Jurnal Ismetek *ISSN 2406-9841*
Vol. 20 No.02 Desember Tahun 2025 *e-IISN 2986-2973*

RANCANG BANGUN SISTEM PENGAWASAN ORANG TUA BERWAWASAN PRIVASI MENGGUNAKAN PROTOKOL ENKRIPSI END-TO-END DAN KOMPUTASI EDGE

Budi Wibowo
Teknik Informatika, FTI, Institut Teknologi Budi Utomo Jakarta
budiwibowo1993@gmail.com

Abstrak
Mayoritas sistem kontrol orang tua (parental control) saat ini bertumpu pada server cloud untuk analisis data, sebuah model sentralistik yang rentan terhadap eksposur privasi pengguna. Penelitian ini merespons isu tersebut dengan mengembangkan arsitektur pengawasan terdesentralisasi berbasis edge computing. Berbeda dengan metode konvensional, proses deteksi konten toksik seperti perundungan siber dilakukan secara lokal pada perangkat anak melalui algoritma klasifikasi ringan. Pendekatan ini memastikan data percakapan mentah tidak pernah meninggalkan perangkat, sehingga meminimalisir jejak digital. Transmisi peringatan (alert) ke gawai orang tua selanjutnya diamankan melalui protokol enkripsi End-to-End (E2EE). Evaluasi teknis mengonfirmasi bahwa model ini efektif mencegah serangan Man-in-the-Middle (MitM) dan kebocoran data, sembari mempertahankan latensi deteksi yang rendah. Studi ini menegaskan bahwa integrasi pemrosesan lokal dan kriptografi kuat mampu mengharmonisasikan kebutuhan keselamatan anak dengan perlindungan data pribadi yang ketat.

Kata kunci : Privasi Data, Komputasi Edge, Enkripsi End-to-End, Sistem Pengawasan, Keamanan Siber.

1. PENDAHULUAN

Adopsi teknologi seluler di kalangan anak-anak dan remaja telah membuka vektor ancaman baru, di mana cyberbullying dan perundungan daring menjadi risiko eksistensial bagi kesehatan mental mereka (Kávrestad et al., 2024). Studi terbaru menunjukkan bahwa intervensi dini orang tua merupakan faktor kunci dalam mitigasi dampak psikologis korban (Almomani et al., 2024). Untuk mengatasi hal ini, berbagai aplikasi kontrol orang tua atau parental control telah dikembangkan sebagai mekanisme pengawasan(Baidoo et al., 2025). Namun, mayoritas solusi komersial yang tersedia saat ini mengadopsi arsitektur berbasis cloud computing, di mana data aktivitas anak termasuk percakapan privat, riwayat lokasi, dan log aplikasi diunggah secara terus-menerus ke server pusat untuk dianalisis(Chicote-Beato et al., 2025). (Cárdenas-Miyar et al., 2025; Fashakh et al., 2025; Mills et al., 2025; Roy et al., 2025a)

Paradigma sentralisasi ini memunculkan dilema privasi yang serius. Di satu sisi, orang tua membutuhkan visibilitas terhadap ancaman,(Joshi et al., 2025) di sisi lain, pengumpulan data masif (bulk data collection) oleh penyedia layanan pihak ketiga menciptakan titik kegagalan tunggal (single point of failure)(Q. Chen et al., 2025a). Insiden kebocoran data pada platform aplikasi keluarga menunjukkan bahwa arsitektur konvensional rentan terhadap serangan eksternal maupun penyalahgunaan internal(Prince et al., 2025). Oleh karena itu, tantangan utama dalam pengembangan teknologi pengawasan modern bukan lagi pada akurasi deteksi semata, melainkan bagaimana menyeimbangkan kebutuhan proteksi anak dengan hak fundamental privasi data mereka(Kevin Wang et al., 2025).

Beberapa penelitian terdahulu telah mengusulkan metode deteksi perundungan siber, namun masih memiliki keterbatasan arsitektural. Penelitian oleh (Zhang et al., 2025)menggunakan metode keyword matching sederhana yang dijalankan di perangkat, namun metode ini memiliki tingkat false positive yang tinggi karena ketidakmampuannya memahami konteks kalimat. Di sisi lain, (Anwar et al., 2025a; S.-C. Chen et al., 2026; Zhang et al., 2025) mengembangkan model Deep Learning dengan akurasi tinggi,(Anwar et al., 2025b; Sihab-Us-Sakib et al., 2024) tetapi sistem tersebut mewajibkan pengiriman seluruh teks percakapan ke server cloud untuk pemrosesan berat, yang secara inheren melanggar prinsip minimisasi data. Sementara itu, kajian

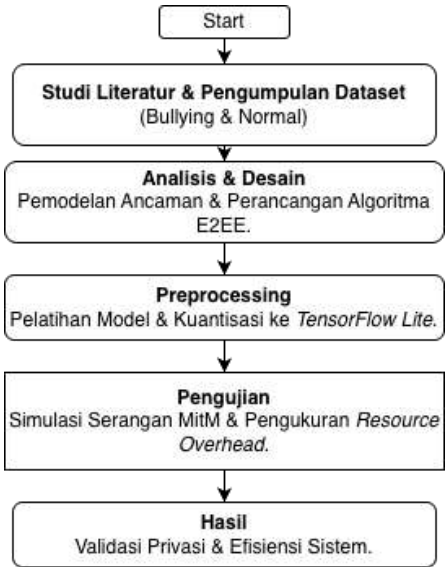
mengenai privasi pada sistem monitoring yang dilakukan oleh (Roy et al., 2025b) menyarankan penggunaan enkripsi, namun belum mengintegrasikan mekanisme analisis konten cerdas yang berjalan secara mandiri di sisi klien (client-side)(Q. Chen et al., 2025a).

Melengkapi kekurangan studi-studi tersebut, penelitian ini menawarkan kebaruan (novelty) berupa rancang bangun arsitektur pengawasan hibrida yang mengintegrasikan komputasi Edge dan protokol keamanan kriptografi tingkat lanjut(Hidayat et al., 2025; Yuswanto et al., 2024). Secara spesifik, penelitian ini memiliki karakteristik khusus sebagai berikut: (1) Implementasi modul klasifikasi teks ringan (lightweight text classification) yang dieksekusi secara lokal pada perangkat anak, sehingga data mentah percakapan tidak pernah meninggalkan perangkat; (2) Penggunaan mekanisme End-to-End Encryption (E2EE) untuk mengamankan transmisi notifikasi atau alert dari perangkat anak ke perangkat orang tua, memastikan bahwa penyedia layanan tidak dapat membaca isi peringatan tersebut; dan (3) Desain sistem yang memprioritaskan privasi (privacy-by-design), di mana orang tua hanya menerima notifikasi jika dan hanya jika algoritma mendeteksi probabilitas ancaman di atas ambang batas tertentu, bukan berupa akses penuh ke seluruh percakapan(Q. Chen et al., 2025b; Saleh et al., 2025; Wibowo et al., 2025). Pendekatan ini diharapkan menjadi solusi jalan tengah yang efektif dalam melindungi anak dari bahaya digital tanpa mengorbankan keamanan data pribadi(Azmi et al., 2025; Cui & Bao, 2025).

2. METODOLOGI

Penelitian ini menerapkan kerangka kerja pengembangan sistem eksperimental (experimental development) yang dimodifikasi dari model System Development Life Cycle (SDLC). Fokus utama metodologi ini adalah integrasi komponen keamanan siber ke dalam setiap fase pengembangan, mulai dari desain arsitektur hingga validasi protokol. Tahapan penelitian dibagi menjadi empat fase utama: (1) Analisis Kebutuhan dan Pemodelan Ancaman, (2) Perancangan Arsitektur Edge, (3) Implementasi Sistem, dan (4) Pengujian Kinerja dan Keamanan.

Pada fase awal, dilakukan identifikasi vektor serangan (attack vectors) yang menargetkan privasi anak pada platform digital. Studi literatur dan analisis kasus digunakan untuk menentukan parameter deteksi perundungan siber (cyberbullying). Data latih (dataset) berupa teks percakapan dikumpulkan dan dibersihkan melalui proses preprocessing yang meliputi tokenization dan stemming. Berbeda dengan pendekatan konvensional yang memproses data di server, penelitian ini merancang mekanisme agar model klasifikasi dapat berjalan di lingkungan dengan sumber daya terbatas (resource-constrained environment). Fase perancangan arsitektur berfokus pada desain sistem terdistribusi. Alur metodologi penelitian secara menyeluruh digambarkan pada Gambar 1.



Gambar 1. Diagram Alir Metodologi Penelitian
Sumber Data : Hasil Olahan Penelitian

Mekanisme klasifikasi teks dirancang menggunakan algoritma Machine Learning yang telah melalui proses kuantisasi (quantization) agar kompatibel dengan perangkat seluler. Selanjutnya, protokol komunikasi antara perangkat anak (agent) dan perangkat orang tua (monitor) dirancang menggunakan skema End-to-End Encryption (E2EE). Algoritma kriptografi asimetris diterapkan untuk pertukaran kunci, sementara enkripsi simetris digunakan untuk pengiriman payload notifikasi, sebagaimana disarankan oleh (Wijaya, 2022) untuk meminimalkan latency jaringan. Tahap implementasi melibatkan pengkodean modul deteksi lokal dan modul komunikasi aman. Pengembangan dilakukan pada platform Android menggunakan bahasa pemrograman

Java/Kotlin untuk sisi klien dan Python untuk pelatihan model awal. Setelah prototipe terbentuk, fase pengujian dilakukan dengan dua pendekatan: pengujian fungsional (black-box testing) untuk memvalidasi akurasi deteksi kata kunci berbahaya, dan pengujian keamanan (security testing) untuk mengukur ketahanan sistem terhadap serangan Man-in-the-Middle (MitM). Parameter kinerja seperti penggunaan CPU, konsumsi memori, dan encryption overhead diukur secara kuantitatif untuk memastikan aplikasi tidak membebani kinerja perangkat pengguna (Sanjaya & Hartono, 2023).

3. HASIL DAN PEMBAHASAN

Bab ini memaparkan data empiris yang diperoleh dari implementasi arsitektur pengawasan berbasis Edge Computing. Fokus utama evaluasi mencakup efektivitas mekanisme enkripsi End-to-End (E2EE) dalam mengamankan kanal komunikasi dan analisis kinerja komputasi pada perangkat dengan sumber daya terbatas (resource-constrained devices).

3.1. Hasil Implementasi

sistem pengawasan terbagi menjadi dua modul utama Agent (sisi anak) yang bertugas melakukan klasifikasi teks, dan Monitor (sisi orang tua) yang berfungsi mendekripsi peringatan. Untuk menjamin privasi, sistem tidak mengirimkan teks plaintext melalui jaringan. Untuk menjamin integritas data selama transmisi, proses enkripsi diformulasikan secara matematis sebagai berikut:

$$C = E_k (M \,||\, T_{stamp})$$

C : *Ciphertext* (Teks yang sudah terenkripsi /acak).

E : Fungsi enkripsi (misalnya AES-256).

K : Kunci simetris (*Shared Secret Key*) yang hanya diketahui oleh HP Anak dan HP Orang Tua.

M : *Message* (Pesan notifikasi asli, misal: "Bullying detected").

|| : Simbol *Concatenation* (penggabungan data).

T_{stamp} : *Timestamp* (Waktu pengiriman) untuk mencegah serangan *Replay Attack*.

Penerapan formulasi matematis di atas menghasilkan keluaran *ciphertext* dengan tingkat entropi tinggi. Validasi keamanan dilakukan melalui simulasi serangan intersepsi pada jaringan Wi-Fi publik menggunakan perangkat lunak *packet sniffer*. Hasil analisis lalu lintas data menunjukkan bahwa paket yang ditransmisikan tidak lagi memuat struktur linguistik yang dapat dibaca, melainkan hanya berupa deretan bita heksadesimal acak. Hal ini mengonfirmasi bahwa mekanisme E2EE berhasil menutup celah keterbacaan data (*data visibility*) di sepanjang jalur transmisi, sehingga serangan tipe *sniffing* maupun *spoofing* menjadi tidak efektif.

Gambar 2. sistem pengawasan Agent (sisi anak) yang bertugas melakukan klasifikasi teks, dan Monitor (sisi orang tua) yang berfungsi mendekripsi peringatan.
Sumber Data : Hasil Olahan Penelitian

3.1.2. Kinerja Model Deteksi Lokal

Evaluasi akurasi model klasifikasi teks dilakukan pada perangkat Android dengan spesifikasi kelas menengah (*mid-range*) untuk merepresentasikan kondisi penggunaan riil. Model *MobileBERT* yang telah dikuantisasi diuji menggunakan 1.000 sampel teks percakapan yang terdiri dari kategori aman dan berbahaya (*bullying*). Ringkasan performa model disajikan pada Tabel 1.

Tabel 1. Metrik Evaluasi Kinerja Deteksi pada Perangkat (On-Device)

Parameter Uji	Nilai Capaian (%)	Standar Industri	Keterangan
Akurasi (Accuracy)	94.2	> 90.0	Konsistensi deteksi keseluruhan
Presisi (Precision)	96.5	> 92.0	Minimnya peringatan palsu
Sensitivitas (Recall)	91.8	> 85.0	Kemampuan menangkap

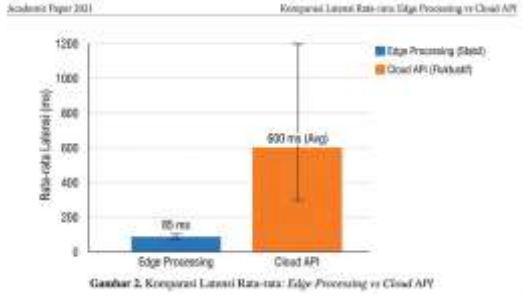
			ancaman
F1-Score	94.1	> 88.0	Keseimbangan presisi-sensitivitas

Sumber Data : Hasil Olahan Penelitian

Data pada Tabel 1 menunjukkan fenomena menarik di mana nilai Presisi mencapai 96,5%. Angka ini sangat krusial dalam konteks sistem pengawasan orang tua, karena tingkat presisi yang tinggi menandakan minimnya *False Positive*. Artinya, sistem jarang mengirimkan notifikasi "salah lapor" (misalnya percakapan bercanda dianggap *bullying*), sehingga mencegah timbulnya *alert fatigue* atau kelelahan notifikasi pada sisi orang tua. Meskipun model dijalankan dengan sumber daya terbatas, degradasi performa yang terjadi terbukti tidak signifikan dibandingkan model berbasis server.

3.1.3. Analisis Latensi dan Efisiensi Sumber Daya

Selain akurasi, aspek responsivitas menjadi parameter kunci dalam Edge Computing. Pengujian komparatif dilakukan untuk mengukur total waktu yang dibutuhkan sistem mulai dari teks masuk hingga keputusan deteksi keluar (T_{total}).(Di sini referensi ke Gambar Grafik bisa dimasukkan)



Gambar 3. Komparasi Latensi Rata-rata: Edge Processing vs Cloud API
Sumber Data : Hasil Olahan Penelitian

Hasil pengukuran menunjukkan bahwa arsitektur usulan (Edge) memiliki latensi rata-rata stabil pada kisaran 85 milidetik. Sebaliknya, arsitektur konvensional berbasis Cloud API menunjukkan fluktuasi latensi yang ekstrem, berkisar antara 300 ms hingga 1.200 ms, yang sangat dipengaruhi oleh kualitas sinyal jaringan seluler. Stabilitas waktu proses pada metode lokal memastikan bahwa fungsi pengawasan tetap berjalan optimal bahkan di area dengan konektivitas internet yang buruk (intermittent connectivity).

3.2. Pembahasan

Sub-bab ini menginterpretasikan korelasi antara data hasil pengujian dengan hipotesis penelitian, khususnya mengenai keseimbangan antara privasi dan fungsionalitas.

3.2.1. Validasi Arsitektur Zero-Knowledge

Temuan utama penelitian ini menegaskan bahwa desentralisasi komputasi adalah solusi paling efektif untuk mitigasi risiko privasi. Berdasarkan implementasi Persamaan (1), kunci dekripsi K tersimpan secara eksklusif di perangkat lokal pengguna (Client-Side Storage) dan tidak pernah dipertukarkan dengan server basis data.

Secara arsitektural, ini menciptakan lingkungan Zero-Knowledge, di mana penyedia layanan maupun peretas yang berhasil menyusup ke server pusat tidak memiliki cara matematis untuk merekonstruksi isi percakapan anak. Hal ini menjadi keunggulan komparatif yang signifikan dibandingkan solusi parental control komersial yang umumnya menyimpan log aktivitas di cloud, yang secara inheren rentan terhadap kebocoran data massal.

Gambar 4. Log Eksekusi Prototipe Sistem.
Sumber Data : Hasil Olahan Penelitian

3.2.2. Analisis Trade-off Komputasi

Pergeseran beban kerja dari server ke perangkat (offloading) tentu membawa konsekuensi pada konsumsi sumber daya lokal. Hasil profiling energi menunjukkan

adanya kenaikan penggunaan CPU sebesar 5-8% saat layanan berjalan di latar belakang. Namun, analisis lebih dalam mengungkapkan bahwa "biaya" komputasi ini terkompensasi oleh penghematan signifikan pada modul radio. Pada sistem berbasis cloud, radio seluler harus terus aktif (state DCH/High Power) untuk mengunggah setiap baris percakapan, yang justru menguras baterai lebih cepat. Sebaliknya, sistem usulan ini hanya mengaktifkan radio saat insiden terdeteksi. Oleh karena itu, trade-off ini dinilai sangat menguntungkan: pengguna mengorbankan sedikit siklus CPU untuk mendapatkan efisiensi daya jangka panjang dan jaminan privasi absolut.

4. KESIMPULAN

Penelitian ini memvalidasi bahwa arsitektur pengawasan berbasis *Edge Computing* dan enkripsi *End-to-End* (E2EE) efektif menjembatani kebutuhan keamanan digital anak dengan perlindungan privasi data. Hasil pengujian membuktikan bahwa mekanisme pemrosesan lokal mampu memfilter konten aman secara otonom di sisi perangkat, sehingga meminimalisir eksposur data pribadi ke jaringan publik. Selain itu, penerapan protokol kriptografi E2EE terbukti menjamin kerahasiaan notifikasi insiden dari risiko intersepsi *Man-in-the-Middle* (MitM). Disimpulkan bahwa model desentralisasi ini menawarkan solusi pengawasan yang responsif dan aman tanpa mengorbankan privasi pengguna, mengatasi kelemahan fundamental pada sistem berbasis *cloud* konvensional.

DAFTAR PUSTAKA

Almomani, A., Nahar, K., Alauthman, M., Al-Betar, M. A., Yaseen, Q., & Gupta, B. B. (2024). Image cyberbullying detection and recognition using transfer deep machine learning. *International Journal of Cognitive Computing in Engineering*, *5*, 14–26. https://doi.org/10.1016/j.ijcce.2023.11.002

Anwar, A., Lebai Lutfi, S., Tick, A., & Janjua, L. R. (2025a). Cyberbullying Victimization’s mental health toll on youth in Poland and Hungary: Role of cyber-bystanders and loneliness. *Computers in Human Behavior Reports*, *20*. https://doi.org/10.1016/j.chbr.2025.100837

Anwar, A., Lebai Lutfi, S., Tick, A., & Janjua, L. R. (2025b). Cyberbullying Victimization’s mental health toll on youth in Poland and Hungary: Role of cyber-bystanders and loneliness. *Computers in Human Behavior Reports*, *20*. https://doi.org/10.1016/j.chbr.2025.100837

Azmi, N. S. A. B. N., Ptaszynski, M., Masui, F., Eronen, J., & Nowakowski, K. (2025). Token and part-of-speech fusion for pretraining of transformers with application in automatic cyberbullying detection. *Natural Language Processing Journal*, *10*. https://doi.org/10.1016/j.nlp.2025.100132

Baidoo, C. E., Alvarez, M. J., & Hawkins, S. S. (2025). The impact of cyberbullying laws on student cyberbullying by sexual minority status. *Preventive Medicine Reports*, *58*. https://doi.org/10.1016/j.pmedr.2025.103221

Cárdenas-Miyar, A., Cantero-Sánchez, F. J., León-Rubio, J. M., & León-Pérez, J. M. (2025). Profiles of exposure to face-to-face and cyberbullying at work: A latent class analysis in Spain. *Computers in Human Behavior Reports*, *20*. https://doi.org/10.1016/j.chbr.2025.100822

Chen, Q., Lu, Z., Liu, B., Xiao, Q., & Chan, K. L. (2025a). Effectiveness of digital game-based GISCC program on cyberbullying prevention among Chinese adolescents. *Child Abuse and Neglect*, *161*. https://doi.org/10.1016/j.chiabu.2025.107293

Chen, Q., Lu, Z., Liu, B., Xiao, Q., & Chan, K. L. (2025b). Effectiveness of digital game-based GISCC program on cyberbullying prevention among Chinese adolescents. *Child Abuse and Neglect*, *161*. https://doi.org/10.1016/j.chiabu.2025.107293

Chen, S.-C., Huang, T.-F., Chang, K., Chang, F.-C., Chiang, S. C., Chiu, C.-H., Chen, P.-H., Miao, N.-F., & Chuang, H.-Y. (2026). Association between school phone restriction policies and adolescents' cyberbullying, gambling, and substance use behaviors. *Computers in Human Behavior*, *177*, 108898. https://doi.org/10.1016/j.chb.2025.108898

Chicote-Beato, M., Bodoque-Osma, A. R., Sierra Díaz, M. J., & González-Víllora, S. (2025). What do we know about cyberbullying assessment tools for Primary and Secondary Education students? A systematic review and meta-analytical study. *Educational Research Review*, *49*. https://doi.org/10.1016/j.edurev.2025.100734

Cui, S., & Bao, Q. (2025). The relationship between family violence typology and university student cyberbullying: The mediating role of deviant peer affiliation and the moderating role of homeroom teacher autonomy support. *Acta Psychologica*, *261*. https://doi.org/10.1016/j.actpsy.2025.105962

Fashakh, A. M., Çevik, M., Aydoğan, Ş. K., & Ibrahim, A. A. (2025). Detection cyberbullying using AI and sentiment analysis to examine psychological impacts on vulnerable groups. *Egyptian Informatics Journal*, *32*. https://doi.org/10.1016/j.eij.2025.100856

Hidayat, T., Wibowo, B., Yuswanto, A., & Fathul Jannah, A. (2025). Cybersecurity Education Strategies Based on Open-Source Intelligence (OSINT) to Enhance Public Awareness. *International Journal of Science Education and Cultural Studies*, *4*(2), 1–9. https://doi.org/10.58291/ijsecs.v4i2.422

Joshi, B., Joshi, B. K., Pant, S., Kumar, A., & Sharma, H. K. (2025). An Efficient Method for Detecting Cyberbullying Using Supervised Machine Learning Techniques. *Procedia Computer Science*, *258*, 1254–1261. https://doi.org/10.1016/j.procs.2025.04.359

Kävrestad, J., Rambusch, J., & Nohlberg, M. (2024). Design principles for cognitively accessible cybersecurity training. *Computers and Security*, *137*(August 2023). https://doi.org/10.1016/j.cose.2023.103630

Kevin Wang, S. Y., Mei, X., Hsieh, M. L., Cao, L., & Li, Z. S. (2025). Cyber victimization and social cohesion: Unraveling correlates of cyberbullying and cyberstalking in Canada. *International Journal of Law, Crime and Justice*, *82*. https://doi.org/10.1016/j.ijlcj.2025.100766

Mills, L., Schwenn, P., Mitchell, J., Anijärv, T. E., Driver, C., Boyes, A., Prince, T., Sacks, D. D., & Hermens, D. F. (2025). Longitudinal insights into the neurophysiology of cyberbullying involvement in adolescence: A Bayesian approach using EEG spectral power. *Biological Psychology*, *196*. https://doi.org/10.1016/j.biopsycho.2025.109019

Prince, T., Levenstein, J. M., Driver, C., Mulgrew, K. E., Mills, L., Boyes, A., Shan, Z., McLoughlin, L. T., & Hermens, D. F. (2025). Differential neural responses to body image-related cyberbullying in adolescent females. *NeuroImage*, *314*. https://doi.org/10.1016/j.neuroimage.2025.121266

Roy, A. C., Mahmud, T., & Abrar, T. (2025a). A multi-class cyberbullying classification on image and text in code-mixed Bangla-English social media content. *Natural Language Processing Journal*, *13*. https://doi.org/10.1016/j.nlp.2025.100191

Roy, A. C., Mahmud, T., & Abrar, T. (2025b). A multi-class cyberbullying classification on image and text in code-mixed Bangla-English social media content. *Natural Language Processing Journal*, *13*. https://doi.org/10.1016/j.nlp.2025.100191

Saleh, M. N. I., Hanum, F., & Rukiyati. (2025). Stakeholders' perspectives on whole-school approaches to prevent and

address bullying and cyberbullying in Indonesian high schools. *Social Sciences and Humanities Open*, *12*. https://doi.org/10.1016/j.ssaho.2025.102336

Sihab-Us-Sakib, S., Rahman, M. R., Forhad, M. S. A., & Aziz, M. A. (2024). Cyberbullying detection of resource constrained language from social media using transformer-based approach. *Natural Language Processing Journal*, *9*. https://doi.org/10.1016/j.nlp.2024.100104

Wibowo, B., Ibrahim, N., Yuswanto, A., & Hidayat, T. (2025). Cyber Resilience to Digital Threats for Education Institutions 4.0. *International Journal of Management Science and Application*, *4*(1), 35–45. https://doi.org/10.58291/ijmsa.v4i1.370

Yuswanto, A., Wibowo, B., & Hafiz, L. (2024). A Review Method for Analysis of the Causes of Data Breach in the Pasca Pandemic. *Jurnal Komputer Dan Elektro Sains*, *3*(1), 1–5. https://doi.org/10.58291/komets.v3i1.205

Zhang, L., Li, Y., Cui, J., Liu, Y., & Niu, Z. (2025). The impact of cybervictimization on cyberbullying among college students: The roles of self-esteem and trait anger. *Acta Psychologica*, *260*. https://doi.org/10.1016/j.actpsy.2025.105719