Jurnal JAMIKA Manajemen Informatika

Jurnal Manajemen Informatika (JAMIKA)
Volume xx Nomor x Edisi xxxx 20xx E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Evaluasi Kesadaran Keamanan Data Pribadi Pelajar Vokasi Jurusan Informatika dalam Penggunaan Smartphone Berdasarkan Model Knowledge, Attitude, and Behaviour (KAB): Studi Kasus di SMK XYZ Bekasi

Evaluation of Vocational Informatics Students' Personal Data Security Awareness in Smartphone Use Based on the Knowledge, Attitude, and Behaviour (KAB) Model: A Case Study at SMK XYZ Bekasi

Mega Thianka[1], Muhammad Idris[2*]
[1,2]Program Studi Rekayasa Keamanan Siber, Jurusan Teknik Informatika, Politeknik Negeri Batam, Batam, Indonesia
**E-mail: mega.thianka@students.polibatam.ac.id*

Abstrak

Generasi Z dikenal sebagai digital natives, namun kefasihan teknologi tidak selalu berbanding lurus dengan kesadaran keamanan data pribadi yang memadai. Penelitian ini bertujuan mengevaluasi kesadaran keamanan data pribadi pelajar vokasi jurusan informatika di SMK XYZ Bekasi menggunakan model Knowledge, Attitude, and Behaviour (KAB) dengan pendekatan kuantitatif deskriptif-korelatif. Sampel sebanyak 60 siswa aktif jurusan RPL dan TKJ berusia 15–18 tahun pada satu sekolah dipilih melalui purposive sampling (non-probabilitas). Instrumen kuesioner 30 butir berskala Likert lima poin menunjukkan reliabilitas tinggi (Cronbach Alpha: Knowledge=0,875, Attitude=0,910, Behaviour=0,911) dan seluruh 30 butir dinyatakan valid. Uji normalitas Shapiro-Wilk menunjukkan distribusi tidak normal (p<0,05), sehingga analisis korelasi menggunakan Spearman's Rho. Hasil menunjukkan dimensi Knowledge berada pada kategori Tinggi (M=4,18), Attitude Tinggi (M=4,32), dan Behaviour Tinggi (M=4,11). Meskipun demikian, terdapat kesenjangan Attitude–Behaviour sebesar 0,217 yang terbukti signifikan secara statistik (uji Wilcoxon signed-rank, p=0,00031), dan 8 responden (13,3%) teridentifikasi menunjukkan pola privacy paradox. Korelasi Spearman antardimensi seluruhnya signifikan: K–A (rs=0,525), K–B (rs=0,543), dan A–B (rs=0,744; kuat); analisis mediasi formal (Sobel, bootstrapping) mengonfirmasi bahwa Attitude memediasi secara parsial dan signifikan hubungan Knowledge–Behaviour (ab=0,441; p<0,001). Temuan ini menunjukkan bahwa meski kesadaran umum sudah tinggi, masih terdapat kesenjangan antara sikap dan perilaku nyata (dengan Behaviour diukur secara self-report) yang perlu ditangani melalui intervensi literasi keamanan siber berbasis bukti; temuan bersifat spesifik pada konteks studi kasus ini dan belum tentu merepresentasikan Generasi Z secara umum.

Kata kunci: *Pelajar Vokasi Jurusan Informatika, Keamanan Data Pribadi, Knowledge Attitude Behaviour, Privacy Paradox, Smartphone.*

Abstract

Generation Z is widely recognized as digital natives; however, technological fluency does not always correspond to adequate personal data security awareness. This study evaluates the level of personal data security awareness among vocational informatics students at SMK XYZ Bekasi using the Knowledge, Attitude, and Behaviour (KAB) model with a quantitative descriptive-correlational approach. Sixty active students from software engineering (RPL) and computer network engineering (TKJ) majors, aged 15–18, at a single vocational school were selected via purposive (non-probability) sampling. A 30-item five-point Likert scale questionnaire demonstrated high reliability (Cronbach Alpha: Knowledge=0.875, Attitude=0.910, Behaviour=0.911) with all 30 items confirmed valid. Shapiro-Wilk normality tests revealed non-normal distributions (p<0.05), so Spearman's Rho was used for correlation analysis. Results indicate all three dimensions fall in the High category: Knowledge (M=4.18), Attitude (M=4.32), and Behaviour (M=4.11). However, a statistically significant Attitude–Behaviour gap of 0.217 was identified (Wilcoxon signed-rank test, p=0.00031), with 8 respondents (13.3%) exhibiting a privacy paradox pattern. Spearman correlations between all dimension pairs were significant: K–A (rs=0.525), K–B (rs=0.543), and A–B (rs=0.744; strong); formal mediation analysis (Sobel test, bootstrapping) confirmed that Attitude partially and significantly mediates the Knowledge–Behaviour relationship (ab=0.441, p<0.001). These findings suggest that while overall awareness is high, a gap between attitude and actual behaviour persists (with Behaviour measured via self-report), warranting targeted evidence-based cybersecurity literacy interventions; findings are specific to this case-study context and may not generalize to Generation Z at large.

Keywords: *Vocational Informatics Students, Personal Data Security, Knowledge Attitude Behaviour, Privacy Paradox, Smartphone.*

Naskah diterima xx Jun. 2026; direvisi xx Jun. 2026; dipublikasikan xx Jul. 2026.

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah mengubah cara masyarakat berinteraksi dengan dunia digital, terutama melalui perangkat smartphone. Berdasarkan laporan We Are Social dan Hootsuite [1], jumlah pengguna smartphone di Indonesia telah melampaui 167 juta jiwa, menjadikan Indonesia salah satu negara dengan penetrasi smartphone tertinggi di Asia Tenggara. Di tengah pesatnya adopsi teknologi ini, keamanan data pribadi menjadi isu yang semakin kritis

mengingat smartphone kini menyimpan berbagai informasi sensitif seperti data keuangan, komunikasi pribadi, riwayat lokasi, dan identitas digital.

Generasi Z, yakni individu yang lahir antara tahun 1997 hingga 2012 [2], merupakan kelompok yang paling intens berinteraksi dengan teknologi digital sejak usia dini sehingga sering disebut sebagai *digital natives*. Meskipun demikian, familiaritas terhadap teknologi tidak serta merta berbanding lurus dengan pemahaman akan keamanan data pribadi. Penelitian Adrian, Lindawaty, dan Kurniawan [3] pada konteks Generasi Z Indonesia menunjukkan bahwa kelompok ini cenderung mengabaikan pengaturan privasi dan kurang waspada terhadap risiko siber. Kondisi ini dikenal sebagai *privacy paradox*—kontradiksi antara kepedulian yang dinyatakan dengan perilaku yang dipraktikkan.

Nugraha et al. [4] menemukan bahwa meskipun pelajar Indonesia memiliki kesadaran umum yang cukup, ancaman spesifik seperti *phishing* dan penyalahgunaan izin aplikasi masih kurang dipahami secara konkret. Zwilling et al. [5] dalam studi komparatif empat negara menegaskan bahwa pengguna internet umumnya memiliki pengetahuan yang memadai namun hanya menerapkan langkah perlindungan yang minimal—kesenjangan yang hanya dapat terdeteksi melalui pengukuran simultan ketiga dimensi KAB. Ahamed et al. [7] secara empiris mengonfirmasi bahwa sikap (Attitude) berfungsi sebagai mediator antara pengetahuan dan perilaku, memperkuat urgensi evaluasi ketiga dimensi secara simultan.

Penelitian ini secara spesifik berfokus pada siswa SMK XYZ Bekasi sebagai studi kasus, khususnya siswa jurusan Rekayasa Perangkat Lunak (RPL) dan Teknik Komputer dan Jaringan (TKJ) yang merupakan calon tenaga kerja di bidang perangkat lunak dan jaringan komputer sehingga rentan terhadap ancaman siber dalam praktik profesional maupun pribadi. Model *Knowledge, Attitude, and Behaviour* (KAB) yang pertama kali diusulkan Kruger dan Kearney [6] dipilih sebagai kerangka analisis karena mampu mengukur secara komprehensif dimensi pengetahuan, sikap, dan perilaku nyata pengguna terhadap keamanan data pribadi.

Perlu ditegaskan bahwa penelitian ini merupakan studi survei psikometrik yang mengukur kesadaran keamanan data pribadi tanpa disertai artefak rekayasa teknis (pembangunan sistem, kontrol keamanan, atau audit teknis). Posisi penelitian dalam kurikulum Program Studi Rekayasa Keamanan Siber diperlakukan sebagai tahap kajian kebutuhan (need assessment) berbasis bukti, yaitu pemetaan kesenjangan pengetahuan, sikap, dan perilaku pengguna yang menjadi dasar empiris bagi perancangan intervensi maupun kontrol keamanan teknis pada penelitian lanjutan (misalnya rancangan modul pelatihan berbasis skenario atau kebijakan teknis manajemen izin aplikasi). Keterbatasan cakupan teknis ini dibahas lebih lanjut pada bagian Keterbatasan Penelitian.

II. TINJAUAN PUSTAKA

A. Kajian Penelitian Terdahulu

Berikut disajikan rangkuman penelitian-penelitian terdahulu yang relevan dengan topik penelitian ini, sebagai dasar komparasi dan penguatan argumentasi ilmiah:

TABEL 1
RINGKASAN TINJAUAN PUSTAKA

No.	Judul Penelitian	Peneliti / Tahun	Inti Penelitian	Relevansi
1	Cyber Security Awareness, Knowledge and Behavior: A Comparative Study	Zwilling et al. (2022)	Mengevaluasi hubungan antara kesadaran, pengetahuan, dan perilaku keamanan siber menggunakan model KAB pada pengguna internet di empat negara. Pengguna memiliki pengetahuan memadai namun hanya menerapkan perlindungan minimal.	Menjadi acuan utama penerapan model KAB. Kesenjangan antara pengetahuan dan perilaku memperkuat urgensi evaluasi ketiga dimensi KAB secara simultan pada pelajar vokasi jurusan informatika.
2	The Influence of Social Education Level on Cybersecurity Awareness and Behaviour	Hong et al. (2022)	Mengusulkan model KAB yang diperluas dengan tingkat pendidikan sebagai moderator; menemukan paparan lingkungan kerja memengaruhi Attitude dan Behaviour secara signifikan.	Mendukung validitas model KAB sebagai kerangka evaluasi dan memberikan dasar komparatif untuk konteks pendidikan SMK.
3	Indonesian Generation Z's Awareness of Data Privacy in the Use of Social Media	Adrian et al. (2023)	Mengukur kesadaran privasi data Generasi Z Indonesia terhadap media sosial. Gen Z mengaku cukup sadar namun perilaku aktual	Sangat relevan karena fokus pada Generasi Z Indonesia dan menemukan pola privacy paradox—mendukung argumen

			tidak mencerminkan tindakan perlindungan nyata.	penelitian pada dimensi Behaviour.
4	Analysis of Higher Education Students' Awareness in Indonesia on Personal Data Security in Social Media	Nugraha et al. (2023)	Menganalisis kesadaran mahasiswa Indonesia; ancaman spesifik seperti phishing dan penyalahgunaan izin aplikasi masih kurang dipahami meski kesadaran umum cukup.	Memberikan konteks empiris lokal mengenai kesadaran keamanan data, mendukung konstruksi butir instrumen pada dimensi Knowledge dan Attitude.
5	How Education Level Influences Internet Security Knowledge, Behaviour, and Attitude	Hong & Xu (2023)	Menguji hubungan tingkat pendidikan dengan tiga dimensi KAB menggunakan HAIS-Q; tingkat pendidikan tidak selalu menjadi prediktor konsisten terhadap perilaku aman.	Mendukung operasionalisasi instrumen KAB dan menegaskan kelompok pendidikan menengah perlu dievaluasi secara mandiri.
6	Empowering Students for Cybersecurity Awareness Management: The Role of Cybersecurity Attitude	Ahamed et al. (2024)	Mengkonfirmasi Attitude sebagai mediator antara pengetahuan dan perilaku aman pada mahasiswa; sikap menjadi jembatan antara Knowledge dan Behaviour.	Memperkuat posisi Attitude sebagai variabel kunci model KAB dan mendukung rancangan analisis korelasi antardimensi pada pelajar vokasi jurusan informatika.

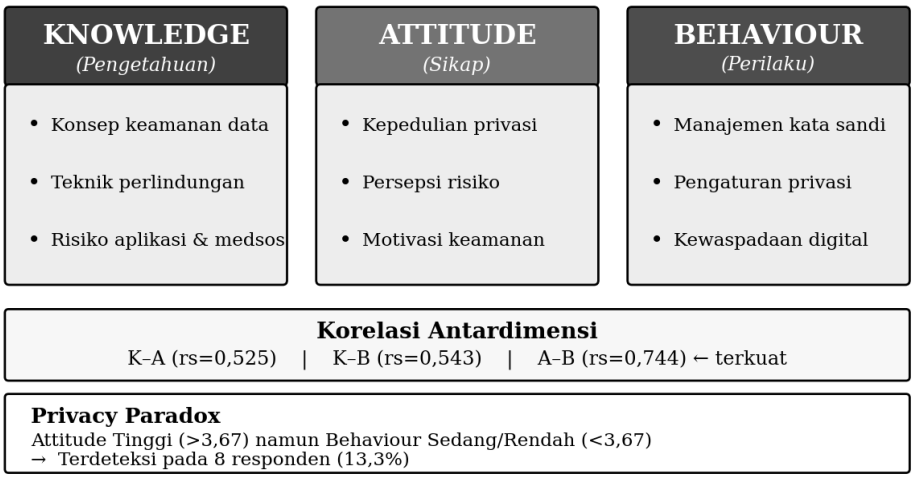
Tabel 1. Ringkasan Tinjauan Pustaka

B. Model Knowledge, Attitude, and Behaviour (KAB)

Model *Knowledge, Attitude, and Behaviour* (KAB) pertama kali diusulkan oleh Kruger dan Kearney [6] sebagai kerangka untuk mengukur kesadaran keamanan informasi. Model ini berakar pada tiga komponen psikologi sosial, yaitu kognisi, afeksi, dan konasi, yang masing-masing berkorespondensi dengan dimensi *Knowledge*, *Attitude*, dan *Behaviour* [11].

Dimensi pertama, **Knowledge** (pengetahuan), merujuk pada pemahaman kognitif individu terhadap konsep, ancaman, dan mekanisme perlindungan keamanan data pribadi. Pengetahuan yang memadai dianggap sebagai prasyarat terbentuknya sikap yang positif. Dimensi kedua, **Attitude** (sikap), mencerminkan evaluasi afektif individu terhadap isu keamanan digital. Ahamed et al. [7] secara empiris menemukan bahwa sikap berperan sebagai jembatan antara pengetahuan dan perilaku keamanan—pengetahuan yang tinggi perlu disertai pembentukan sikap positif agar terwujud dalam tindakan nyata. Dimensi ketiga, **Behaviour** (perilaku), merupakan manifestasi nyata dari kedua dimensi sebelumnya dalam tindakan keamanan sehari-hari, seperti penggunaan autentikasi dua faktor, pembaruan perangkat lunak secara rutin, dan kewaspadaan terhadap serangan *phishing*.

Kerangka konseptual model KAB dalam penelitian ini disajikan pada Gambar 1 berikut:



Gambar 1. Kerangka Konseptual Model KAB

C. Konsep Keamanan Data Pribadi

Keamanan data pribadi (*personal data security*) merujuk pada serangkaian praktik, kebijakan, dan mekanisme teknis yang bertujuan melindungi informasi yang dapat mengidentifikasi individu dari akses, pengungkapan, modifikasi, atau penghancuran yang tidak sah. Di Indonesia, perlindungan ini secara yuridis diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang mendefinisikan data pribadi sebagai setiap data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri maupun dikombinasi dengan informasi lainnya [13].

Nugraha et al. [4] menemukan bahwa pelajar Indonesia memiliki kesadaran umum yang cukup terhadap keamanan data, namun ancaman spesifik seperti *phishing*, pencurian akun, dan penyalahgunaan izin aplikasi masih kurang dipahami secara konkret. Dalam konteks penggunaan smartphone, ancaman tersebut mencakup: (1) *malware* dan *spyware* yang mengeksfiltrasi data; (2) serangan *phishing* melalui pesan teks maupun surel; (3) kebocoran data akibat izin aplikasi yang berlebihan; (4) penggunaan jaringan Wi-Fi publik yang tidak terenkripsi; serta (5) praktik *social engineering* yang memanipulasi pengguna untuk mengungkapkan informasi sensitif.

D. Karakteristik Generasi Z dan Privacy Paradox

Generasi Z didefinisikan sebagai individu yang lahir antara tahun 1997 hingga 2012 [2]. Generasi ini tumbuh bersamaan dengan perkembangan internet cepat, media sosial, dan smartphone sehingga memiliki kefasihan teknologi yang tinggi. Namun, berbagai studi terkini menunjukkan bahwa kefasihan teknologi tidak identik dengan literasi keamanan digital yang memadai.

Penelitian yang secara khusus berfokus pada Generasi Z Indonesia oleh Adrian et al. [3] menemukan bahwa sebagian besar Gen Z mengaku cukup sadar terhadap privasi data, namun perilaku aktual mereka tidak mencerminkan tindakan perlindungan yang nyata. Kondisi ini dikenal sebagai **privacy paradox**—suatu kondisi di mana terdapat kontradiksi antara kepedulian yang dinyatakan (Attitude) dan perilaku yang dipraktikkan (Behaviour). Pola ini konsisten dengan temuan Hong & Xu [11] yang menunjukkan bahwa kelompok dengan tingkat pendidikan menengah cenderung menunjukkan kesenjangan lebih besar antara sikap dan perilaku aman dibandingkan kelompok dengan paparan pendidikan lebih tinggi.

III. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif deskriptif-korelatif untuk mengevaluasi tingkat kesadaran keamanan data pribadi serta menganalisis hubungan antardimensi KAB [8]. Pengumpulan data dilaksanakan dalam satu hari pada tanggal 18 Mei 2026 di SMK XYZ Bekasi.

A. Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh siswa aktif SMK XYZ Bekasi yang menggunakan smartphone secara aktif. Teknik sampling yang digunakan adalah *purposive sampling* (non-probabilitas) dengan kriteria inklusi: (1) siswa aktif berusia 15–18 tahun (Generasi Z), dan (2) menggunakan smartphone secara aktif. Populasi total siswa aktif SMK XYZ Bekasi pada tiga angkatan (kelas 10–12) adalah 743 siswa. Berdasarkan formula Slovin dengan margin of error 10%, ukuran sampel minimum yang disyaratkan adalah $n = N/(1+Ne^2) = 743/(1+743\times0{,}1^2) \approx 89$ responden. Sampel yang berhasil dikumpulkan sebanyak 60 responden berada di bawah ambang tersebut, yang jika dihitung mundur ($e = \sqrt{((N-n)/(N\cdot n))}$ setara dengan margin of error aktual sebesar ±12,4%. Penulis mengakui bahwa penerapan formula Slovin di sini bersifat indikatif dan tidak sepenuhnya konsisten dengan teknik purposive sampling non-probabilitas yang sebenarnya digunakan; angka sampel akhir semestinya dipandang sebagai hasil keterbatasan akses lapangan (tiga kelas yang bersedia berpartisipasi) dan bukan hasil perhitungan probabilitas formal. Keterbatasan ini dijelaskan lebih lanjut pada bagian Keterbatasan Penelitian. Total sampel yang berhasil dikumpulkan adalah 60 responden dari tiga kelas, yakni kelas 11 RPL (n=22), kelas 10 RPL (n=22), dan kelas 11 TKJ (n=16). Sebaran usia responden: 37 siswa berusia 17 tahun (61,7%), 19 siswa berusia 16 tahun (31,7%), dan 4 siswa berusia 15 tahun (6,7%). Kuesioner didistribusikan secara daring melalui Google Form kepada siswa di dalam kelas dengan pendampingan guru/wali kelas pada tanggal 18 Mei 2026; seluruh 60 respons terkumpul dalam satu hari (pukul 10.27–17.02 WIB), dengan response rate 100% (60 dari 60 kuesioner yang dibagikan terisi lengkap). Persetujuan partisipasi diperoleh secara lisan dari pihak sekolah (guru/wali kelas) serta dari masing-masing responden sebelum pengisian kuesioner, tanpa dokumentasi tertulis (formulir informed consent). Penulis mengakui hal ini sebagai keterbatasan prosedural, mengingat sebagian responden berusia di bawah 18 tahun; penelitian lanjutan pada populasi pelajar disarankan menggunakan formulir persetujuan tertulis baik dari pihak sekolah/wali maupun siswa untuk memenuhi standar etik penelitian pada subjek anak/remaja. Data identitas responden (nama dan alamat surel) yang terekam pada formulir Google Form digunakan semata untuk keperluan verifikasi internal selama pengumpulan data dan tidak pernah dipublikasikan maupun disebarluaskan; berkas mentah tersebut disimpan secara pribadi oleh peneliti dan tidak diakses pihak ketiga. Seluruh data yang diolah, dianalisis, dan dilampirkan dalam naskah ini telah menggunakan kode responden standar (R01–R60) tanpa menyertakan atribut identitas pribadi, sehingga memenuhi prinsip minimalisasi data sebagaimana diatur dalam UU PDP No. 27/2022.

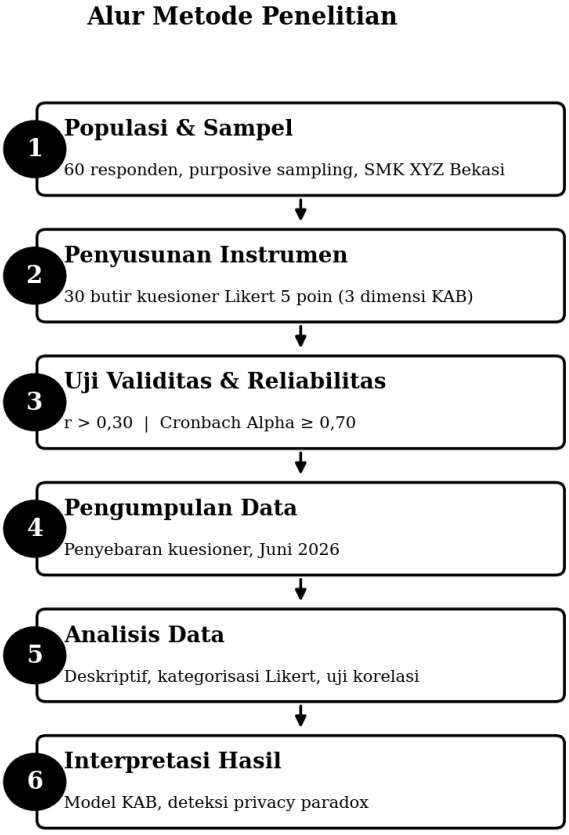
B. Instrumen dan Uji Instrumen

Instrumen penelitian berupa kuesioner berskala Likert lima poin (1=Sangat Tidak Setuju hingga 5=Sangat Setuju) dengan 30 butir pernyataan—10 butir per dimensi. Uji validitas menggunakan *corrected item-total correlation* (Pearson r) dengan batas $r > 0{,}30$ dan $p < 0{,}05$. Uji reliabilitas menggunakan Cronbach Alpha dengan batas penerimaan $\geq 0{,}70$ [9].

Hasil uji validitas menunjukkan seluruh 30 butir pernyataan dinyatakan valid ($r = 0{,}419$–$0{,}801$; seluruhnya $p < 0{,}001$). Hasil uji reliabilitas menunjukkan nilai Cronbach Alpha yang sangat tinggi: Knowledge = 0,875, Attitude = 0,910, dan Behaviour = 0,911, yang berarti seluruh instrumen sangat reliabel.

C. Teknik Analisis Data

Analisis data dilakukan melalui tahapan: (1) Uji normalitas Kolmogorov-Smirnov dan Shapiro-Wilk sebagai pembuka analisis; (2) Analisis deskriptif (mean, SD, min, max); (3) Kategorisasi tingkat kesadaran berdasarkan interval skala Likert: Rendah (1,00–2,33), Sedang (2,34–3,66), Tinggi (3,67–5,00) [8]; (4) Uji korelasi antardimensi; (5) Interpretasi berbasis model KAB termasuk deteksi privacy paradox.



Gambar 2. Alur Metode Penelitian

IV. HASIL DAN PEMBAHASAN

A. Uji Normalitas

Uji normalitas dilakukan menggunakan Shapiro-Wilk (lebih sensitif untuk n=60) dan Kolmogorov-Smirnov. Hasil selengkapnya disajikan pada Tabel 2.

TABEL 2
HASIL UJI NORMALITAS DIMENSI KAB

Dimensi	SW Statistic	SW p-value	KS Statistic	Distribusi
Knowledge	0,9102	0,0003*	0,1147	Tidak Normal
Attitude	0,8563	0,0000*	0,1527	Tidak Normal
Behaviour	0,9116	0,0004*	0,1139	Tidak Normal

Tabel 2. Hasil Uji Normalitas Dimensi KAB (p < 0,05 = tidak normal)*

Hasil uji Shapiro-Wilk menunjukkan bahwa ketiga dimensi memiliki distribusi tidak normal ($p < 0,05$), meskipun uji KS memberikan hasil yang lebih moderat. Mengacu pada hasil Shapiro-Wilk sebagai uji yang lebih sensitif untuk ukuran sampel n=60, analisis korelasi selanjutnya menggunakan metode non-parametrik Spearman's Rho.

B. Analisis Deskriptif Dimensi KAB

Tabel 3 menyajikan statistik deskriptif ketiga dimensi KAB beserta kategorisasinya.

TABEL 3
STATISTIK DESKRIPTIF DAN KATEGORISASI DIMENSI KAB (n=60)

Dimensi	Mean	SD	Min	Max	Kategori	% Tinggi
Knowledge	4,18	0,681	2,00	5,00	Tinggi	83,3%
Attitude	4,32	0,660	2,10	5,00	Tinggi	86,7%
Behaviour	4,11	0,741	1,80	5,00	Tinggi	76,7%

Tabel 3. Statistik Deskriptif dan Kategorisasi Dimensi KAB (n=60)

Ketiga dimensi KAB secara keseluruhan berada pada kategori Tinggi. Dimensi Attitude memiliki mean tertinggi (4,32), diikuti Knowledge (4,18) dan Behaviour (4,11). Kesenjangan Attitude–Behaviour sebesar 0,217 poin meskipun keduanya berada pada kategori yang sama, hal ini konsisten dengan temuan Zwilling et al. [5] yang menemukan bahwa pengguna internet umumnya memiliki pengetahuan dan sikap yang baik namun implementasi perilaku nyata cenderung lebih rendah.

C. Analisis Per Butir Instrumen

Tabel 4 menyajikan mean dan standar deviasi setiap butir instrumen pada dimensi Knowledge.

TABEL 4
ANALISIS PER BUTIR DIMENSI KNOWLEDGE

No	Pernyataan (Knowledge)	Mean	SD
K1	Izin akses aplikasi (kamera/mikrofon/lokasi) memengaruhi privasi	4.083	1.109
K2	Data lokasi dapat digunakan untuk melacak aktivitas	4.067	1.103
K3	Kunci layar (PIN/pola/sidik jari/wajah) melindungi data	4.567	0.831
K4	Memasang aplikasi di luar toko resmi meningkatkan risiko	4.033	1.119
K5	Wi-Fi publik tanpa proteksi membahayakan data pribadi	4.067	1.023
K6	Pembaruan OS dan aplikasi penting untuk keamanan	4.100	0.877
K7	Data di layanan cloud tetap berisiko jika tidak diamankan	3.900	1.003
K8	Menyimpan dokumen penting di galeri tanpa proteksi berisiko	4.017	1.017
K9	Kode OTP tidak boleh dibagikan kepada siapa pun	4.583	0.743
K10	Akun media sosial dapat diambil alih jika password diketahui	4.383	1.027
	Rata-rata Dimensi Knowledge	**4,180**	**0,681**

Tabel 4. Analisis Per Butir Dimensi Knowledge

Butir K9 (kode OTP tidak boleh dibagikan) memperoleh mean tertinggi (4,583), menandakan hampir semua responden memahami risiko kebocoran kode OTP. Sementara itu, butir K7 (risiko data di layanan cloud) memiliki mean terendah (3,900), mengindikasikan pemahaman tentang keamanan cloud masih perlu ditingkatkan.

Tabel 5 menyajikan analisis per butir dimensi Attitude.

TABEL 5
ANALISIS PER BUTIR DIMENSI ATTITUDE

No	Pernyataan (Attitude)	Mean	SD
A1	Penting untuk selalu mengaktifkan kunci layar	4.450	0.769
A2	Penting membaca izin aplikasi sebelum menginstal	4.150	0.860
A3	Perlu membatasi aplikasi yang mengakses lokasi terus-menerus	4.233	0.945
A4	Tidak nyaman login akun penting di Wi-Fi publik	4.100	1.100
A5	Penting mengaktifkan two-factor authentication	4.550	0.790
A6	Menyimpan dokumen tanpa proteksi adalah tindakan berisiko	4.333	0.951
A7	Perlu memisahkan akun penting dengan akun hiburan	4.317	0.833
A8	Berbagi password/PIN kepada orang lain adalah berbahaya	4.283	0.940
A9	Penting segera bertindak jika smartphone hilang/dicuri	4.483	0.892
A10	Penting mengurangi pembagian info pribadi di media sosial	4.333	0.752
	Rata-rata Dimensi Attitude	**4,323**	**0,660**

Tabel 5. Analisis Per Butir Dimensi Attitude

Dimensi Attitude menunjukkan mean yang paling merata di antara ketiga dimensi. Butir A5 (pentingnya two-factor authentication) memperoleh mean tertinggi (4,550), sedangkan butir A4 (ketidaknyamanan login di Wi-Fi publik) memiliki mean terendah (4,100), mengindikasikan sebagian siswa masih kurang waspada terhadap risiko Wi-Fi publik dalam konteks praktis.

Tabel 6 menyajikan analisis per butir dimensi Behaviour.

TABEL 6
ANALISIS PER BUTIR DIMENSI BEHAVIOUR

No	Pernyataan (Behaviour)	Mean	SD
B1	Membiasakan mengunci layar dengan PIN/pola/biometrik	4.433	0.789
B2	Jarang/tidak pernah memasang aplikasi luar toko resmi	3.717	1.075
B3	Rutin menghapus aplikasi yang tidak digunakan	3.750	1.019
B4	Sering meninjau dan mengatur ulang izin aplikasi	3.867	1.033
B5	Menghindari Wi-Fi publik untuk akun penting	4.050	1.048
B6	Rutin melakukan update OS dan aplikasi	3.867	0.999
B7	Menggunakan sidik jari/face ID/pengunci aplikasi penting	4.167	1.044
B8	Tidak membagikan password/PIN/OTP kepada siapa pun	4.450	0.946
B9	Menghapus/memindahkan foto dokumen penting ke folder aman	4.250	1.019
B10	Segera bertindak pengamanan jika ada aktivitas mencurigakan	4.517	0.930
	Rata-rata Dimensi Behaviour	**4,107**	**0,741**

Tabel 6. Analisis Per Butir Dimensi Behaviour

Pada dimensi Behaviour, butir B10 (segera bertindak pengamanan saat ada aktivitas mencurigakan) memperoleh mean tertinggi (4,517), sedangkan butir B2 (jarang memasang aplikasi dari luar toko resmi) memiliki mean terendah (3,717). Butir B2, B3, dan B4 semuanya di bawah 3,90, mengindikasikan masih terdapat kebiasaan penggunaan aplikasi pihak ketiga, minimnya rutinitas membersihkan aplikasi tak terpakai, dan jarangnya peninjauan izin aplikasi—tiga perilaku kritis yang perlu mendapat perhatian intervensi.

D. Uji Korelasi Spearman Antardimensi KAB

Mengacu pada hasil uji normalitas yang menunjukkan distribusi tidak normal, uji korelasi menggunakan Spearman's Rho. Hasil selengkapnya disajikan pada Tabel 7.

TABEL 7
HASIL UJI KORELASI SPEARMAN'S RHO ANTARDIMENSI KAB

Pasangan Dimensi	Spearman rs	p-value	Kekuatan	Sig.
Knowledge – Attitude (K–A)	0,525	0,000016	Sedang	**
Knowledge – Behaviour (K–B)	0,543	0,000007	Sedang	**
Attitude – Behaviour (A–B)	0,744	0,000000	Kuat	**

*Tabel 7. Hasil Uji Korelasi Spearman's Rho Antardimensi KAB (** p < 0,01)*

Seluruh korelasi antardimensi KAB signifikan secara statistik ($p < 0,01$). Korelasi Attitude–Behaviour ($rs=0,744$) merupakan yang terkuat, selaras dengan gagasan Ahamed et al. [7] bahwa sikap memiliki hubungan yang erat dengan perilaku keamanan. Untuk menguji secara formal klaim peran Attitude sebagai mediator (Ahamed et al. [7]), dilakukan analisis mediasi mengikuti pendekatan Baron & Kenny disertai uji Sobel dan bootstrapping (5.000 resampel) menggunakan data mentah 60 responden. Hasil regresi menunjukkan Knowledge berpengaruh signifikan terhadap Attitude (jalur a: $b=0,663$; $SE=0,093$; $p<0,001$), dan Attitude berpengaruh signifikan terhadap Behaviour dengan mengontrol Knowledge (jalur b: $b=0,665$; $SE=0,123$; $p<0,001$). Efek langsung Knowledge terhadap Behaviour tetap signifikan setelah mengontrol Attitude (c'=0,287; $SE=0,119$; $p=0,019$), sedangkan efek total sebelum mengontrol mediator adalah $c=0,728$ ($p<0,001$). Efek tidak langsung (indirect effect) Knowledge→Attitude→Behaviour sebesar $ab=0,441$ terbukti signifikan baik melalui uji Sobel ($z=4,31$; $p<0,001$) maupun bootstrapping (interval kepercayaan 95%: 0,168–0,802, tidak mencakup nol). Karena efek langsung c' tetap signifikan setelah mediator dimasukkan, hasil ini mengindikasikan mediasi parsial (partial mediation)—Attitude memediasi sekitar 60,6% dari total pengaruh Knowledge terhadap Behaviour, sementara sisanya merupakan pengaruh langsung Knowledge yang tidak melalui Attitude. Temuan ini secara empiris mengonfirmasi dan memperkuat klaim Ahamed et al. [7] dalam konteks siswa SMK. Korelasi Knowledge–Attitude ($rs=0,525$) dan Knowledge–Behaviour ($rs=0,543$) keduanya berada pada kategori sedang, mengindikasikan bahwa pengetahuan saja tidak cukup menjamin terbentuknya sikap dan perilaku aman—intervensi perlu menargetkan penguatan sikap sebagai jalur mediasi yang telah terbukti signifikan.

E. Interpretasi Model KAB dan Fenomena Privacy Paradox

Meskipun ketiga dimensi berada pada kategori Tinggi, analisis lebih rinci mengungkapkan adanya kesenjangan Attitude–Behaviour sebesar 0,217 poin. Signifikansi statistik kesenjangan ini diuji menggunakan uji Wilcoxon signed-rank atas data berpasangan 60 responden, mengingat data tidak berdistribusi normal (lihat Tabel 2). Hasil uji menunjukkan bahwa kesenjangan Attitude–Behaviour signifikan secara statistik ($W=186$; $p=0,00031$; $p<0,01$), dikonfirmasi pula oleh uji-t berpasangan ($t(59)=3,51$; $p=0,00086$). Dengan demikian, skor Behaviour yang secara konsisten lebih rendah daripada Attitude bukan sekadar variasi deskriptif, melainkan perbedaan yang signifikan secara statistik. Selain itu, dimensi Behaviour diukur murni melalui self-report (persepsi diri responden) tanpa validasi teknis/objektif (misalnya audit izin aplikasi aktual atau pemeriksaan pengaturan keamanan perangkat), sehingga skor Behaviour yang tinggi berpotensi dipengaruhi oleh bias social desirability dan perlu dimaknai sebagai persepsi diri, bukan bukti praktik aktual. Terlepas dari keterbatasan tersebut, sebanyak 8 responden (13,3%) tetap teridentifikasi menunjukkan pola *privacy paradox*—yaitu skor Attitude > 3,67 (Tinggi) tetapi skor Behaviour < 3,67 (Sedang atau Rendah). Kondisi ini konsisten dengan temuan Adrian et al. [3] yang mengidentifikasi privacy paradox pada Generasi Z Indonesia, di mana kepedulian yang dinyatakan tidak terwujud dalam tindakan perlindungan nyata.

Hong & Xu [11] menemukan bahwa kelompok dengan tingkat pendidikan menengah cenderung menunjukkan kesenjangan lebih besar antara sikap dan perilaku aman dibandingkan kelompok pendidikan tinggi. Temuan ini memperkuat relevansi penelitian spesifik pada kelompok siswa SMK seperti yang dilakukan dalam studi ini. Butir-butir Behaviour dengan mean terendah (B2=3,717; B3=3,750; B4=3,867) mengindikasikan bahwa kebiasaan memasang aplikasi dari sumber tidak resmi, minimnya rutinitas membersihkan aplikasi, dan jarangnya peninjauan izin aplikasi merupakan area prioritas intervensi.

Berdasarkan temuan ini, rekomendasi intervensi yang dapat diterapkan oleh SMK XYZ Bekasi secara spesifik mencakup: (1) program pelatihan literasi keamanan siber berbasis skenario nyata yang berfokus pada perilaku dengan skor terendah, yaitu manajemen aplikasi pihak ketiga dan peninjauan izin aplikasi (butir B2–B4), serta kewaspadaan Wi-Fi publik (butir A4) dan keamanan layanan cloud (butir K7); (2) integrasi materi keamanan data pribadi dan UU PDP No. 27/2022 ke dalam kurikulum kejuruan RPL dan TKJ; (3) kebijakan sekolah terkait penggunaan aplikasi pihak ketiga dan audit berkala izin aplikasi pada perangkat yang digunakan untuk kegiatan pembelajaran; serta (4) penyampaian laporan hasil pengukuran ini secara resmi

kepada pihak manajemen SMK XYZ Bekasi sebagai dasar evaluasi program literasi digital sekolah, mengingat temuan bersifat spesifik pada populasi sekolah tersebut dan belum tentu merepresentasikan Generasi Z secara umum.

F. Keterbatasan Penelitian

Penelitian ini memiliki beberapa keterbatasan yang perlu menjadi perhatian pembaca dalam menginterpretasikan temuan. Pertama, sampel diambil hanya dari tiga kelas (RPL dan TKJ) pada satu sekolah (SMK XYZ Bekasi) melalui purposive sampling non-probabilitas, sehingga temuan bersifat spesifik pada konteks sekolah tersebut dan tidak dapat digeneralisasikan secara langsung kepada pelajar vokasi jurusan informatika di Indonesia secara luas, maupun kepada Generasi Z secara umum. Judul penelitian telah direvisi untuk secara eksplisit membatasi klaim cakupan pada pelajar vokasi jurusan informatika (RPL dan TKJ) sebagai studi kasus, alih-alih menggunakan label "Generasi Z" yang berpotensi menyiratkan representasi populasi yang lebih luas. Kedua, dimensi Behaviour diukur murni melalui self-report tanpa validasi teknis/objektif, sehingga rentan terhadap bias social desirability; hasil uji Wilcoxon dan mediasi formal yang dilaporkan pada Bagian IV-D dan IV-E tetap tunduk pada keterbatasan ini karena seluruh data Behaviour bersumber dari persepsi diri responden. Ketiga, desain penelitian bersifat cross-sectional sehingga hasil analisis mediasi (Bagian IV-D) menggambarkan pola hubungan statistik, bukan hubungan kausal yang teruji secara eksperimental maupun perubahan kesadaran dari waktu ke waktu. Keempat, penetapan ukuran sampel menggunakan formula Slovin yang dikombinasikan dengan teknik purposive sampling non-probabilitas merupakan inkonsistensi metodologis yang diakui penulis; populasi total siswa aktif SMK XYZ Bekasi adalah 743 siswa, yang berdasarkan formula Slovin (e=10%) mensyaratkan sampel minimum 89 responden, sedangkan sampel yang berhasil dikumpulkan hanya 60 responden (setara margin of error aktual ±12,4%), sehingga sampel penelitian ini berada di bawah ambang minimum yang disyaratkan formula tersebut. Kelima, tinjauan pustaka konseptual (model KAB, privacy paradox) sebagian besar bersumber dari konteks internasional/pendidikan tinggi sehingga literatur spesifik mengenai literasi keamanan siber pelajar kejuruan (SMK) masih terbatas. Keenam, formulir pengumpulan data (Google Form) turut merekam nama lengkap dan alamat surel responden yang berstatus anak/remaja untuk keperluan verifikasi internal; data tersebut tidak pernah dipublikasikan atau disebarluaskan dan disimpan secara pribadi oleh peneliti, sementara seluruh data yang diolah dan dilampirkan dalam naskah ini telah menggunakan kode responden standar (R01–R60) tanpa atribut identitas. Ketujuh, persetujuan partisipasi responden diperoleh secara lisan dari pihak sekolah dan siswa tanpa dokumentasi tertulis (informed consent form), yang merupakan keterbatasan prosedural mengingat sebagian responden berusia di bawah 18 tahun. Penelitian lanjutan disarankan untuk memperluas sampel lintas sekolah serta menyertakan indikator perilaku yang terverifikasi secara teknis (mis. audit izin aplikasi aktual) sebagai pembanding data self-report.

V. KESIMPULAN

Penelitian ini mengevaluasi kesadaran keamanan data pribadi 60 pelajar vokasi jurusan informatika (RPL dan TKJ) di SMK XYZ Bekasi menggunakan model KAB dengan pendekatan kuantitatif deskriptif-korelatif. Seluruh 30 butir instrumen terbukti valid dan reliabel (Cronbach Alpha 0,875–0,911). Uji normalitas Shapiro-Wilk menunjukkan distribusi tidak normal sehingga analisis korelasi menggunakan Spearman's Rho. Ketiga dimensi KAB berada pada kategori Tinggi: Knowledge (M=4,18), Attitude (M=4,32), dan Behaviour (M=4,11). Meskipun demikian, kesenjangan Attitude–Behaviour sebesar 0,217 terbukti signifikan secara statistik melalui uji Wilcoxon signed-rank (W=186; p=0,00031), dan 8 responden (13,3%) menunjukkan pola privacy paradox, mengindikasikan bahwa tidak semua siswa yang memiliki sikap positif benar-benar mengimplementasikannya dalam perilaku nyata; temuan ini juga perlu dimaknai dengan kehati-hatian mengingat dimensi Behaviour hanya diukur melalui self-report. Korelasi Spearman antardimensi seluruhnya signifikan dengan korelasi A–B (rs=0,744) sebagai yang terkuat. Analisis mediasi formal (Sobel dan bootstrapping 5.000 resampel) mengonfirmasi bahwa Attitude memediasi secara parsial dan signifikan hubungan antara Knowledge dan Behaviour (efek tidak langsung ab=0,441; Sobel z=4,31; p<0,001; CI bootstrap 95%: 0,168–0,802), membuktikan secara empiris gagasan Ahamed et al. [7] pada konteks siswa SMK. Sebagai studi survei psikometrik pada Program Studi Rekayasa Keamanan Siber, penelitian ini diposisikan sebagai kajian kebutuhan berbasis bukti yang menjadi landasan bagi perancangan intervensi maupun kontrol keamanan teknis pada penelitian lanjutan, khususnya pada penguatan perilaku manajemen aplikasi dan izin akses smartphone di lingkungan SMK XYZ Bekasi. Keterbatasan generalisasi, desain cross-sectional, dan sifat self-report data Behaviour dijelaskan pada bagian Keterbatasan Penelitian.

Sebagai catatan reflektif, penelitian ini murni bersifat survei psikometrik pengukuran kesadaran (Knowledge, Attitude, Behaviour) dan tidak menghasilkan artefak rekayasa teknis seperti pembangunan sistem, tool, atau audit keamanan. Penulis menyadari bahwa kompetensi 'rekayasa' pada Program Studi Rekayasa Keamanan Siber idealnya diwujudkan melalui implementasi atau audit kontrol keamanan secara langsung. Posisi penelitian ini adalah sebagai tahap need assessment berbasis data empiris—memetakan area kelemahan perilaku spesifik (manajemen aplikasi pihak ketiga, penggunaan Wi-Fi publik,

keamanan layanan cloud) yang selanjutnya dapat menjadi dasar rancangan artefak teknis, misalnya: (1) modul pelatihan keamanan siber berbasis skenario yang divalidasi secara teknis; (2) sistem/tool audit otomatis izin aplikasi pada perangkat siswa sebagai pembanding data self-report; atau (3) kebijakan teknis manajemen akses aplikasi pihak ketiga yang dapat diuji efektivitasnya pada penelitian lanjutan. Dengan demikian, kontribusi rekayasa dari topik ini dipandang bersifat tidak langsung, yaitu sebagai fondasi bukti (evidence base) bagi rancangan solusi teknis, dan bukan solusi teknis itu sendiri.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak Muhammad Idris, S.Tr., M.Tr.Kom. selaku dosen pembimbing atas arahan dan bimbingannya, serta kepada seluruh siswa dan pihak SMK XYZ Bekasi yang telah berpartisipasi dalam penelitian ini. Terima kasih juga kepada Program Studi Rekayasa Keamanan Siber, Jurusan Teknik Informatika, Politeknik Negeri Batam atas dukungan akademis yang diberikan.

DAFTAR PUSTAKA

[1] We Are Social and Hootsuite, "Digital 2023: Indonesia," *We Are Social*, Jan. 2023. [Online]. Available: https://wearesocial.com/id/blog/2023/01/digital-2023-indonesia/

[2] M. Dimock, "Defining generations: Where millennials end and Generation Z begins," *Pew Research Center*, Jan. 2019. [Online]. Available: https://www.pewresearch.org/short-reads/2019/01/17/

[3] N. Adrian, D. F. Lindawaty, and Y. Kurniawan, "Indonesian Generation Z's awareness of data privacy in the use of social media," in *Proc. Int. Conf. Industrial Engineering and Operations Management (IEOM)*, Istanbul, Turkey, 2023. [Online]. Available: https://ieomsociety.org/proceedings/2022istanbul/318.pdf

[4] A. Nugraha, R. F. Sari, M. H. Yudhistira, and G. A. P. Saptawati, "Analysis of higher education students' awareness in Indonesia on personal data security in social media," *Sustainability*, vol. 15, no. 4, p. 3814, Feb. 2023, doi: 10.3390/su15043814.

[5] M. Zwilling, G. Klien, D. Lesjak, L. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82–97, 2022, doi: 10.1080/08874417.2020.1712269.

[6] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, June 2006, doi: 10.1016/j.cose.2006.02.008.

[7] B. Ahamed, M. R. H. Polas, A. I. Kabir, A. S. M. Sohel-Uz-Zaman, A. Al Fahad, S. Chowdhury, and M. R. Dey, "Empowering students for cybersecurity awareness management in the emerging digital era: The role of cybersecurity attitude," *SAGE Open*, vol. 14, no. 1, 2024, doi: 10.1177/21582440241228920.

[8] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*, 2nd ed. Bandung, Indonesia: Alfabeta, 2019.

[9] J. C. Nunnally, *Psychometric Theory*, 2nd ed. New York, NY, USA: McGraw-Hill, 1978.

[10] R. Likert, "A technique for the measurement of attitudes," *Arch. Psychol.*, vol. 22, no. 140, pp. 1–55, 1932.

[11] W. C. H. Hong and X. Xu, "How education level influences internet security knowledge, behaviour, and attitude: A comparison among undergraduates, postgraduates and working graduates," *Int. J. Inf. Secur.*, vol. 22, pp. 505–523, 2023, doi: 10.1007/s10207-022-00637-z.

[12] W. C. H. Hong, L. K. Cheong, and X. Xu, "The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates," *Educ. Inf. Technol.*, 2022, doi: 10.1007/s10639-022-11121-5.

[13] Republik Indonesia, *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Jakarta, Indonesia: Sekretariat Negara, 2022.