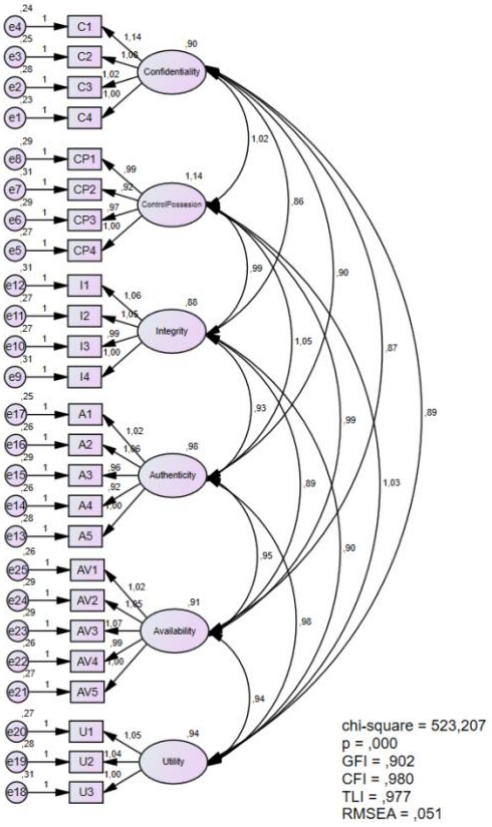
Tabel 5. Hasil Uji Reliabilitas Instrumen

Variabel	Jumlah Item	Cronbach's Alpha	Keterangan
Confidentiality	4	0.941	Reliabel
Control/Possession	4	0.936	Reliabel
Integrity	4	0.927	Reliabel
Authenticity	5	0.946	Reliabel
Availability	5	0.946	Reliabel
Utility	3	0.913	Reliabel

Berdasarkan hasil dari uji validitas dan reliabilitas, dapat dilihat bahwa seluruh konstruk pada instrumen penelitian ini memiliki konsistensi internal yang sangat baik. Tidak ada konstruk yang perlu diperbaiki atau item yang harus dibuang.

4.3. Confirmatory Factor Analysis (CFA)

Analisis CFA digunakan untuk menguji model pengukuran enam faktor. Hasil CFA ditampilkan pada gambar 3.



Gambar 4.1 Hasil Pengukuran CFA

Hasil pengujian CFA menunjukkan bahwa seluruh indikator memiliki loading faktor yang tinggi dan signifikan terhadap konstruk masing-masing, yang berarti setiap item mampu menjelaskan variabel laten dengan baik. Indeks kesesuaian model (fit indices) juga menunjukkan hasil yang sangat baik, dengan demikian dapat disimpulkan bahwa struktur faktor CS-S sesuai dengan model teoritis enam dimensi keamanan siber dan fit dengan data empiris. Penelitian ini juga sejalan dengan studi sebelumnya yang menekankan pentingnya pengujian validitas dan reliabilitas instrumen pengukuran melalui Confirmatory Factor Analysis (CFA) dalam konteks keamanan informasi (Eryc 2023).

4.4. Perbandingan dengan Penelitian terdahulu

- Sejalan dengan (Corallo et al. 2023) yang menekankan pentingnya pengamanan IT dan OT di industri 4.0, penelitian ini menunjukkan bahwa perusahaan Batam sudah cukup siap pada aspek confidentiality, integrity, dan availability.
- Hal ini juga konsisten dengan (Cremer et al. 2022) yang menekankan keterbatasan data ketersediaan sebagai risiko siber.

4.5. Implikasi bagi Perusahaan di Batam

- Kesiapan adopsi Zero Trust Architecture (ZTA) di Batam masih parsial. Perusahaan lebih siap pada aspek teknis (CIA Triad)

- Temuan ini menunjukkan bahwa prinsip ZTA "never trust, always verify" belum sepenuhnya diterapkan. Perusahaan masih cenderung mengandalkan kontrol perimeter tradisional

4.6. Hasil Hipotesis Penelitian

H1: Model enam faktor CS-S sesuai dengan data empiris perusahaan di Batam melalui CFA. Analisis faktor konfirmatori (CFA) menunjukkan bahwa model enam faktor CS-S cocok dengan data empiris. Semua item menunjukkan signifikansi, dengan loading faktor yang memadai, dan indeks kesesuaian model (CFI = 0.980; TLI = 0.977; RMSEA = 0.051) tergolong dalam kategori baik hingga sangat baik. Ini menunjukkan bahwa struktur enam faktor CS-S dapat diterapkan dalam konteks perusahaan di Batam. Dengan demikian, H1 dapat didukung.

H2: Instrumen CS-S memiliki validitas dan reliabilitas yang baik dalam konteks perusahaan di Batam. Hasil analisis validitas konstruk melalui CFA menunjukkan bahwa semua indikator secara signifikan memuat konstruknya. Selain itu, hasil pengujian reliabilitas menunjukkan nilai Cronbach's Alpha untuk setiap dimensi berada dalam rentang 0.913–0.946, jauh melampaui batas minimum 0.70. Dengan kata lain, instrumen CS-S terbukti valid dan reliabel dalam konteks penelitian ini. H2 didukung.

H3: Hasil CFA menunjukkan bahwa setiap dimensi CS-S valid dan reliabel, termasuk kontrol/kepemilikan dan keaslian. Akan tetapi, menurut teori dan konteks peraturan, kedua aspek ini memiliki fungsi strategis dalam penerapan ZTA. UU PDP mengharuskan perusahaan untuk menjamin pengawasan penuh terhadap data pribadi, sedangkan prinsip ZTA 'never trust, always verify' menyoroti pentingnya verifikasi identitas. Hal ini diperkuat oleh kajian literatur yang menunjukkan bahwa integrasi teknologi digital dan AI dapat meningkatkan visibilitas, monitoring real-time, serta akuntabilitas dalam rantai pasok, yang merupakan fondasi penting bagi penerapan arsitektur Zero Trust (Eryc and Deu 2024). Oleh karena itu, meskipun secara statistik semua dimensi memiliki kekuatan, faktor non-teknis ini tetap menjadi kunci keberhasilan implementasi ZTA.

4.7. Diskusi

Penelitian ini menunjukkan bahwa model enam faktor Cybersecurity Scale (CS-S) terbukti sah dan konsisten untuk diterapkan dalam konteks industri di Batam. Setiap indikator pada masing-masing dimensi memiliki faktor loading yang tinggi dan signifikan terhadap konstruk masing-masing (rata-rata > 0.88), sedangkan nilai Cronbach's Alpha berada di antara 0.913–0.946, menunjukkan konsistensi internal yang sangat baik.

Secara mendalam, hasil statistik ini dapat diartikan dalam kerangka Zero Trust Architecture (ZTA). Tingginya loading factor pada dimensi Authenticity menunjukkan bahwa responden sangat menyadari pentingnya verifikasi identitas dan autentikasi yang terus-menerus, dua aspek dasar dalam penerapan prinsip ZTA "never trust, always verify". Ini mengindikasikan bahwa pemahaman manusia mengenai praktik autentikasi telah menjadi bagian penting dalam kesiapan dasar sumber daya manusia di Batam.

Selanjutnya, tingkat reliabilitas yang tinggi pada dimensi Kontrol/Kepemilikan menegaskan pemahaman responden akan pentingnya kontrol penuh terhadap data dan hak akses sistem. Dalam konteks ZTA, ini menggambarkan penerapan pilar Identity and Access Management (IAM) yang efisien, di mana organisasi tidak lagi bergantung pada kepercayaan implisit, tetapi memverifikasi setiap kali akses dilakukan.

Sementara itu, tiga aspek utama keamanan siber, yaitu Confidentiality, Integrity, dan Availability (Triad CIA) memperlihatkan kesiapan teknis yang kuat di kalangan perusahaan Batam. Nliai reliabilitas yang tinggi pada dimensi-dimensi ini menunjukkan bahwa praktik perlindungan data, validasi informasi, serta jaminan ketersediaan sistem sudah terintegrasi dengan baik dalam kegiatan sehari-hari. Ini menunjukkan bahwa sektor industri Batam telah memiliki dasar teknis yang cukup untuk mengimplementasikan kerangka ZTA yang lebih komprehensif.

Dimensi Utility, yang juga menunjukkan tingkat realibilitas tinggi, menandakan bahwa penggunaan data secara strategis telah disertai oleh kesadaran akan risiko keamanan yang menyertainya. Dalam konteks ZTA, ini memperkuat pilar policy enforcement and visibility, di mana setiap pemanfaatan data harus bisa terdeteksi dan diaudit.

Secara keseluruhan, hasil ini memperkuat posisi penelitian bahwa validasi CS-S bukan sekadar uji instrumen, melainkan langkah awal untuk mengukur kesiapan sumber daya manusia sebagai pilar utama adopsi ZTA. Dengan nilai validitas dan reliabilitas yang tinggi, penelitian ini menunjukkan bahwa organisasi di Batam memiliki potensi besar untuk bertransisi menuju model keamanan berbasis Zero Trust, selama aspek teknis dan perilaku manusia dapat dikelola secara terpadu.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil dari analisis dan pembahasan, penelitian ini menemukan kesimpulan sebagai berikut :

1. Cybersecurity Scale (CS-S) terbukti valid dan reliabel sebagai instrumen untuk mengukur kesiapan sumber daya manusia (SDM) dalam

konteks penerapan Zero Trust Architecture (ZTA) di industri Batam.

2. Hasil Analisis Faktor Konfirmatori (CFA) menunjukkan bahwa model enam faktor CS-S—Confidentiality, Integrity, Availability, Control/Possession, Authenticity, dan Utility—memiliki loading factor tinggi dan kesesuaian model yang baik (CFI = 0.980; TLI = 0.977; RMSEA = 0.051).
3. Uji reliabilitas Cronbach's Alpha (0.913–0.946) menegaskan bahwa semua konstruk memiliki konsistensi internal yang sangat kuat, menandakan bahwa instrumen CS-S dapat dipercaya dalam mengukur perilaku dan kesadaran keamanan individu.
4. Dimensi Authenticity dan Control/Possession menunjukkan nilai tertinggi, mengindikasikan kesadaran responden terhadap pentingnya verifikasi identitas dan kontrol akses data, dua elemen utama dari pilar Identity and Access Management (IAM) dalam ZTA.
5. Dimensi Confidentiality, Integrity, dan Availability (CIA Triad) mencerminkan kesiapan teknis yang baik di perusahaan-perusahaan Batam, menandakan bahwa praktik keamanan dasar sudah tertanam sebelum adopsi ZTA secara penuh.
6. Dimensi Utility menggambarkan kemampuan organisasi dalam menggunakan data secara strategis dengan tetap memperhatikan keamanan dan kepatuhan, selaras dengan pilar Policy Enforcement and Visibility pada ZTA.
7. Secara keseluruhan, penelitian ini menegaskan bahwa kesiapan SDM merupakan pilar fundamental dalam asesmen kesiapan ZTA, dan validasi CS-S menjadi langkah awal menuju pengukuran komprehensif kesiapan keamanan siber nasional.
8. Penelitian ini memberikan kontribusi ilmiah dan praktis: memperluas validasi instrumen keamanan siber di Indonesia, serta menyediakan dasar empiris bagi perusahaan dan pembuat kebijakan untuk merancang strategi adopsi ZTA yang lebih efektif dan terukur.

5.2. Saran

Berdasarkan temuan penelitian, disarankan beberapa langkah berikut:

1. Untuk perusahaan

- Integrasikan prinsip ZTA ke dalam budaya organisasi. Lakukan pelatihan kesadaran keamanan siber berkelanjutan yang menekankan pentingnya autentikasi berlapis dan pengendalian akses berbasis peran.
- Gunakan hasil pengukuran CS-S sebagai dasar untuk memetakan tingkat kesiapan SDM dalam penerapan kebijakan keamanan berbasis Zero Trust.
- Implementasikan langkah konkret seperti penerapan Multi-Factor Authentication (MFA), audit keamanan berkala, serta pemantauan aktivitas pengguna secara real-time untuk memperkuat pilar Identity and Access Management dan Visibility.

2. Untuk penelitian selanjutnya

- Lakukan adaptasi budaya terhadap instrumen CS-S agar lebih kontekstual untuk lingkungan organisasi di Indonesia. I
- Perluasan studi ke wilayah dan sektor lain (misalnya finansial, kesehatan, dan pemerintahan) agar validasi instrumen dapat digeneralisasi.
- Gunakan pendekatan mixed-method atau longitudinal study untuk menggali hubungan antara kesiapan SDM, kepatuhan regulasi, dan efektivitas implementasi ZTA secara jangka panjang.

DAFTAR PUSTAKA

Abrahams, Temitayo Oluwaseun, Sarah Kuzankah Ewuga, Simon Kaggwa, Prisca Ugomma Uwaoma, Azeez Olanipekun Hassan and Samuel Onimisi Dawodu. 2023. "Review of Strategic Alignment: Accounting and Cybersecurity for Data Confidentiality and Financial Security". *World Journal of Advanced Research and Reviews* 20: 1743–1756. <https://doi.org/10.30574/wjarr.2023.20.3.2691>.

Alexander, Richard C, Liran Ma, Ze-Li Dou, Zhipeng Cai and Yan Huang. 2023. "Integrity, Confidentiality, and Equity: Using Inquiry-Based Labs to help Students Understand AI and Cybersecurity". *Journal of Cybersecurity Education, Research and Practice* 2024. <https://doi.org/https://doi.org/10.32727/8.2023.34> [accessed 16 December 2024].

Arpaci, Ibrahim and Kadir Sevinc. 2022. "Development of the Cybersecurity Scale (CS-S): Evidence of Validity and Reliability". *Information Development* 38: 218–226. <https://doi.org/10.1177/0266666921997512>.

Bartol, Nadya, Michael Coden, David Gee and Craig Lawton. n.d. "ENSURING CYBERSECURITY IN THE ELECTRIC UTILITY INDUSTRY".

Corallo, Angelo, Mariangela Lazoi, Marianna Lezzi and Pierpaolo Pontrandolfo. 2023. "Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level". *IEEE Transactions on Engineering Management* 70: 3745–3765. <https://doi.org/10.1109/TEM.2021.3084687

Cremer, Frank, Barry Sheehan, Michael Fortmann, Arash N. Kia, Martin Mullins, Finbarr Murphy and Stefan Materne. 2022. "Cyber Risk and Cybersecurity: A Systematic Review of Data Availability". *Geneva Papers on Risk and Insurance: Issues and Practice* 47: 698–736.

<https://doi.org/10.1057/s41288-022-00266-6>.

Eryc. 2023. "ANALISA PEMANFAATAN INSTAGRAM DALAM MEMPENGARUHI MOTIVASI DAN INTENSI GREEN CONSUMPTION". *Jurnal Ilmiah Ilmu Komputer Fakultas Ilmu Komputer Universitas AL Asyariah Mandar* 9: 63–72. <http://ejournal.fikom-unasman.ac.id>.

Eryc and Indasari Deu. 2024. "INTEGRASI TEKNOLOGI DIGITAL DAN AI DALAM MEMPERKUAT AKUNTABILITAS PADA OPERASI MANAJEMEN RANTAI PASOKAN: ANALISIS LITERATUR SISTEMATIS (THE INTEGRATION OF DIGITAL TECHNOLOGIES AND AI IN STRENGTHENING ACCOUNTABILITY IN SUPPLY CHAIN OPERATIONS: A SYSTEMATIC LITERATURE REVIEW)". *TEKNIMEDIA* 5: 200–211.

Eryc and Didi Santoso. 2024. "PENENTUAN FAKTOR-FAKTOR KUNCI KEBERHASILAN IMPLEMENTASI PERANGKAT LUNAK ERP BERBAHASA MANDARIN: ANALISIS STUDI KASUS PADA PERUSAHAAN MANUFAKTUR DI BATAM". *Journal of Information System Management (JOISM) e-ISSN* 5: 176–182.

Eryc, Lilian Nurul Wildani, Tiara Plorist Sibarani, Raihan and Jhohari. 2024. "Analisis Penerapan Teknologi Manajemen Informasi Di Netflix Global : Optimalisasi Pengalaman Pengguna Dan Efisiensi Operasional". *Amanah Mengabdi* 1: 102–111. <https://jurnalamanah.com/index.php/amanahmengabdi/index>.

Jeffry, Sebastian, Junaidi, Wenny and Eryc. 2024. "Strategi Implementasi Teknologi Informasi Manajemen Untuk Kesuksesan Bisnis". *Vifada Management and Social Sciences* 2: 16–23. <https://doi.org/10.70184/hm552369>.

Kerman, Alper, Murugiah Souppaya, Susan Symington, Karen Scarfone and William Barker. 2020. "Implementing a Zero Trust Architecture". *National Institute of Standards and Technology* 2020.

Pant, Abhishek, Dr. Amarjit R Deshmukh, Mr. Yashwant Kumar and Mr. Anmol Soi. 2023. "Importance of Data Security and Privacy Compliance". *International Journal for Research in Applied Science and Engineering Technology* 11: 1561–1565. <https://doi.org/10.22214/ijraset.2023.56862>.

Prastyanti, Rina Arum, Istiyawati Rahayu, Eiad Yafi, Kelik Wardiono and Arief Budiono. 2022. "Law And Personal Data: Offering Strategies For Consumer Protection In New Normal Situation In Indonesia". *Jurnal Jurisprudence* 11: 82–99. <https://doi.org/10.23917/jurisprudence.v11i1.14756>.

Sasada, Taisho, Yuzo Taenaka, Youki Kadobayashi and Doudou Fall. 2024. "Web-Biometrics for User Authenticity Verification in Zero Trust Access Control". *IEEE Access*. <https://doi.org/10.1109/ACCESS.2024.3413696>.