Full Paper

Analisis Perkembangan Teknologi Keamanan Jaringan Untuk Mencegah Cyber Crime

Rati Elmiyanti[1], Andhika Dwi Pramudya[2], Lucky Edward[3], Muhammad Khairul Hisan[4], Hoddy Halomoan Manalu[5]

[1,2,3,4,5]Program Studi Teknik Komputer, Institut Teknologi Batam, Indonesia

Informasi Artikel

Terbit: Juli 2026

Kata Kunci:

Keamanan jaringan, cybercrime, Artificial Intelligence (AI), kesadaran siber, kebijakan keamanan.

ABSTRAK

Penelitian ini menganalisis perkembangan teknologi keamanan jaringan dan perannya dalam mencegah cybercrime dengan meninjau faktor kesadaran pengguna, kebijakan, dan teknologi modern seperti Artificial Intelligence (AI). Menggunakan metode deskriptif kuantitatif melalui survei terhadap 50 responden (mahasiswa, dosen, dan praktisi TI), penelitian ini mengukur lima dimensi utama keamanan menggunakan skala Likert. Hasil analisis menunjukkan tingkat kesadaran dan persepsi positif yang sangat tinggi dengan rata-rata skor di atas 4.0 pada seluruh dimensi, di mana dimensi kesadaran ancaman memperoleh skor tertinggi (4.31) dan teknologi keamanan lanjutan memperoleh skor terendah (4.04). Penelitian menyimpulkan bahwa faktor manusia, edukasi, dan kebijakan pemerintah krusial dalam pertahanan siber, sementara penerapan AI sangat potensial untuk memperkuat keamanan asalkan diimbangi dengan regulasi dan kesadaran etis guna memitigasi risiko baru di era digital.

Corresponding Author:

Rati Elmiyanti
Email: 2322013@student.iteba.ac.id

1. PENDAHULUAN

Perkembangan globalisasi dan kemajuan pesat Teknologi Informasi dan Komunikasi (TIK) di era digital telah menjadi pendorong utama transformasi sosial, ekonomi, dan budaya[1].

Namun, kemajuan ini juga menciptakan dampak negatif berupa munculnya bentuk-bentuk aktivitas kriminal yang canggih, yang dikenal sebagai cybercrime[2]. Cybercrime adalah tindakan kriminal yang melanggar hukum yang menggunakan teknologi komputer, jaringan internet, atau sistem informasi sebagai alat atau target kejahatan[1] [3]

Indonesia menghadapi ancaman siber yang serius. Negara ini dilaporkan menempati peringkat ketiga di dunia dengan jumlah kasus kejahatan siber tertinggi [4], Dengan lebih dari 78,4% populasi Indonesia telah menggunakan internet[5], adopsi masif media digital dan e-commerce telah memperluas permukaan serangan, membuat individu, institusi finansial, hingga infrastruktur pemerintah menjadi sangat rentan.

Jenis ancaman telah berevolusi dari sekadar hacking konvensional menjadi serangan yang lebih terstruktur dan merusak, seperti Distributed Denial of Service (DDoS) [4], ransomware, dan penipuan berbasis rekayasa sosial (phishing)[6].

Urgensi penelitian ini didasarkan pada kesenjangan antara kecepatan adopsi teknologi dan kesiapan pertahanan siber di Indonesia. Meskipun telah dilakukan upaya regulatif melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan pembentukan lembaga seperti Badan Siber dan Sandi Negara (BSSN)[5], penegakan hukum dan efektivitas pencegahan masih menghadapi tantangan besar, terutama masalah literasi digital dan SDM[4] [1]. Oleh karena itu, analisis mendalam terhadap teknologi keamanan jaringan yang berkembang (seperti firewall dan biometrik)[3] [7]dan implementasinya, serta keterkaitannya

dengan upaya mitigasi risiko dan kerangka hukum[8], menjadi krusial untuk merumuskan strategi penanggulangan cybercrime yang efektif dan berkelanjutan[9]. Penelitian ini secara spesifik berupaya menguji persepsi mahasiswa[10], Institut Teknologi Batam ITEBA sebagai kelompok terpelajar dan pengguna teknologi tinggi terhadap isu-isu ini.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kuantitatif, dengan dukungan pendekatan literatur dan hukum normatif untuk memperkuat landasan teoritis dan regulatif yang terkait dengan keamanan jaringan dan pencegahan cybercrime.

Selain kajian literatur, penelitian ini juga menerapkan metode survei berbasis kuesioner untuk memperoleh data primer dari responden mengenai persepsi, tingkat kesadaran, serta pandangan mereka terhadap ancaman cybercrime dan teknologi keamanan jaringan yang digunakan.

Instrumen penelitian berupa kuesioner yang terdiri atas 20 pernyataan dengan skala Likert 1–5, yaitu:

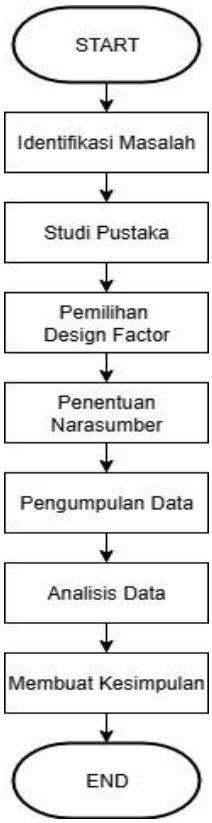
1 = Sangat Tidak Setuju (STS)
2 = Tidak Setuju (TS)
3 = Netral (N)
4 = Setuju (S)
5 = Sangat Setuju (SS)

Responden dalam penelitian ini berjumlah 50 orang, terdiri atas mahasiswa, tenaga IT, dan dosen yang memiliki pengalaman dalam penggunaan layanan digital dan sistem jaringan.

Data yang diperoleh kemudian dianalisis menggunakan metode analisis deskriptif kuantitatif, dengan menghitung:

- Nilai rata-rata (Mean) untuk mengetahui kecenderungan umum setiap dimensi,
- Modus untuk melihat nilai yang paling sering muncul, dan
- Persentase kesepakatan (Setuju & Sangat Setuju) untuk menggambarkan persepsi dominan responden terhadap setiap indikator.

Tahapan penelitian dilakukan secara sistematis sebagaimana ditunjukkan pada gambar berikut:



Gambar 1. Tahapan Metode Penelitian

1. Identifikasi Masalah
   Menentukan permasalahan utama terkait peningkatan ancaman *cybercrime* dan kebutuhan akan keamanan jaringan yang lebih kuat.
2. Studi Literatur dan Analisis Teoretis
   Melakukan kajian terhadap teori, penelitian terdahulu, serta regulasi yang relevan untuk membangun kerangka konseptual penelitian.
3. Perancangan Instrumen Penelitian (Kuesioner)
   Menyusun indikator pertanyaan berdasarkan dimensi kesadaran keamanan, kebijakan, teknologi tradisional, dan teknologi lanjutan.
4. Pengumpulan Data (Survei Responden)
   Menyebarkan kuesioner kepada responden melalui media daring untuk memperoleh data primer.
5. Pengolahan dan Analisis Data
   Mengolah data kuesioner menggunakan analisis deskriptif kuantitatif untuk menilai persepsi dan kesadaran keamanan siber.
6. Interpretasi Hasil
   Menafsirkan hasil analisis untuk memahami tingkat kesadaran, peran teknologi, dan efektivitas kebijakan keamanan siber.
7. Kesimpulan
   Menyusun hasil akhir penelitian berdasarkan temuan utama dan memberikan rekomendasi terkait peningkatan keamanan jaringan.

3. HASIL DAN ANALISIS

3.1 *Analisis Dimensi dan Skor Rata-Rata (Mean)*

Berdasarkan hasil pengolahan data dari 50 responden, diperoleh rata-rata skor per dimensi sebagai berikut:

Tabel 1. *Design Factor* 1: *Enterprise Strategy*

Dimensi Analisis	Nomor Pertanyaan	Skor Rata-Rata	Jumlah Pertanyaan
Kesadaran/Persepsi Ancaman	1, 2, 10, 12	4.31	4
Peran Eksternal/Edukasi	14, 15	4.22	2
Kebijakan/Manajemen Keamanan	11, 13, 18, 20	4.155	4
Teknologi Keamanan Tradisional	4, 6, 7, 16	4.08	4
Teknologi Keamanan Lanjutan/Baru	3, 5, 8, 9, 17, 19	4.0367	6

Semua dimensi memperoleh skor di atas 4.0, menandakan tingkat kesadaran dan kepercayaan yang tinggi terhadap pentingnya keamanan jaringan.

Berdasarkan analisis ini memperlihatkan lima kategori dengan skor rata-rata masing-masing (skala 1–5):

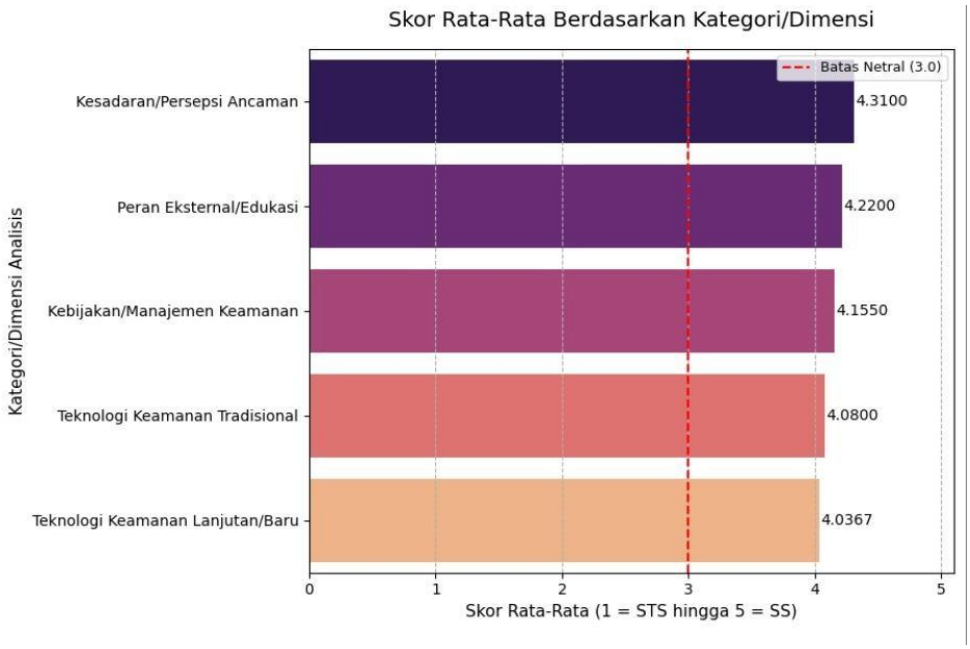
1.3 Analisis Kategori/Dimensi Skor Rata-Rata (Berdasarkan 50 Responden)

Dimensi Analisis	Nomor Pertanyaan (1-20)	Skor Rata-Rata	Jumlah Pertanyaan
Kesadaran/Persepsi Ancaman	1, 2, 10, 12	4.31	4
Peran Eksternal/Edukasi	14, 15	4.22	2
Kebijakan/Manajemen Keamanan	11, 13, 18, 20	4.155	4
Teknologi Keamanan Tradisional	4, 6, 7, 16	4.08	4
Teknologi Keamanan Lanjutan/Baru	3, 5, 8, 9, 17, 19	4.0367	6

Gambar 1. Analisis Kategori/Dimensi Skor Rata-Rata berdasarkan 50 Responden

1. Kesadaran/Persepsi Ancaman - 4.3100
2. Peran Eksternal/Edukasi - 4.2200
3. Kebijakan/Manajemen Keamanan - 4.1550
4. Teknologi Keamanan Tradisional - 4.0800
5. Teknologi Keamanan Lanjutan/Baru - 4.0367

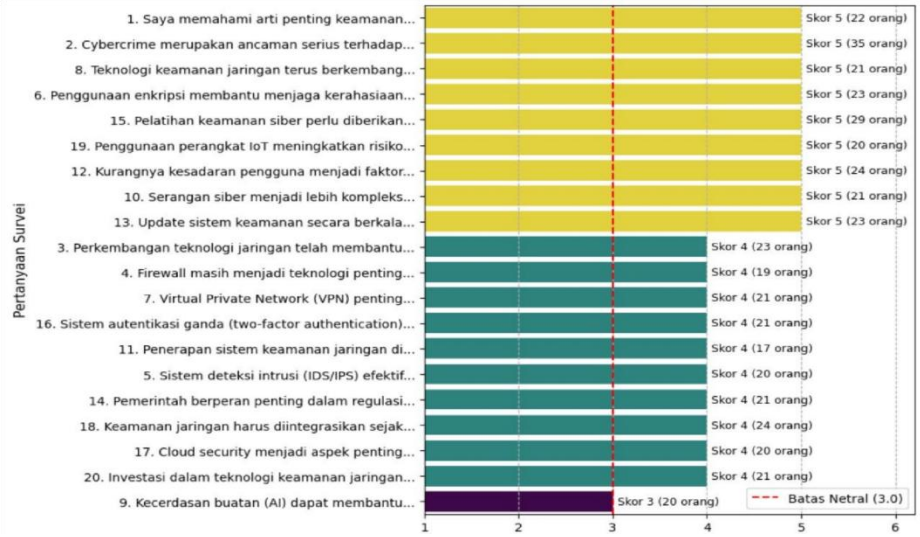
Terdapat juga garis vertikal merah bertanda "Batas Netral (3.0)", menunjukkan bahwa semua nilai berada di atas batas netral, artinya responden secara umum memiliki pandangan positif terhadap keamanan jaringan dan pencegahan cybercrime di setiap dimensi yang diukur.



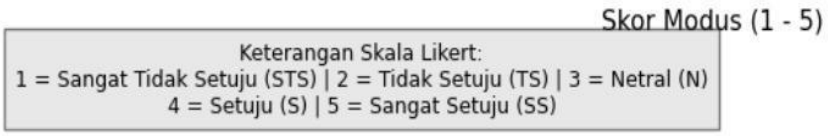
Gambar 2. Grafik Analisis Dimensi dan Skor Rata-Rata (Mean)

3.2 Analisis Modus (Skor yang Paling Sering Dipilih)

Sebagian besar responden memberikan skor 5 (Sangat Setuju) pada 13 dari 20 pernyataan, terutama yang berkaitan dengan kesadaran akan pentingnya keamanan, pelatihan siber, dan ancaman cybercrime.



Gambar 3. Grafik Analisis Modus



Gambar 4. Diagram Skor Modus per Pertanyaan

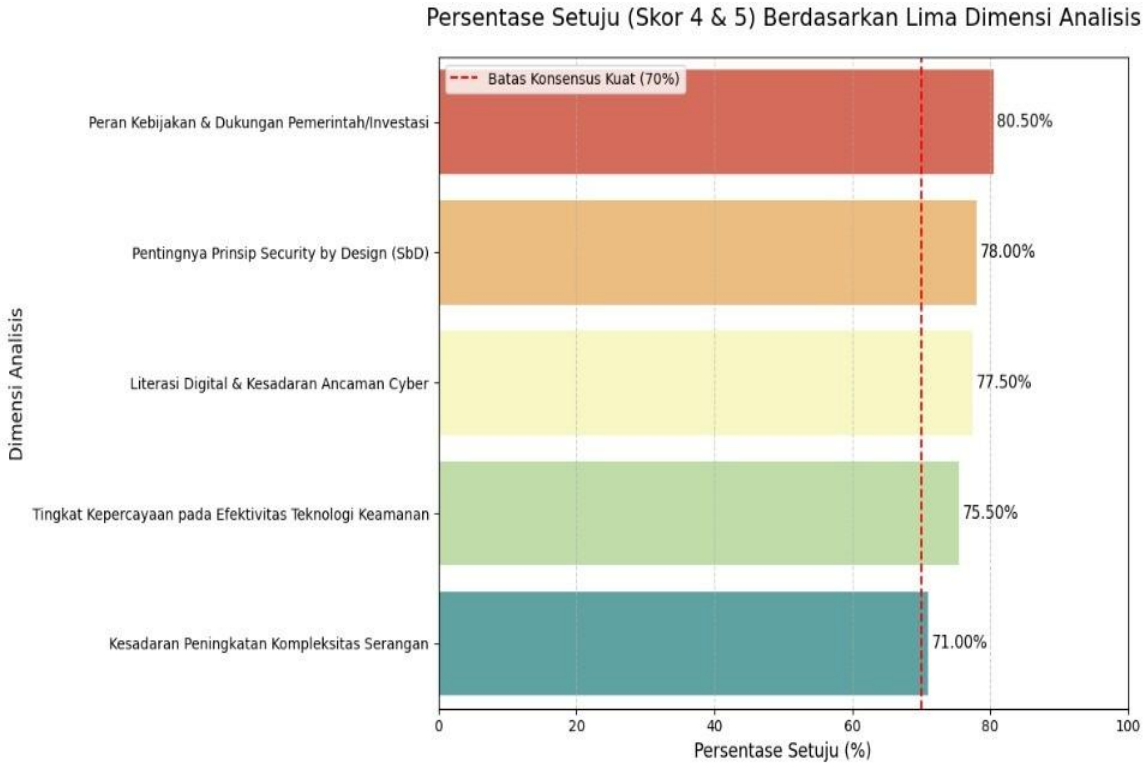
3.3 Persentase Tingkat Kesepakatan (Setuju & Sangat Setuju)

Berdasarkan analisis persentase jawaban (skor 4 dan 5), kelima dimensi menunjukkan tingkat konsensus yang melampaui batas kuat (70%), dengan rincian sebagai berikut:

Dimensi Analisis	Persentase Setuju (4 & 5)
Peran Kebijakan & Dukungan Pemerintah/Investasi	**80.5%**
Prinsip Security by Design (SbD)	**78.0%**
Literasi Digital & Kesadaran Ancaman Cyber	**77.5%**
Efektivitas Teknologi Keamanan	**75.5%**
Kesadaran Peningkatan Kompleksitas Serangan	**71.0%**

Tabel 2. Dimensi Analisis Persentase Tingkat Kesepakatan

Semua dimensi melewati ambang 70%, yang berarti terdapat konsensus kuat bahwa keamanan jaringan memerlukan dukungan kebijakan, peningkatan literasi, dan adopsi teknologi keamanan efektif.



Gambar 4. Grafik Persentase Setuju Berdasarkan Lima Dimensi

3.4 Interpretasi Hasil

Berdasarkan hasil analisis data dan grafik skor rata-rata per dimensi, dapat diinterpretasikan bahwa:

1. Tingkat kesadaran dan persepsi terhadap keamanan jaringan berada pada kategori sangat tinggi dengan nilai rata-rata di atas 4.0. Hal ini menunjukkan bahwa mayoritas responden memiliki pemahaman yang baik tentang pentingnya keamanan jaringan dan dampak serius dari ancaman cybercrime.
2. Faktor manusia dan edukasi keamanan siber masih menjadi fokus utama dalam peningkatan perlindungan jaringan. Meskipun teknologi keamanan terus berkembang, efektivitas sistem tetap sangat bergantung pada perilaku, kesadaran, dan kepatuhan pengguna terhadap prinsip-prinsip keamanan digital.
3. Teknologi berbasis kecerdasan buatan (AI) dinilai memiliki potensi besar dalam memperkuat sistem keamanan jaringan. Namun demikian, sebagian responden masih menunjukkan sikap hati-hati dan skeptis terhadap risiko baru yang mungkin timbul, seperti kerentanan data dan penyalahgunaan sistem otomatis.
4. Dukungan kebijakan pemerintah dan penerapan manajemen keamanan yang komprehensif dianggap sebagai faktor penting dalam menjaga ketahanan sistem digital nasional. Adanya regulasi yang tegas, program literasi digital, dan kolaborasi lintas sektor dapat memperkuat kemampuan pencegahan dan penanggulangan cybercrime di Indonesia.

5. KESIMPULAN

Berdasarkan hasil analisis data kuesioner dan interpretasi hasil penelitian, dapat disimpulkan bahwa:

1. Tingkat kesadaran terhadap keamanan jaringan tergolong sangat tinggi. Hal ini dibuktikan dengan nilai rata-rata keseluruhan dimensi di atas 4.0, menunjukkan bahwa sebagian besar responden memahami pentingnya menjaga keamanan sistem digital dan potensi ancaman dari cybercrime.
2. Faktor manusia dan edukasi keamanan siber merupakan elemen utama dalam pencegahan cybercrime. Meskipun teknologi keamanan terus berkembang, keberhasilan perlindungan jaringan sangat bergantung pada perilaku pengguna, disiplin penerapan kebijakan, dan peningkatan literasi digital.
3. Teknologi keamanan modern seperti AI (Artificial Intelligence) mulai mendapat perhatian, namun masih terdapat keraguan dalam penerapannya karena potensi risiko baru yang muncul. Hal ini menunjukkan perlunya penelitian lanjutan dan pengembangan strategi penerapan teknologi secara aman dan etis.
4. Peran pemerintah, lembaga pendidikan, dan organisasi sangat penting dalam membangun sistem keamanan siber nasional yang tangguh. Dukungan berupa regulasi, program pelatihan, dan kebijakan perlindungan data diperlukan agar upaya pencegahan cybercrime berjalan lebih efektif dan berkelanjutan.
5. Secara keseluruhan, hasil penelitian ini menegaskan bahwa kombinasi antara kesadaran pengguna, penerapan teknologi yang tepat, dan dukungan kebijakan yang kuat menjadi fondasi utama dalam memperkuat keamanan jaringan dan mencegah kejahatan siber di era digital.

DAFTAR PUSTAKA

[1] R. D. Hapsari and K. G. Pambayun, “ANCAMAN CYBERCRIME DI
[2] INDONESIA: Sebuah Tinjauan Pustaka Sistematis,” *Jurnal Konstituen*, vol. 5, no. 1, pp. 1–17, Oct. 2023, doi: 10.33701/jk.v5i1.3208.
[3] D. R. Akhiruddin and T. Sutabri, “ANALISIS PENINGKATAN KEAMANAN
[4] PADA SIMPLE NETWORK TIME PROTOCOL (SNTP) UNTUK
[5] MENDETEKSI CYBERCRIME DALAM AKTIFITAS JARINGAN
[6] MENGGUNAKAN METODE FIREWALL,” *Blantika : Multidisciplinary Jornal*, vol. 2, no. 1, p. 2023, [Online]. Available: https://blantika.publikasiku.id/141

[7] R. Kuswulandari, A. Wirid, I. Jowanka, T. Nabila, P. Riyanto, and T. Listiani, “Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Aplikasi Whatsapp.”
[8] T. Digital, K. Siber, : Upaya, P. Kejahatan Di Era, and M. A. Djibu, “Transformasi Digital dan Keamanan Siber: Upaya Penanggulangan Kejahatan di Era Teknologi di Indonesia,” *Judge : Jurnal Hukum*, vol. 06, 2025, doi:
[9] 10.54209/judge.v6i01.1182.
[10] U. Muhammadiyah Kotabumi PENGARUH KEMAJUAN TEKNOLOGI TERHADAP PERKEMBANGAN TINDAK PIDANA CYBERCRIME, I.
[11] Yurita, M. Kevin Ramadhan, M. Candra, and U. Muhammadiyah Kotabumi, “,2,3).”
[12] A. Ancaman Cybercrime dan, F. Yustinne Nadhotul Sufi, D. Kharisma Putri, D. Suhartini, U. Pembangunan Nasional, and J. Timur, “Analisis Ancaman Cybercrime dan Peran Sistem Biometrik: Systematic Literature Review,” vol. 3, no. 1, pp. 19–29.
[13] V. Stevanus, “Analisis Teknologi Informasi Menggunakan Framework COBIT 2019 di PT. Adi Bintan Permata.” [Online]. Available:
[14] https://journal.iteba.ac.id/index.php/jurnalsiteba
[15] M. Miswanto, “ANALISIS TINGKAT KESADARAN MASYARAKAT TERHADAP BAHAYA CYBERCRIME (STUDI KASUS KECAMATAN
[16] JATIYOSO),” *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 2, Apr. 2025, doi: 10.23960/jitet.v13i2.6418.
[17] I. Rahmawati, “THE ANALYSIS OF CYBER CRIME THREAT RISK MANAGEMENT TO INCREASE CYBER DEFENSE.” [Online]. Available: https://news.detik.com/