MEASURING THE LEVEL OF CYBERSECURITY AWARENESS OF SOCIAL MEDIA USERS AMONG STUDENTS

MENGUKUR TINGKAT KESADARAN CYBERSECURITY PADA PENGGUNA MEDIA SOSIAL DI KALANGAN MAHASISWA

Muhammad Agung Al Affan[1], Mona Fronita[2], Eki Saputra[3], Muhammad Luthfi Hamzah[4], Zarnelly[5]
[1,2,3,4,5] Universitas Islam Negeri Sultan Syarif Kasim, Jl. HR. Soebrantas No. 155 KM. 15, Panam, Riau
email : 12050313771@students.uin-suska.ac.id[1], monafronita@uin-suska.ac.id[2], eki.saputra@uin-suska.ac.id[3], Muhammad.luthfi@uin-suska.ac.id[4], zarnelly@uin-suska.ac.id[5]

Abstract *- The role of social media is increasingly important and easily accessible through mobile phones, slowly replacing conventional mass media. The development of Internet technology has made many users forget the importance of cybersecurity awareness, which impacts social media activities. As a result, cyber-attacks on social networks are now more frequent because many users still need help understanding cybersecurity well. Based on data BSSN, cyberattacks in Indonesia increased significantly from 290.3 million in 2019 to 495.3 million in 2020, representing a 41% rise. Social media users need to understand cybersecurity, a technology that protects data, networks, and programs from illegal access or digital attacks, known as cybercrime. Eighty-four respondents participated in the study. This study aims to measure the level of cybersecurity awareness and contribute to the existing literature by providing empirical insights into the level of cybersecurity awareness among university students. This study can also help raise awareness among the public, particularly young users, about the importance of protecting privacy and security while engaging in the digital world. This behaviour is measured using the five TPB variables: attitude, subjective form, perceived behaviour control, intention, and behaviour. Variables from TPB are then processed using SEM-PLS tools with the help of SmartPLS. Based on the study's results, it is concluded that the attitude and subjective form variables do not significantly affect the intention variable. In contrast, the perceived behaviour control variable significantly affects the intention variable, and the behaviour variable significantly affects intention.*
Keywords *- Cybersecurity, Cyberattacks, TPB, Social Media.*

Abstrak - Peran media sosial yang semakin penting dan mudah diakses melalui telepon seluler perlahan menggantikan media massa konvensional. Perkembangan teknologi internet membuat banyak pengguna melupakan pentingnya kesadaran keamanan siber, sehingga berdampak pada aktivitas media sosial. Akibatnya, serangan siber di jejaring sosial kini semakin sering terjadi karena masih banyak pengguna yang membutuhkan bantuan untuk memahami keamanan siber dengan baik. Berdasarkan data BSSN didapatkan bahwa meningkatnya serangan siber di Indonesia sebanyak 290,3 juta pada tahun 2019 menjadi 495,3 juta pada tahun 2020, meningkat sebanyak 41%. Pengguna media sosial perlu memahami keamanan siber, sebuah teknologi yang melindungi data, jaringan, dan program dari akses ilegal atau serangan digital, yang dikenal sebagai kejahatan dunia maya. Delapan puluh empat responden berpartisipasi dalam penelitian ini. Penelitian ini bertujuan untuk mengukur tingkat kesadaran kemananan siber dan berkontribusi pada literatur yang ada dengan memberikan wawasan empiris mengenai tingkat kesadaran keamanan siber di kalangan mahasiswa. Penelitian ini juga dapat membantu meningkatkan kesadaran masyarakat, khususnya pengguna muda, tentang pentingnya menjaga privasi dan keamanan saat beraktivitas di dunia digital. Perilaku ini diukur dengan menggunakan lima variabel TPB: sikap, bentuk subjektif, kontrol perilaku yang dirasakan, niat, dan perilaku. Variabel-variabel dari TPB selanjutnya diolah menggunakan *tools*SEM-PLS dengan bantuan SmartPLS. Berdasarkan hasil penelitian disimpulkan bahwa variabel sikap dan bentuk subjektif tidak berpengaruh signifikan terhadap variabel niat. Sebaliknya variabel kontrol perilaku yang dirasakan berpengaruh signifikan terhadap variabel niat, dan variabel perilaku berpengaruh signifikan terhadap niat.
Kata Kunci - *Cybersecurity, Cyberattacks, TPB, Social Media.*

I. PENDAHULUAN

Internet telah mengalami transformasi dari sekadar fasilitas pelengkap menjadi kebutuhan pokok dalam kehidupan masyarakat modern. Pergeseran perilaku masyarakat menuju digitalisasi semakin menegaskan hal ini. Baik anak-anak, dewasa, maupun lansia kini sangat bergantung pada internet dalam berbagai aspek kehidupan sehari-hari, menunjukkan bahwa akses internet telah menjadi kebutuhan dasar bagi semua kalangan [1]. Generasi milenial di Indonesia sangat erat kaitannya dengan dunia digital. Survei CSIS menunjukkan bahwa 81,7% dari mereka menggunakan Facebook, 70,3% menggunakan WhatsApp, dan 54,7% menggunakan Instagram setiap hari. Pertumbuhan pengguna media sosial yang mencapai 150 juta pada tahun 2019, seperti yang dilaporkan oleh We Are Social dan Hootsuite, semakin mengukuhkan peran penting media sosial dalam kehidupan mereka. Namun, insiden kebocoran data besar-besaran seperti yang dilakukan oleh Cambridge Analytica pada tahun 2018 menjadi pengingat akan pentingnya perlindungan data pribadi di tengah pesatnya perkembangan teknologi digital [2].

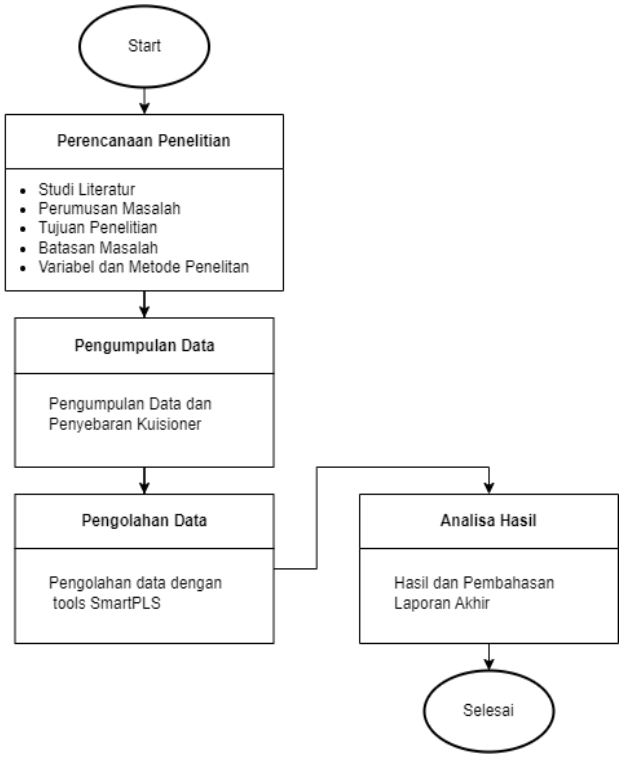
Penelitian ini mengadopsi *Theory of Planned Behavior* (TPB) dan *Technology Acceptance Model* (TAM) mengidentifikasi faktor-faktor kunci yang mempengaruhi penerimaan teknologi. Analisis ini berfokus pada enam dimensi utama, meliputi kemudahan penggunaan, kegunaan, sikap, norma sosial, kontrol perilaku, dan minat penggunaan teknologi [3]. Dengan menggunakan TPB, penelitian ini memiliki dasar teoritis yang mapan untuk menjelaskan perilaku mahasiswa terkait keamanan siber. Teori ini memungkinkan peneliti untuk tidak hanya mengukur perilaku, tetapi juga memahami faktor-faktor psikologis dan sosial yang mendorong atau menghambat perilaku tersebut, memberikan wawasan yang lebih mendalam untuk intervensi yang efektif. Internet telah menjadi bagian tak terpisahkan dari kehidupan modern. Dalam konteks penelitian, internet berfungsi sebagai alat utama untuk mengumpulkan data yang relevan [4]. Berkembangnya teknologi di Internet ini, hampir semua pengguna sudah melupakan kesadaran akan *cybersecurity*, yang tentunya sangat mempengaruhi aktivitas media sosial di Internet. Namun, masih banyak pengguna yang belum memahami dengan jelas *cybersecurity* di jejaring sosial, sehingga *cyberattack* semakin sering terjadi di jejaring sosial saat ini [5]. Pelaku kejahatan siber memanfaatkan perkembangan teknologi untuk melancarkan berbagai serangan, mulai dari penyebaran informasi palsu (hoaks), penipuan online, hingga pencurian data pribadi. Data Interpol menunjukkan bahwa serangan siber semakin canggih dan terorganisir, dengan target yang semakin beragam, termasuk sektor kesehatan, perusahaan, dan individu. Pandemi Covid-19 juga dimanfaatkan oleh para pelaku kejahatan siber untuk melancarkan serangan yang lebih terarah [6].

Cybersecurity ialah usaha yang dilakukan guna melindungi identitas pengguna dari ancaman atau akses ilegal [7]. Oleh karena itu, pemahaman mengenai *cybersecurity* menjadi sangat penting bagi pengguna media sosial untuk mencegah terjadinya pelanggaran data dan penyalahgunaan informasi pribadi [8]. C*yber* artinya dunia maya atau dunia internet dan *security* artinya keamanan. *Cybersecurity* mempunyai fungsi atau peran untuk mendeteksi, memperbaiki atau mengurangi tingkat risiko ancaman dan serangan siber serta aktivitas apa pun yang dapat mengancam keamanan seluruh komponen sistem jaringan itu sendiri, termasuk perangkat keras dan perangkat lunak, data. informasi dan infrastruktur [9]. Perlindungan terhadap jaringan perangkat ataupun program dari serangan siber,serta peretasan data pengguna merupakan tujuan dari *cybersecurity* [7]. Dengan berkembangnya teknologi informasi, berbagai jenis serangan siber, termasuk *malware* seperti *virus, worm, trojan horse, spyware, ransomware,* dan lainnya, telah muncul dan bervariasi [10]. *Ransomware* merupakan jenis malware yang dirancang untuk memfasilitasi berbagai aktivitas jahat, seperti mencegah akses ke data pribadi kecuali uang tebusan dibayarkan [11], *trojan horse* memasukkan program jahat ke aplikasi lain, seperti *virus, spyware, adware, keyloger*, dan *malware* lainnya untuk merusak dan mencuri data seperti kartu kredit dan *password* [12].

The British Law mendefinisikan *cybercrime* sebagai tindakan manipulasi komputer dengan tujuan jahat [13]. Sementara itu, definisi lain yang lebih umum mencakup segala aktivitas ilegal yang memanfaatkan komputer sebagai alat untuk melakukan kejahatan, termasuk di media sosial [14]. Platform media sosial telah menjadi ruang virtual utama bagi generasi Z untuk bersosialisasi [15]. Dapat diartikan bahwa media sosial merupakan perkembangan dari teknologi digital yang memudahkan seseorang untuk melakukan komunikasi dengan orang banyak tanpa perlu memikirkan batasan jarak lokasi [16]. Melalui media sosial, pengguna dapat dengan mudah menyebarkan konten. Seiring berkembangnya teknologi, pentingnya media sosial dan perannya meningkat pesat. Saat ini, jejaring sosial dapat dengan mudah diakses melalui ponsel. Dampak ini juga mulai sedikit demi sedikit menggantikan media massa konvensional (televisi, majalah, surat kabar, radio) dalam rangka penyebaran informasi [17].

Berdasarkan jumlah banyaknya pengguna Internet khususnya kalangan mahasiswa, peneliti melakukan penelitian ini guna mengukur tingkat kesadaran kemananan siber dan melihat kesenjangan pengetahuan spesifik yang dimiliki mahasiswa tentang *cybersecurity* dalam menggunakan internet dalam kesehariannya. Berfokusnya pada mahasiswa itu sangat penting dikarenakan mahasiswa merupakan salah satu kelompok yang paling aktif menggunakan sosial media dalam kehidupan sehari-hari, baik untuk tujuan akademik maupun personal. Temuan penelitian ini juga dapat digunakan untuk merancang program pendidikan atau pelatihan yang lebih efektif, dengan fokus pada area spesifik di mana mahasiswa memiliki kesenjangan pengetahuan atau perilaku yang kurang aman dalam hal keamanan siber.

II. SIGNIFIKASI STUDI



Gambar 1. Alur Metode Penelitian

Perancangan Penelitian

Pada tahapan ini peneliti melakukan studi literatur. Kemudian, mengidentifikasi fenomena riset untuk menjadi topik pembahasan pada penelitian ini serta perumusan masalah dan memperbanyak referensi yang berhubungan dengan topikatau isu yang akan diteliti. Setelah itu, menentukan tujuan dari target penelitian agar penelitian lebih terarah. Kemudian menentukan batasan pembahasan agar penelitian lebih terfokus pada pokok pembahasan dan menentukan variabel dan metode yang sesuai dengan topik penelitian.

Pengumpulan Data

Selanjutnya adalah tahap pengumpulan data, pada tahap ini menggunakan metode kuantitatif untuk meneliti tentang perilaku mahasiswa dalam bermedia sosial khususnya dari kacatama *cybersecurity*. Seluruh mahasiswa aktif Program Studi Sistem Informasi UIN Suska Riau menjadi target dalam pengumpulan data penelitian ini. Kuesioner yang disusun dalam bentuk Google Form telah disebarluaskan melalui berbagai media sosial untuk menjangkau responden secara efektif.

1) Polulasi dan Sampel

Penelitian ini melibatkan seluruh mahasiswa aktif program studi Sistem Informasi UIN Suska Riau sebagai populasi. Untuk memastikan bahwa sampel yang diambil dapat mewakili karakteristik populasi secara keseluruhan, peneliti menggunakan rumus Slovin. Rumus ini membantu dalam menentukan ukuran sampel yang sesuai dengan tingkat ketelitian yang diinginkan [18]. Berikut adalah rincian perhitungannya:

$$n = \frac{N}{1 + N\,e^2}$$
$$n = \frac{518}{1 + (518\ (0{,}01^2))}$$
$$n = \frac{518}{1 + (518\ (0{,}01))}$$
$$n = \frac{518}{1 + (5.18)}$$
$$n = \frac{518}{6.18}$$
$$n = 83{,}82$$
$$n \approx 84$$

"n = Jumlah sampel yang akan dicari"
"N = Jumlah populasi = 518 orang"
"e = Batas toleransi kesalahan (*error tolerance*)
= 10% atau 0.10 yang merupakan besaran kesalahan yang diharapkan atau ditetapkan"

Maka nilai sampel yang didapat sebesar 84 responden. Metode *random sampling* memberikan kesempatan yang sama untuk menjadi sampel dalam penelitian [19]. Penelitian ini mengumpulkan 84 sampel, masing-masing pria dan wanita. Dipilih 62 pria dan 22 wanita untuk berpartisipasi dalam penelitian.

2) Kuisoner Penelitian

Penyebaran kuesioner dilakukan untuk mengukur tingkat kesadaran dan perilaku Mahasiswa dalam menggunakan media sosial dari kacamata *cybersecurity*.

Tabel 1. Variabel dan Indikator

*Attitude towards cybersecurity (*AT)	AT1	Saya menganggap penting untuk menjaga keamanan informasi pribadi saya saat menggunakan sosial media
	AT2	Saya merasa pentingnya memahami resiko yang terkait dengan berbagai informasi pribadi di sosial media

	AT3	Saya serius menganggap ancaman keamanan seperti *phising/malware* saat menggunakan sosial media.
Subjective Norm (SN)	SN1	Saya setuju bahwa orang-orang disekitar saya menganggap penting untuk memperhatikan *cybersecurity* saat menggunakan sosial media
	SN2	Saya sering mendapatkan dukungan dari teman saya untuk meningkatkan keamanan akun sosial media saya
Perceived Behavior Control (PB)	PB1	Saya yakin bahwa saya dapat mengidentifikasi tautan yang mencurigakan/pesan yang berpotensi berbahaya di sosial media
	PB2	Saya setuju bahwa saya memiliki keterampilan yang diperlukan untuk mengelola pengaturan privasi dan keamanan akun sosial media saya dengan efektif
	PB3	Saya yakin bahwa saya dapat merespons dengan cepat dan tepat jika akun sosmed saya terkena ancaman keamanan
Intention (IN)	IN1	Saya berniat mempelajari *cybersecurity* dalam keseharian bersosial media
	IN2	Saya berniat untuk memverifikasi identitas pengirim sebelum membuka tautan atau lampiran yang diterima melalui pesan di media sosial
Behavior (BE)	BE1	Saya mempelajari mengenai *cybersecurity* melalui seminar-seminar terkait *cybersecurity*
	BE2	Saya mempraktikkan keamanan mengenai *cybersecurity* dengan sikap berhati-hati dalam bersosial media

Pengolahan Data

Pada tahap ini, data dikelompokkan dan disesuaikan sesuai dengan klasifikasi penelitian, seperti jumlah responden berdasarkan jenis kelamin, umur, dan penggunaan media sosial. Analisis lebih lanjut dilakukan menggunakan model persamaan struktural (SEM) melalui perangkat lunak SmartPLS. Perangkat lunak ini berguna untuk menguji hubungan antar variabel dan menghasilkan berbagai output statistik yang membantu dalam penyajian hasil penelitian.

Hipotesis Penelitian

H1 : *Attitude* (AT) mahasiswa berpengaruh terhadap *intention* (IN) mahasiswa dalam bermedia sosial.

H2 : *Subjective Norm* (SN) mahasiswa berpengaruh terhadap *intention* (IN) mahasiswa dalam bermedia sosial.

H3 : *Perceived Behavior Control* (PB) mahasiswa berpengaruh terhadap *Intention* (IN) mahasiswa dalam bermedia sosial.

H4 : *Intention* (IN) mahasiswa berpengaruh terhadap *Behavior* (BE) mahasiswa dalam bermedia sosial.

III. HASIL DAN PEMBAHASAN

Bab ini menjelaskan proses analisis data survei yang dilakukan berdasarkan pengunaan SmartPLS 4.0. Tahapan analisis meliputi pemeriksaan awal terhadap data, seperti distribusi responden berdasarkan demografi (jenis kelamin, usia, dan penggunaan media sosial). Selanjutnya, model pengukuran, model struktural, dan hipotesis penelitian akan diuji secara empiris.

Hasil Penyebaran Kuesioner

Mahasiswa aktif jurusan Sistem Informasi yang terlibat dalam penelitian ini dikumpulkan melalui kuesioner. Jumlah total kuesioner yang disebar berjumlah 84 dan dikirim dari 2 September 2024 hingga 27 September 2024, seperti yang disebutkan dalam bab 3 tentang jumlah responden yang akan digunakan. Adapun total kuesioner yang disebar ditunjukkan dalam Tabel 2.

Tabel 2. Jumlah Persebaran Kuisioner

Keterangan	Jumlah	Persentase
Kuisioner yang disebar	84	100%
Kuisioner yang dapat diolah	84	100%

Analisis Karakteristik Responden

Penelitian ini telah mengumpulkan sampel data dari 84 responden berdasarkan hasil survei, baik online maupun offline, dan mengirimkannya ke pengguna media sosial aktif di UIN Suska Riau. Ada sekitar 84 responden, dan mereka dikelompokkan berdasarkan kelamin, usia, dan penggunaan media sosial mereka dalam kehidupan sehari-hari.

1) Jenis Kelamin

Tabel 3 mempresentasikan distribusi frekuensi responden berdasarkan variabel demografis jenis kelamin :

Tabel 3. Kategori Responden Berdasarkan Jenis Kelamin

Jenis Kelamin	Jumlah	Persentase
Pria	62	74%
Wanita	22	26%
Total	84	100%

Berdasarkan data pada Tabel 3 profil responden penelitian ini didominasi oleh pria dengan jumlah 62 orang (74%). Sebaliknya, jumlah responden perempuan hanya 22 orang (26%). Dominasi responden laki-laki ini mengindikasikan bahwa penelitian ini lebih banyak melibatkan partisipasi dari populasi pria.

2) Usia

Tabel 4. Sebaran Usia Responden

Usia	Jumlah	Persentase
<18	2	2%
18-25	81	97%
25-30	1	1%

Analisis lebih lanjut terhadap karakteristik demografis responden pada Tabel 4 mengungkapkan temuan yang menarik. Sebanyak 97% dari total 84 responden tergolong dalam rentang usia 18-25 tahun atau setara dengan 81 orang, mengindikasikan bahwa penelitian ini memberikan gambaran yang mendalam mengenai perilaku penggunaan internet di kalangan generasi muda, khususnya mahasiswa. Konsentrasi pada kelompok usia ini memungkinkan untuk

mengidentifikasi tren dan pola penggunaan yang spesifik. jenis serangan siber yang pernah dialami.

3) Penggunaan Sosial Media

Tabel 5. Karakteristik Responden Menggunakan Sosial Media

Indikator	Jumlah	Persentase
Lama waktu mengakses sosial media		
<2 jam	11	13%
2-3 jam	29	35%
3-4 jam	22	26%
>5 jam	22	26%
Sosial media yang sering digunakan		
Facebook	15	18%
Instagram	10	12%
Whatsapp	12	14%
Tiktok	45	56%
Pernah mengalami serangan digital selama menggunakan sosial media		
Pernah	45	54%
Tidak Pernah	39	46%
Jenis serangan digital yang pernah dialami		
Phishing	31	70%
Malware	6	14%
Ransomware	1	2%
Denial of Service	6	14%

Berdasarkan Tabel 5, hasil demografi responden menunjukkan bahwa 56% responden paling sering menggunakan TikTok, diikuti oleh Facebook dengan 18%, WhatsApp dengan 14%, dan Instagram dengan 12%. Selain itu, 35% responden mengakses media sosial selama 2-3 jam, 26% selama 3-4 jam, dan 13% kurang dari 2 jam.

Pengujian Model Pengukuran *(Outer Model)*

Penelitian ini mengadopsi pendekatan *Structural Equation Model-Partial Least Squares* (SEM-PLS), yaitu suatu metode statistik yang memungkinkan kita untuk membangun dan menguji model-model yang kompleks. SEM-PLS sangat berguna dalam menganalisis hubungan sebab-akibat antar variabel laten dan variabel indicator [20]. Untuk mengukur validitas konstruk dan reliabilitas instrumen penelitian, dilakukan analisis pengukuran model menggunakan SmartPLS. Analisis ini mencakup empat tahap, yaitu: (1) reliabilitas item individu, (2) reliabilitas internal konsistensi, (3) variasi rata-rata yang terekstrak (*average variance extracted*/AVE), dan (4) validitas diskriminan. Hasil analisis dijabarkan dalam empat tahap di sini.

1) Uji *Individual Item Reability*

Loading factor adalah nilai yang dimiliki oleh setiap indikator, dan indikator dianggap valid jika nilainya di atas 0,7 [21].

Tabel 6. Uji Individual Item Reliability

Indikator	AT	BE	IN	PB	SN
AT1	0.923				
AT2	0.941				
AT3	0.888				
BE1		0.856			
BE2		0.891			
IN1			0.930		
IN2			0.928		
PB1				0.925	
PB2				0.898	
PB3				0.904	
SN1					0.927
SN2					0.905

Analisis *outer loading* menggunakan SmartPLS 4.0 terhadap 84 responden menunjukkan bahwa nilai *loading factor* seluruh indikator melebihi ambang batas 0,7. Hasil ini mengindikasikan semua indikator memiliki validitas yang baik dan dapat digunakan dalam analisis selanjutnya.

2) Uji *Internal Consistency Reliability*

Analisis reliabilitas internal menggunakan *Cronbach's Alpha* menunjukkan bahwa semua indikator penelitian memiliki nilai reliabilitas yang memadai ($\alpha > 0,7$). Hasil ini mengindikasikan bahwa item-item dalam setiap konstruk saling konsisten dan dapat diandalkan untuk mengukur konstruk laten yang bersangkutan.

Tabel 7. Hasil Uji *Composite Reliability*

Indikator	*Composite Reliability*
Attitude	0.941
Behavior	0.866
Intention	0.927
Perceived Behavior	0.935
Subjective Norm	0.912

3) Uji *Average Variance Extracted*

Average Variance Extracted (AVE) merupakan indikator penting untuk menilai validitas konvergen. Suatu konstruk laten dianggap valid jika nilai AVE-nya melebihi 0,5 yang berarti setidaknya 50% varians indikator dapat dijelaskan oleh konstruk tersebut [22].

Tabel 8. Hasil Uji *Average Variance Extracted*

Indikator	*Average Variance Extracted*
Attitude	0.863
Behavior	0.842
Intention	0.839
Perceived Behavior	0.827
Subjective Norm	0.763

Berdasarkan Tabel 8, semua konstruk penelitian memiliki nilai AVE di atas 0,50. Hal ini menunjukkan bahwa semua konstruk telah memenuhi kriteria validitas konvergen.

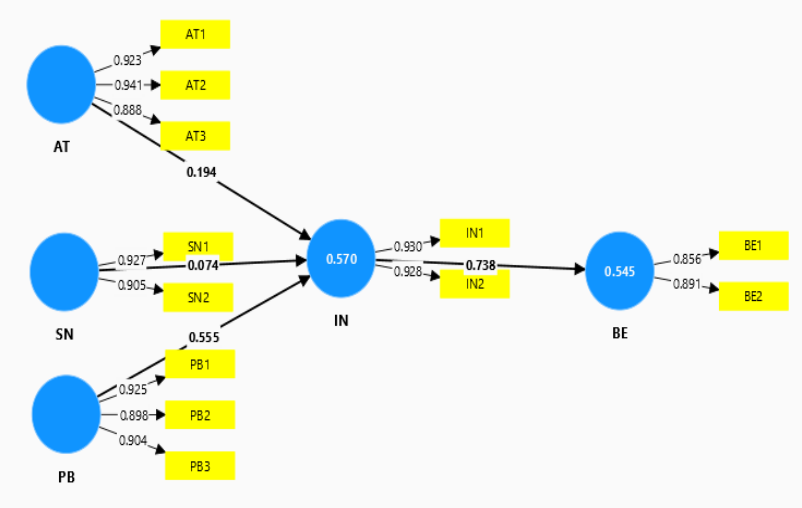
4) Uji *Discriminant Validity*

Analisis *cross loading* digunakan untuk menguji apakah suatu indikator lebih terkait dengan variabel laten yang seharusnya diukur dibandingkan dengan variabel laten lainnya. Jika nilai *loading* memenuhi kriteria tertentu dan nilai AVE juga memenuhi syarat, maka dapat disimpulkan bahwa variabel laten dalam model memiliki validitas diskriminan yang memadai.

Tabel 9. Uji *Cross Loading*

Indikator	AT	BE	IN	PB	SN
AT1	0.923	0.475	0.530	0.523	0.516
AT2	0.941	0.511	0.599	0.651	0.606
AT3	0.888	0.579	0.527	0.620	0.607
BE1	0.419	0.856	0.602	0.580	0.545
BE2	0.565	0.891	0.684	0.706	0.536
IN1	0.553	0.690	0.930	0.684	0.617
IN2	0.568	0.682	0.928	0.684	0.500
PB1	0.654	0.678	0.735	0.925	0.721
PB2	0.593	0.699	0.626	0.898	0.638
PB3	0.528	0.643	0.637	0.904	0.623
SN1	0.619	0.548	0.583	0.658	0.927
SN2	0.527	0.586	0.515	0.681	0.905

Analisis *cross loading* yang disajikan pada Tabel 9 mengkonfirmasi bahwa setiap indikator dalam model memiliki hubungan yang lebih kuat dengan konstruk yang diukur dibandingkan dengan konstruk lainnya. Temuan ini mengindikasikan bahwa masing-masing konstruk dalam model mengukur konsep yang berbeda dan tidak tumpang tindih.



Gambar 2. Hasil Analisis *Outer Model*

Analisis pengukuran model yang disajikan pada Gambar 2 menunjukkan bahwa indikator-indikator penelitian telah diukur dengan baik. Dengan demikian, model penelitian ini dapat dilanjutkan ke tahap pengujian hubungan antar konstruk (model struktural).

Pengujian Model Struktural *(Inner Model)*

Analisis menggunakan perangkat lunak SmartPLS 4 dilakukan untuk menguji seberapa kuat dan bagaimana arah hubungan antar konsep abstrak (variabel laten) yang telah diidentifikasi dalam penelitian ini.

1) Uji *Path Coeffiecients*

Hasil analisis menunjukkan bahwa keempat jalur hubungan dalam model penelitian ini signifikan secara statistik. Hal ini dapat dilihat pada Tabel 10, di mana nilai-nilai p (probabilitas) untuk semua jalur berada di bawah 0,05.

Tabel 10. Uji *Path Coefficients*

Hubungan Antar Variabel	*Path Coefficients*
AT → IN	0.194
IN → BE	0.738
PB → IN	0.555
SN → IN	0.074

2) *Uji Coefficient of Determination*

Koefisien determinasi digunakan untuk mengukur seberapa baik model mampu menjelaskan variasi dalam variabel dependen. Nilai ini dianggap kuat jika di atas 0,75, sedang jika berada antara 0,50 dan 0,75, dan lemah jika di bawah 0,50 [23].

Tabel 11. Uji *Coeffiecient of Determination*

Variabel Endogen	*R-Square*
BE	0.539
IN	0.554

Hasil analisis menunjukkan bahwa model mampu menjelaskan 55,4% varians dalam niat pengguna (IN) dan 53,9% varians dalam perilaku pengguna (BE). Artinya, variabel sikap, norma subjektif, dan kontrol perilaku secara bersama-sama memberikan kontribusi yang moderat terhadap niat dan perilaku pengguna. Sisanya, masing-masing 44,6% dan 46,1% varians dapat dijelaskan oleh faktor-faktor lain yang tidak termasuk dalam model ini.

3) Pengujian Hipotesis

Setelah model pengukuran dan struktural dinyatakan valid, langkah selanjutnya adalah pengujian hipotesis. Untuk menguji signifikansi pengaruh antar variabel, analisis PLS digunakan. Hipotesis penelitian diterima jika nilai t-statistik yang dihasilkan lebih besar dari nilai t-tabel pada tingkat signifikansi 5% (biasanya sekitar 1,96).

Tabel 12. Hasil Uji Hipotesis

Hipotesis	T-Tabel	T-Statistics	*P Values*	Keterangan
H1: AT Terhadap IN	1.96	1.605	0.109	Tidak Signifikan
H2: IN Terhadap BE	1.96	9.846	0.000	Signifikan
H3: PB Terhadap IN	1.96	4.236	0.000	Signifikan
H4: SN Terhadap IN	1.96	0.515	0.607	Tidak Signifikan

Pengujian hipotesis menggunakan metode *bootstrapping* menunjukkan hasil sebagai berikut. Pengujian signifikansi hubungan antar variabel dilakukan dengan membandingkan nilai t-statistik yang diperoleh dengan nilai t-tabel pada taraf signifikansi 5%. Jika nilai t-statistik lebih besar dari nilai t-tabel dan nilai p kurang dari 0,05, maka hipotesis nol ditolak dan dapat disimpulkan bahwa terdapat pengaruh yang signifikan. Hasil uji hipotesis pada Tabel 12 menunjukkan bahwa :

- Hipotesis 1 (H1) ditolak. Variabel sikap terhadap perilaku (AT) tidak memiliki pengaruh signifikan terhadap niat perilaku (IN). Hal ini ditunjukkan oleh nilai t-statistik yang lebih rendah dari 1,96 dan nilai p sebesar 0,109 yang lebih besar dari 0,05.
- Hipotesis 2 (H2) diterima. Variabel niat perilaku (IN) memiliki pengaruh signifikan terhadap perilaku (BE). Nilai t-statistik yang diperoleh lebih besar dari nilai t-tabel dan nilai p kurang dari 0,05.

- Hipotesis 3 (H3) diterima. Variabel kontrol perilaku (PB) juga memiliki pengaruh signifikan terhadap niat perilaku (IN). Nilai t-statistik dan nilai p yang diperoleh mendukung penerimaan hipotesis ini.
- Hipotesis 4 (H4) ditolak: Tidak terdapat pengaruh signifikan antara norma subjektif (SN) dan niat perilaku (IN). Nilai t-statistik yang diperoleh lebih rendah dari nilai kritis dan nilai p-value lebih besar dari 0,05.

IV. KESIMPULAN

Perilaku mahasiswa dalam kesehariannya yang diukur menggunakan *Theory of Planned Behavior* dan SEM-PLS dalam analisisnya dapat disimpulkan bahwa variabel niat dalam penggunaan sosial media pada mahasiswa tidak memiliki keterkaitan dengan variabel sikap terhadap perilaku dari mahasiswa dan juga variabel subjektif norma. Dari keterangan ini, dapat disimpulkan bahwa niat mahasiswa dalam penggunaan sosial media tidak akan mengalami peningkatan ataupun penurunan karena mahasiswa tidak mendapatkan dukungan dari lingkungan sekitar yang bisa memberikan pengaruh terhadap sikap mahasiswa dalam menggunakan sosial media. Sementara niat mahasiswa dalam menggunakan sosial media dipengaruhi oleh variabel kontrol perilaku secara signifikan, dimana hal ini merepresentasikan tingginya niat dari mahasiswa dalam penggunaan sosial media dipengaruhi oleh tingginya kontrol terhadap perilaku maupun kepercayaan dalam penggunaan sosial media.

Dari simpulan diatas, dapat dipahami dilihat dari kacamata *cybersecurity* bahwa niat untuk perlindungan diri dari *cyberattack* dipengaruhi oleh seberapa besar tingkat kontrol perilaku maupun kepercayaan dari mahasiswa dalam menggunakan sosial media sebelum membuka tautan atau lampiran yang diterima melalui pesan di media sosial. Hasil penelitian ini mendukung temuan dari penelitian sebelumnya yang menunjukkan bahwa kesadaran keamanan siber sering kali dipengaruhi oleh tingkat literasi digital individu. Hasil penelitian ini juga memperkuat pandangan bahwa edukasi adalah elemen kunci untuk meningkatkan kesadaran keamanan siber untuk melindungi privasi dari serangan siber di kalangan mahasiswa. Hasil penelitian ini dapat dimanfaatkan oleh lembaga pendidikan untuk merancang program pelatihan dan kampanye yang meningkatkan kesadaran keamanan siber mahasiswa, seperti modul literasi digital, workshop simulasi serangan *phishing*, atau integrasi keamanan siber dalam kurikulum. Tindakan ini tidak hanya meningkatkan kesadaran tetapi juga menciptakan lingkungan digital yang lebih aman bagi pengguna media sosial.

REFERENSI

[1] R. Riyandhika and R. Pratama, “Analisis Kesadaran Cybersecurity pada Kalangan Mahasiswa di Indonesia,” *Uii*, vol. 1, no. 2, p. 1, 2020.

[2] M. B. Yel and M. K. M. Nasution, “Keamanan informasi data pribadi pada media sosial,” *J. Inform. Kaputama*, vol. 6, no. 1, pp. 92–101, 2022.

[3] L. Chen and X. Yang, “Using EPPM to Evaluate the Effectiveness of Fear Appeal Messages Across Different Media Outlets to Increase the Intention of Breast Self-Examination Among Chinese Women,” *Health Commun.*, vol. 34, no. 11, pp. 1369–1376, 2019, doi: 10.1080/10410236.2018.1493416.

[4] Tedyyana, Agus, Osman Ghazali, and Onno Purbo. "Model Design of Intrusion Detection System on Web Server Using Machine Learning Based." *Proceedings of the 11th International Applied Business and Engineering Conference, ABEC 2023, September 21st, 2023, Bengkalis, Riau, Indonesia*. 2024..

[5] V. A. Kairupan and A. A. Rahman, "ANALISIS KESADARAN CYBERSECURITY PADA PENGGUNA MEDIA SOSIAL DI KALANGAN MAHASISWA KOTA BANDUNG," *J. Darma Agung*, 2022.

[6] A. Kusumaningrum, H. Wijayanto, and B. D. Raharja, "Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat Study From Home dengan Multiple Criteria Decision Analysis (MCDA)," *J. Ilm. SINUS*, vol. 20, no. 1, p. 69, 2022, doi: 10.30646/sinus.v20i1.586.

[7] A. Y. I. Mauliza, R. D. S. Machmudi, and R. Indrarini, "PENGARUH PERLINDUNGAN DATA DAN CYBER SECURITY," *J. Ilm. Bid. Sos. Budaya , Teknol. dan Pendidik.*, vol. 1, no. 11, pp. 2497–2516, 2022.

[8] P. Wahib *et al.*, "Sosialisasi Cyber Security Untuk Meningkatkan Literasi Digital," *Abdi J. Publ.*, vol. 1, no. 2, pp. 64–68, 2022, [Online]. Available: https://jurnal.portalpublikasi.id/index.php/AJP/index

[9] M. Ramadhani and P. A. Raf, "Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia," *Automata*, vol. Vol. 1 No., 2020.

[10] Z. Fuada, "PENERAPAN KEAMANAN JARINGAN MENGGUNAKAN SISTEM SNORT DAN HONEYPOT SEBAGAI PENDETEKSI DAN PENCEGAH MALWARE," *J. FTK. PTI*, 2023.

[11] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Comput. Secur.*, vol. 111, p. 102490, 2021, doi: 10.1016/j.cose.2021.102490.

[12] M. A. H. Nasution and A. T. Laksono, "Investigasi Serangan Backdoor Remote Access Trojan (RAT) Terhadap Smartphone," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 4, pp. 505–510, 2020, doi: 10.30865/jurikom.v7i4.2301.

[13] F. Kwarto and M. Angsito, "Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan," *J. Akunt. Bisnis*, vol. 11, no. 2, pp. 99–110, 2018, doi: 10.30813/jab.v11i2.1382.

[14] M. Herlina and S. Husada, "Dampak Kejahatan Cyber dan Informasi Hoax Terhadap Kecemasan Remaja di Media Online The Impact of Cyber Crime and Hoax Information on Teenage Anxiety in Online Media," *J. Promedia (Publik Commun. dan Media Komunikasi)*, vol. Vol. 5 No., no. 2, pp. 89–110, 2019.

[15] A. Pujiono, "Media Sosial Sebagai Media Pembelajaran Bagi Generasi Z," *Didache J. Christ. Educ.*, vol. 2, no. 1, p. 1, 2021, doi: 10.46445/djce.v2i1.396.

[16] G. L. A. Kusuma Putra and G. P. P. A. Yasa, "Komik Sebagai Sarana Komunikasi Promosi Dalam Media Sosial," *J. Nawala Vis.*, vol. 1, no. 1, pp. 1–8, 2019, doi: 10.35886/nawalavisual.v1i1.1.

[17] Malahayati and F. Darul, "ANALISIS KEAMANAN INFORMASI PENGGUNA MEDIA SOSIAL," *J. Inf. Technol. Res.*, vol. 2, no. 1, pp. 21–28, 2021.

[18] M. Rizki, M. Arhami, and H. Huzeni, "Perbaikan Algoritma Naive Bayes Classifier Menggunakan Teknik Laplacian Correction," *J. Teknol.*, vol. 21, no. 1, p. 39, 2021, doi: 10.30811/teknologi.v21i1.2209.

[19] S. Muntahanah, H. Cahyo, H. Setiawan, and S. Rahmah, "Literasi Keuangan, Pendapatan dan Gaya Hidup terhadap Pengelolaan Keuangan di Masa Pandemi," *J. Ilm. Univ. Batanghari Jambi*, vol. 21, no. 3, p. 1245, 2021, doi: 10.33087/jiubj.v21i3.1647.

[20] Rensya Siwalette dkk, "Analisi Faktor-Faktor Yang Berpengaruh Terhadap Pembelian Secara Online Di Kota Ambon Menggunakan Metode Structural Equation Modeling - Partial Least Square (SEM-PLS) (Analysis Of Factors That Influence Online Shopping in The City of Ambon Using Struc," *J. Stat. its Appl.*, vol. 4, pp. 57–64, 2022.

[21] Z. Dhaefina, M. A. Nur, V. F. Sanjaya, and I. Artikel, "Pengaruh Celebrity Endorsment, Brand Image dan Testimoni terhadap Minat Beli Konsumen Produk Mie Lemonilo pada Media Sosial Intagram," *J. Manaj.*, vol. 7, no. 1, pp. 43–48, 2021, [Online]. Available: http://ejournal.lmiimedan.net

[22] E. Wulandari and I. Murniawaty, "Peningkatan Keunggulan Bersaing Melalui Diferensiasi Produk Dan Diferensiasi Citra Serta Pengaruhnya Terhadap Kinerja Pemasaran Ikm Kopi Di Kabupaten Temanggung," *J. Manaj. Pemasar.*, vol. 13, no. 2, pp. 69–77, 2019, doi: 10.9744/pemasaran.13.2.69-77.

[23] N. Z. Fikar, "Analisis Penggunaan Pengguna Aplikasi Gopay Menggunakan Model UTAUT 2 dengan Extended Variable," p. 99, 2024.