Jurnal Komputer dan Elektro Sains, Vol.4 No.1, Maret 2026, 80-90
https://ejournal.sultanpublisher.com/komets

Received : 27 Juli 2026; Revision: 18 Agustus 2026; Accepted: 18 Agustus 2026; Publication: 21 Agustus 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.718

Antisipasi Ancaman Cyberbullying Melalui Arsitektur Jaringan Telekomunikasi Cerdas

Adi Affandi Rotib[1], Silviana Windasari[1*], Abdurohman[2], Mardiyan Dama[1]

[1]Department of Electrical Engineering, Faculty of Engineering, Universitas Sains Indonesia, Bekasi, Indonesia
[2]Graduate School of Electrical Engineering, School of Bioscience, Technology and Innovation (SBTI), Atma Jaya Catholic University of Indonesia, Jakarta, Indonesia

Penulis Korespondensi: Silviana Windasari (e-mail: silviana.windasari@lecturer.sains.ac.id)

ABSTRAK

Perkembangan jaringan telekomunikasi 5G dan penerapan End-to-End Encryption (E2EE) meningkatkan kapasitas, kecepatan, dan privasi komunikasi digital, tetapi membatasi akses terhadap muatan pesan yang digunakan dalam moderasi konten dan deteksi cyberbullying. Penelitian ini bertujuan menganalisis literatur dan merumuskan arsitektur konseptual jaringan telekomunikasi cerdas yang mengintegrasikan Mobile Edge Computing (MEC), Federated Learning (FL), dan Encrypted Traffic Analysis (ETA). Penelitian menggunakan metode Systematic Literature Review (SLR) terhadap studi mengenai deteksi cyberbullying, analisis trafik terenkripsi, komputasi tepi, dan pembelajaran mesin terdistribusi. Hasil sintesis literatur menunjukkan bahwa MEC mendukung pemrosesan dan inferensi lebih dekat dengan pengguna sehingga berpotensi mengurangi latensi, sedangkan FL memungkinkan pembelajaran model terdistribusi tanpa memusatkan data mentah pengguna. ETA dapat melengkapi mekanisme tersebut dengan menganalisis karakteristik statistik dan pola trafik terenkripsi sebagai indikator risiko pada tingkat jaringan, tetapi tidak digunakan untuk menentukan konteks cyberbullying secara langsung. Model deep learning, seperti CNN-BiLSTM dan BERT, dapat digunakan sebagai komponen klasifikasi pada perangkat atau lingkungan edge yang memiliki akses sah terhadap fitur sebelum proses enkripsi. Kontribusi utama kajian ini adalah merumuskan arsitektur konseptual MEC–FL–ETA yang menghubungkan pemrosesan berlatensi rendah, pembelajaran terdistribusi, dan analisis trafik terenkripsi dalam kerangka mitigasi cyberbullying yang mempertimbangkan privasi pengguna. Arsitektur tersebut diselaraskan dengan kerangka regulasi Indonesia, khususnya UU No. 1 Tahun 2024 dan Permenkominfo No. 5 Tahun 2020 sebagaimana diubah dengan Permenkominfo No. 10 Tahun 2021.

KATA KUNCI: cyberbullying, Encrypted Traffic Analysis, Federated Learning, Mobile Edge Computing, telekomunikasi.

ABSTRACT

The development of 5G telecommunication networks and the implementation of End-to-End Encryption (E2EE) have enhanced the capacity, speed, and privacy of digital communications, while simultaneously limiting access to message content commonly used for content moderation and cyberbullying detection. This study aims to analyze the existing literature and formulate a conceptual intelligent telecommunication network architecture integrating Mobile Edge Computing (MEC), Federated Learning (FL), and Encrypted Traffic Analysis (ETA). A Systematic Literature Review (SLR) was conducted on studies related to cyberbullying detection, encrypted traffic analysis, edge computing, and distributed machine learning. The synthesis of the reviewed literature indicates that MEC supports processing and inference closer to end users, thereby offering the potential to reduce latency, while FL enables distributed model training without centralizing users' raw data. ETA can complement these mechanisms by analyzing statistical characteristics and encrypted traffic patterns as network-level risk indicators; however, it cannot directly determine the semantic context of cyberbullying. Deep learning models, such as CNN-BiLSTM and BERT, may serve as classification components on devices or within edge environments that have legitimate access to features prior to encryption. The main contribution of this study is the formulation of a conceptual MEC–FL–ETA architecture that integrates low-latency processing, distributed learning, and encrypted traffic analysis within a privacy-aware cyberbullying mitigation framework. The proposed architecture is also aligned with the Indonesian regulatory framework, particularly Law No. 1 of 2024 and Minister of Communication and Informatics Regulation No. 5 of 2020 as amended by Regulation No. 10 of 2021.

KEYWORDS: cyberbullying, Encrypted Traffic Analysis, Federated Learning, Mobile Edge Computing, telecommunication.

Jurnal Komputer dan Elektro Sains, Vol.4 No.1, Maret 2026, 80-90
https://ejournal.sultanpublisher.com/komets

Received : 27 Juli 2026; Revision: 18 Agustus 2026; Accepted: 18 Agustus 2026; Publication: 21 Agustus 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.718

1. PENDAHULUAN

PPerkembangan komunikasi digital, perangkat cerdas, dan jaringan telekomunikasi generasi kelima (5G) telah memperluas interaksi masyarakat dalam berbagai aktivitas sosial, ekonomi, dan pendidikan. Peningkatan konektivitas tersebut juga memperbesar ruang terjadinya penyalahgunaan teknologi, salah satunya cyberbullying. Cyberbullying merupakan bentuk perilaku agresif atau merugikan yang dilakukan melalui teknologi digital dan dapat melibatkan tindakan berulang, ketimpangan kekuasaan, serta dampak terhadap individu yang menjadi sasaran [1], [2]. Perkembangan kecerdasan buatan kemudian mendorong berbagai pendekatan otomatis untuk mendeteksi cyberbullying, terutama melalui analisis konten pada media sosial. Meskipun pendekatan tersebut menunjukkan perkembangan yang signifikan, peningkatan penggunaan End-to-End Encryption (E2EE) menimbulkan tantangan karena isi komunikasi tidak dapat diakses secara langsung oleh penyedia jaringan maupun perangkat perantara. Kondisi tersebut menuntut pendekatan mitigasi yang tidak hanya bergantung pada inspeksi muatan pesan, tetapi juga mempertimbangkan karakteristik jaringan, latensi pemrosesan, dan perlindungan privasi pengguna. Kajian state of the art menunjukkan bahwa penelitian cyberbullying masih didominasi oleh pendekatan pada lapisan aplikasi melalui Natural Language Processing (NLP), Machine Learning (ML), dan Deep Learning (DL). Metode seperti Support Vector Machine (SVM), Naïve Bayes, Random Forest, dan Term Frequency-Inverse Document Frequency (TF-IDF) telah digunakan untuk mengklasifikasikan teks cyberbullying [3]. Perkembangan berikutnya mengarah pada penggunaan BiLSTM, CNN-BiLSTM, serta model berbasis deep learning untuk meningkatkan kemampuan klasifikasi terhadap pola bahasa yang lebih kompleks [4]. Studi pada lingkungan social edge computing juga telah mengembangkan identifikasi peran dalam skenario cyberbullying menggunakan fitur berbasis konten, sentimen, dan karakteristik pengguna [5]. Namun, sebagian besar pendekatan tersebut masih membutuhkan akses terhadap konten, representasi linguistik, atau fitur pengguna yang tersedia pada lapisan aplikasi. Dengan demikian, pendekatan berbasis NLP dan DL memiliki kemampuan untuk menangkap konteks semantik cyberbullying, tetapi penerapannya menjadi terbatas ketika analisis dilakukan pada bagian jaringan yang hanya memperoleh trafik komunikasi terenkripsi.

Pada trafik yang dilindungi E2EE, teknik inspeksi berbasis payload, termasuk Deep Packet Inspection (DPI) berbasis konten, memiliki keterbatasan karena perangkat jaringan tidak memperoleh akses terhadap plaintext. Kajian Encrypted Traffic Analysis (ETA) menunjukkan bahwa informasi non-payload, seperti ukuran paket, arah aliran, waktu antar-paket, durasi sesi, dan karakteristik statistik trafik, masih dapat dimanfaatkan untuk klasifikasi trafik dan deteksi anomali tanpa melakukan dekripsi [6]. Namun, karakteristik tersebut tidak merepresentasikan makna semantik suatu percakapan sehingga tidak dapat digunakan secara langsung untuk menyimpulkan bahwa suatu komunikasi merupakan cyberbullying. Oleh karena itu, ETA dalam kajian ini diposisikan sebagai mekanisme untuk memperoleh indikator risiko atau anomali pada tingkat jaringan, sedangkan identifikasi semantik tetap memerlukan fitur yang diperoleh secara sah pada perangkat pengguna atau lingkungan edge sebelum proses enkripsi. Pada sisi lain, Mobile Edge Computing (MEC) memungkinkan fungsi komputasi ditempatkan lebih dekat dengan sumber data sehingga mendukung pemrosesan berlatensi rendah, sedangkan Federated Learning (FL) memungkinkan pembelajaran model secara terdistribusi tanpa mengharuskan data mentah pengguna dikumpulkan pada server pusat [7]. Berdasarkan literatur yang ditinjau dalam kajian ini, penelitian cyberbullying berbasis AI, penelitian ETA pada trafik terenkripsi, serta integrasi MEC dan FL pada umumnya masih berkembang sebagai bidang yang relatif terpisah. Studi cyberbullying pada social edge computing telah menunjukkan potensi pemrosesan pada sisi edge [5], tetapi belum secara khusus mengintegrasikan ETA dan FL sebagai satu kerangka konseptual untuk komunikasi yang terlindungi E2EE. Sebaliknya, kajian ETA lebih banyak diarahkan pada klasifikasi aplikasi, karakterisasi trafik, dan deteksi anomali, bukan pada penentuan konteks semantik cyberbullying [6]. Dengan demikian, berdasarkan literatur yang ditinjau, integrasi MEC, ETA, dan FL secara terpadu untuk mendukung mitigasi cyberbullying pada komunikasi E2EE masih terbatas. Kesenjangan tersebut menjadi dasar dalam perumusan arsitektur konseptual pada penelitian ini.

Berdasarkan kesenjangan tersebut, penelitian ini melalui pendekatan Systematic Literature Review (SLR) merumuskan arsitektur konseptual jaringan telekomunikasi cerdas yang mengintegrasikan MEC, ETA, dan FL untuk mendukung mitigasi cyberbullying dengan tetap mempertimbangkan keterbatasan teknis E2EE. Kontribusi utama kajian ini meliputi: (1) mensintesis keterkaitan antara pendekatan deteksi cyberbullying berbasis AI dengan analisis trafik terenkripsi dan komputasi edge; (2) merumuskan

Jurnal Komputer dan Elektro Sains, Vol.4 No.1, Maret 2026, 80-90
https://ejournal.sultanpublisher.com/komets

Received : 27 Juli 2026; Revision: 18 Agustus 2026; Accepted: 18 Agustus 2026; Publication: 21 Agustus 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.718

pembagian fungsi MEC, ETA, dan FL dalam suatu arsitektur konseptual, yaitu MEC sebagai lingkungan pemrosesan berlatensi rendah, ETA sebagai sumber indikator risiko pada tingkat jaringan, dan FL sebagai mekanisme pembelajaran model terdistribusi; (3) memperjelas batas antara analisis karakteristik trafik dan analisis semantik sehingga ETA tidak diposisikan sebagai mekanisme yang secara langsung menentukan konteks cyberbullying; serta (4) mengontekstualisasikan arsitektur yang diusulkan terhadap kebutuhan Quality of Service (QoS), perlindungan privasi, dan regulasi digital Indonesia. Aspek regulasi dalam kajian ini mengacu pada UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE [8], UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi [9], serta Permenkominfo No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat sebagaimana diubah dengan Permenkominfo No. 10 Tahun 2021 [10], [11]. Kerangka regulasi tersebut menjadi konteks dalam mempertimbangkan tata kelola sistem elektronik, perlindungan data pribadi, moderasi konten, serta mekanisme penanganan konten yang melanggar ketentuan. Dengan demikian, kajian ini bertujuan menganalisis literatur dan merumuskan cetak biru arsitektur MEC–ETA–FL sebagai kerangka konseptual untuk mendukung mitigasi cyberbullying pada lingkungan komunikasi terenkripsi tanpa melakukan dekripsi terhadap muatan pengguna, dengan tetap mempertimbangkan QoS, privasi, dan ketentuan hukum yang berlaku..

2. METODE

Penelitian ini menggunakan pendekatan Systematic Literature Review (SLR) untuk mengidentifikasi, mengevaluasi, dan mensintesis literatur yang berkaitan dengan deteksi cyberbullying, Encrypted Traffic Analysis (ETA), Mobile Edge Computing (MEC), Federated Learning (FL), serta regulasi ruang digital. Pendekatan ini dipilih karena penelitian tidak melakukan pengujian eksperimental terhadap sistem yang telah dibangun, melainkan menyintesis bukti dari beberapa domain untuk merumuskan arsitektur konseptual MEC–ETA–FL. Proses kajian dilakukan melalui tahapan identifikasi sumber, penyaringan, penilaian kelayakan dan kualitas, ekstraksi data, sintesis lintas-domain, serta perumusan arsitektur konseptual. Bukti yang diperoleh dari penelitian terdahulu diperlakukan sebagai bukti literatur, sedangkan arsitektur MEC–ETA–FL merupakan hasil konseptual yang diusulkan dalam penelitian ini.

2.1 Rancangan Penelitian

Rancangan penelitian menggunakan SLR dengan sintesis kualitatif tematik. Literatur dikelompokkan ke dalam empat domain utama, yaitu: (1) deteksi cyberbullying berbasis NLP, ML, dan DL; (2) analisis trafik terenkripsi dan keterbatasan inspeksi berbasis payload; (3) arsitektur MEC dan FL; serta (4) regulasi dan tata kelola sistem elektronik di Indonesia. Pengelompokan tersebut digunakan untuk membandingkan penelitian dari bidang yang berbeda tanpa menganggap bahwa seluruh studi memiliki objek, dataset, metode, dan kondisi eksperimen yang sama.

Setiap domain dianalisis berdasarkan tujuan penelitian, metode atau algoritma, sumber data atau dataset, lingkungan pengujian, metrik yang digunakan, hasil utama, keterbatasan, dan relevansinya terhadap arsitektur konseptual. Studi mengenai cyberbullying digunakan terutama untuk mengidentifikasi kemampuan dan keterbatasan analisis semantik [3]–[5], sedangkan kajian ETA digunakan untuk memahami karakteristik non-payload yang masih dapat dianalisis pada trafik terenkripsi [6]. Literatur MEC dan FL digunakan untuk mengidentifikasi dukungan terhadap pemrosesan pada sisi edge dan pembelajaran model terdistribusi [7], [8]. Sementara itu, dokumen regulasi digunakan untuk mengkaji keselarasan konseptual arsitektur dengan tata kelola sistem elektronik dan perlindungan data di Indonesia [9]–[12].

Angka performa yang ditemukan dalam literatur, seperti akurasi, presisi, recall, F1-score, latensi, throughput, dan computational overhead, tidak digeneralisasi secara langsung antarpenelitian. Setiap nilai dicatat bersama sumber, dataset, metode, lingkungan pengujian, dan kondisi eksperimennya. Perbandingan kuantitatif hanya dilakukan secara deskriptif apabila konteks pengujian memiliki karakteristik yang memadai untuk dibandingkan.

2.2 Sumber Data dan Kriteria Seleksi

Sumber data penelitian terdiri atas artikel ilmiah peer-reviewed, prosiding ilmiah, dokumen standar telekomunikasi, dan regulasi resmi yang relevan dengan fokus penelitian. Penelusuran literatur akademik dilakukan melalui basis data seperti IEEE Xplore, ScienceDirect, Scopus, MDPI, dan repositori ilmiah yang relevan. Dokumen regulasi diperoleh dari sumber resmi pemerintah, khususnya dokumentasi hukum yang berkaitan dengan UU ITE, Pelindungan Data Pribadi, serta Penyelenggara Sistem Elektronik Lingkup Privat.

Kriteria inklusi dan eksklusi digunakan untuk menjaga relevansi literatur terhadap pertanyaan penelitian. Rentang publikasi ditetapkan pada tahun 2015–2026 untuk menangkap perkembangan jaringan 5G, edge computing, E2EE, FL, dan metode AI modern. Literatur di luar

Jurnal Komputer dan Elektro Sains, Vol.4 No.1, Maret 2026, 80-90
https://ejournal.sultanpublisher.com/komets

Received : 27 Juli 2026; Revision: 18 Agustus 2026; Accepted: 18 Agustus 2026; Publication: 21 Agustus 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.718

rentang tersebut hanya digunakan sebagai landasan teoritis apabila memiliki relevansi mendasar yang tidak tergantikan oleh sumber yang lebih mutakhir.

Tabel 1 Kriteria Inklusi dan Eksklusi Literatur.

Parameter	Kriteria Inklusi	Kriteria Eksklusi
Rentang waktu	Literatur tahun 2015–2026 yang relevan dengan AI, E2EE, MEC, FL, dan cyberbullying	Literatur lama yang tidak memiliki relevansi teoritis atau teknis terhadap teknologi yang dikaji
Fokus cyberbullying	Studi deteksi cyberbullying, abusive language, atau perilaku berisiko digital berbasis AI	Studi psikologis atau sosiologis murni tanpa keterkaitan dengan analisis teknis
Fokus jaringan	ETA, E2EE, MEC, FL, trafik terenkripsi, latensi, QoS, dan arsitektur jaringan	Studi jaringan yang tidak berkaitan dengan komunikasi terenkripsi atau pemrosesan cerdas
Validitas sumber	Jurnal peer-reviewed, prosiding ilmiah, standar resmi, dan regulasi pemerintah	Blog, artikel opini, publikasi tidak terverifikasi, dan sumber tanpa metodologi yang dapat ditelusuri
Ketersediaan informasi	Menjelaskan metode, dataset atau lingkungan pengujian, metrik, atau hasil yang dapat diekstraksi	Informasi metodologis atau hasil utama tidak tersedia secara memadai
Regulasi	Peraturan resmi terkait PSE, UU ITE, pelindungan data, moderasi, dan tata kelola konten	Dokumen hukum yang tidak berkaitan langsung dengan ruang lingkup penelitian

Sampel sasaran difokuskan pada artikel-artikel dari domain Ilmu Komputer dan Teknik Telekomunikasi yang mengevaluasi secara spesifik kegagalan filter tradisional dan penerapan model seperti CNN, LSTM, dan Federated Learning pada lapisan proksi atau edge.

2.3 Strategi Pencarian, Screening, dan Penilaian Kualitas

Strategi pencarian menggunakan kombinasi kata kunci Boolean untuk menjangkau literatur dari beberapa domain penelitian. Sintaks pencarian utama dirumuskan sebagai berikut: ("cyberbullying detection" OR "abusive language") AND ("telecommunication network" OR "mobile edge computing" OR "encrypted traffic") AND ("federated learning" OR "deep packet inspection" OR "machine learning"). Pencarian terkait regulasi dilakukan secara terpisah menggunakan kata kunci seperti “UU ITE”, “Pelindungan Data Pribadi”, “PSE Lingkup Privat”, “moderasi konten”, dan istilah lain yang relevan dengan konteks regulasi Indonesia. Pemisahan strategi pencarian dilakukan agar persyaratan kata kunci teknis tidak menghilangkan literatur cyberbullying atau regulasi yang relevan hanya karena tidak menggunakan terminologi jaringan yang sama. Proses seleksi dilakukan melalui empat tahap, yaitu identifikasi, penyaringan judul dan abstrak, penilaian teks lengkap, dan inklusi akhir. Artikel duplikat dihapus pada tahap identifikasi. Selanjutnya, judul dan abstrak diperiksa berdasarkan kesesuaiannya dengan ruang lingkup penelitian. Artikel yang lolos kemudian ditelaah secara penuh untuk memastikan kesesuaian metodologi, ketersediaan informasi, dan relevansinya terhadap salah satu dari empat domain sintesis

Tabel 2. Rekapitulasi Proses Seleksi Literatur.

Tahap Seleksi	Keterangan	Jumlah
Identifikasi	Literatur yang diperoleh dari seluruh basis data	[N1].
Penghapusan duplikat	Artikel yang sama pada lebih dari satu basis data	[N2]

Jurnal Komputer dan Elektro Sains, Vol.4 No.1, Maret 2026, 80-90
https://ejournal.sultanpublisher.com/komets

Received : 27 Juli 2026; Revision: 18 Agustus 2026; Accepted: 18 Agustus 2026; Publication: 21 Agustus 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.718

Penyaringan	Literatur setelah pemeriksaan judul dan abstrak	[N3]
Kelayakan	Artikel yang ditelaah dalam bentuk teks lengkap	[N4]
Eksklusi teks lengkap	Literatur yang tidak memenuhi kriteria akhir	[N5]
Inklusi akhir	Literatur yang digunakan dalam proses sintesis	[N6]

Nilai N1–N6 diisi berdasarkan hasil penelusuran aktual sehingga seluruh tahapan seleksi dapat ditelusuri dan direplikasi. Untuk meningkatkan konsistensi proses seleksi, artikel yang lolos tahap screening dinilai menggunakan matriks penilaian kualitas. Setiap indikator diberi skor 0 apabila tidak terpenuhi, 1 apabila terpenuhi sebagian, dan 2 apabila terpenuhi secara jelas.

Tabel 3. Instrumen Penilaian Kualitas Literatur

Indikator	Kriteria Penilaian
Q1. Relevansi	Kesesuaian penelitian dengan salah satu domain utama kajian
Q2. Kejelasan metode	Metode, algoritma, atau prosedur penelitian dijelaskan secara memadai
Q3. Kejelasan data	Dataset, sumber data, atau lingkungan pengujian dapat diidentifikasi
Q4. Transparansi metrik	Metrik dan hasil penelitian dilaporkan secara jelas
Q5. Keterbatasan	Studi menjelaskan atau memungkinkan identifikasi keterbatasan metode
Q6. Reprodusibilitas	Prosedur penelitian cukup jelas untuk ditelusuri atau direplikasi secara konseptual

Skor maksimum penilaian adalah 12. Artikel dengan skor ≥8 digunakan sebagai sumber utama dalam proses sintesis, sedangkan artikel dengan skor <8 hanya digunakan sebagai sumber pendukung apabila memiliki relevansi khusus terhadap aspek konseptual atau regulasi. Penilaian ini tidak digunakan untuk menyamakan karakteristik penelitian dari berbagai domain, tetapi untuk memastikan bahwa sumber utama memiliki dukungan metodologis yang memadai.

2.4 Ekstraksi dan Analisis Data

Data dari setiap artikel yang memenuhi kriteria akhir diekstraksi ke dalam matriks yang memuat identitas sumber, domain penelitian, tujuan, dataset atau sumber data, metode, lingkungan pengujian, metrik, hasil utama, keterbatasan, serta relevansinya terhadap komponen arsitektur MEC–ETA–FL. Prosedur tersebut memungkinkan penelitian dari bidang cyberbullying, ETA, MEC, dan FL dibandingkan berdasarkan fungsi dan kontribusinya masing-masing, bukan melalui perbandingan langsung terhadap nilai performa yang berasal dari kondisi eksperimen berbeda.

Sintesis dilakukan melalui empat tahap. Pertama, analisis deteksi semantik, yaitu mengidentifikasi kemampuan NLP, ML, dan DL dalam mengenali konteks cyberbullying serta ketergantungannya terhadap akses konten. Kedua, analisis trafik terenkripsi, yaitu mengevaluasi karakteristik non-payload yang dapat dianalisis melalui ETA beserta keterbatasannya dalam menentukan makna semantik komunikasi. Oleh karena itu, ETA tidak diperlakukan sebagai mekanisme yang secara langsung menentukan suatu komunikasi sebagai cyberbullying, tetapi sebagai sumber indikator risiko atau anomali pada tingkat jaringan.

Ketiga, analisis arsitektur MEC dan FL, yaitu menyintesis bukti mengenai penempatan fungsi komputasi pada sisi edge, karakteristik latensi, kebutuhan sumber daya, serta pembelajaran model secara terdistribusi. Setiap angka performa yang ditemukan pada tahap ini tetap dipertahankan dalam konteks sumber, dataset, metode, dan kondisi eksperimen asalnya. Keempat, analisis regulasi, yaitu memetakan fungsi konseptual sistem terhadap prinsip perlindungan data, kewajiban PSE, moderasi konten, dan ketentuan hukum yang relevan di Indonesia [9]–[12].

Jurnal Komputer dan Elektro Sains, Vol.4 No.1, Maret 2026, 80-90
https://ejournal.sultanpublisher.com/komets

Received : 27 Juli 2026; Revision: 18 Agustus 2026; Accepted: 18 Agustus 2026; Publication: 21 Agustus 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.718

Hasil dari keempat kelompok analisis tersebut selanjutnya digunakan untuk merumuskan arsitektur konseptual MEC–ETA–FL. Pada tahap ini dilakukan pemisahan yang tegas antara bukti dari literatur dan arsitektur yang diusulkan. Bukti literatur digunakan untuk menjelaskan kemampuan, keterbatasan, dan persyaratan masing-masing teknologi, sedangkan hubungan antarkomponen dalam arsitektur merupakan hasil sintesis konseptual penelitian.

Arsitektur yang diusulkan mencakup posisi User Equipment (UE), mekanisme E2EE, modul ETA, lingkungan MEC, FL aggregator, Software-Defined Networking (SDN) controller, serta mekanisme respons jaringan. Komponen yang memperoleh akses sah terhadap fitur semantik dibedakan dari komponen jaringan yang hanya menganalisis karakteristik trafik terenkripsi. Diagram teknis arsitektur disajikan pada bagian Hasil dan Pembahasan karena merupakan keluaran dari proses sintesis, bukan bagian dari prosedur pengumpulan data.

Dengan prosedur tersebut, penelitian menghasilkan sintesis lintas-domain sebagai dasar perumusan arsitektur telekomunikasi cerdas untuk mendukung mitigasi cyberbullying, dengan tetap membedakan kemampuan analisis semantik, karakteristik trafik terenkripsi, pemrosesan edge, pembelajaran terdistribusi, QoS, privasi, dan aspek regulasi.

3 HASIL DAN PEMBAHASAN

Hasil Systematic Literature Review (SLR) menunjukkan bahwa pendekatan deteksi cyberbullying, Encrypted Traffic Analysis (ETA), Mobile Edge Computing (MEC), dan Federated Learning (FL) memiliki fungsi yang berbeda, tetapi dapat dikombinasikan dalam suatu arsitektur konseptual. Pada bagian ini, bukti dari literatur dibedakan secara tegas dari arsitektur yang diusulkan. Nilai performa dari penelitian terdahulu dipertahankan dalam konteks dataset, metode, dan kondisi pengujiannya masing-masing sehingga tidak diperlakukan sebagai hasil pengujian arsitektur MEC–ETA–FL pada penelitian ini..

3.1 Keterbatasan Inspeksi Berbasis Konten dan Peran Encrypted Traffic Analysis

Pada komunikasi yang dilindungi End-to-End Encryption (E2EE), perangkat jaringan perantara tidak memiliki akses terhadap plaintext komunikasi pengguna. Kondisi ini membatasi penerapan Deep Packet Inspection (DPI) yang bergantung pada inspeksi payload. Literatur ETA menunjukkan bahwa trafik terenkripsi tetap memiliki karakteristik non-payload, seperti ukuran paket, arah paket, waktu antar-paket, durasi aliran, serta pola statistik trafik yang dapat dimanfaatkan untuk klasifikasi aplikasi dan deteksi anomali [6]. Namun, karakteristik tersebut tidak secara langsung merepresentasikan konteks semantik komunikasi. Ukuran paket kecil, inter-arrival time pendek, pola burst, atau trafik asimetris juga dapat muncul pada aktivitas normal, seperti percakapan intensif, gaming, notifikasi aplikasi, atau layanan interaktif lainnya. Oleh karena itu, hubungan antara karakteristik trafik tersebut dan perilaku cyberbullying masih bersifat tidak langsung dan belum cukup untuk digunakan sebagai dasar klasifikasi semantik. Dalam penelitian ini, ETA tidak digunakan untuk mendeteksi cyberbullying secara langsung, tetapi sebagai indikator awal risiko atau anomali jaringan. Informasi tersebut selanjutnya dapat dikombinasikan dengan hasil klasifikasi semantik yang diperoleh secara sah pada perangkat pengguna atau lingkungan aplikasi. Pendekatan ini penting karena cyberbullying merupakan fenomena yang dipengaruhi bahasa, konteks, intensi, hubungan antarpengguna, dan riwayat interaksi.

Keterbatasan ETA juga mencakup kemungkinan false positive, yaitu trafik normal diklasifikasikan sebagai aktivitas berisiko, serta false negative, yaitu komunikasi berbahaya tidak menunjukkan pola jaringan yang berbeda secara signifikan dari trafik normal. Dengan demikian, ETA lebih tepat diposisikan sebagai mekanisme pendukung dalam arsitektur multilapis dan bukan sebagai satu-satunya dasar pengambilan keputusan.

3.2 MEC, SDN, dan Implikasi terhadap Latensi Pemrosesan

Literatur MEC menunjukkan bahwa penempatan fungsi komputasi lebih dekat dengan pengguna memungkinkan pemrosesan dilakukan tanpa selalu mengirimkan data atau metadata menuju pusat komputasi yang jauh [7]. Dalam konteks arsitektur yang diusulkan, MEC digunakan sebagai lingkungan untuk menjalankan ekstraksi fitur ETA, inferensi risiko, dan fungsi orkestrasi jaringan. Nilai latensi dalam literatur perlu ditafsirkan secara hati-hati. Oladipo et al. [18], misalnya, mengevaluasi Self-Optimizing AI Agent menggunakan dataset CIC-IDS2018, UNSW-NB15, dan trafik broadband sintetis. Penelitian tersebut melaporkan Mean Time to Detect (MTTD) sebesar 38,1 ms pada model SOAA dibandingkan 65,9 ms pada static intrusion detection system. Hasil tersebut menunjukkan potensi agen AI adaptif dalam mempercepat deteksi keamanan jaringan pada skenario pengujian tertentu, tetapi bukan hasil pengujian cyberbullying maupun bukti bahwa arsitektur MEC–ETA–FL yang diusulkan akan menghasilkan latensi yang sama.

Jurnal Komputer dan Elektro Sains, Vol.4 No.1, Maret 2026, 80-90
https://ejournal.sultanpublisher.com/komets

Received : 27 Juli 2026; Revision: 18 Agustus 2026; Accepted: 18 Agustus 2026; Publication: 21 Agustus 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.718

Tabel 4. Ringkasan Hasil Literatur, Dataset, dan Batas Generalisasi.

Sumber	Dataset/Skenario	Metode	Hasil Utama	Batas Generalisasi
Shen et al. [6]	*Berbagai studi trafik terenkripsi*	Survei ETA berbasis ML	ETA dapat mendukung identifikasi aset, karakterisasi jaringan, deteksi kebocoran privasi, dan anomali tanpa akses payload	Tidak membuktikan deteksi cyberbullying secara langsung
Wang et al. [5]	10 dataset Weibo dan 5 dataset publik	Pemodelan peran multilevel dan DEK	DEK mengidentifikasi sembilan peran dalam skenario cyberbullying	Bukan penelitian ETA pada trafik E2EE
Oladipo et al. [18]	Simulasi dan KPI telekomunikasi nyata	AI adaptif, RL, federated observability, dan edge-native detection	Meningkatkan MTTD, menurunkan false positive, dan memperbaiki respons ancaman	Bukan pengujian khusus cyberbullying
Akter et al. [13]	Dataset Bangla, 5 kategori	ML dan DL	LSTM mencapai akurasi 99,80%; XGB >74%	Hasil spesifik dataset dan tidak langsung berlaku pada ETA/E2EE
Jaradat et al. [4]	Klasifikasi multikelas media sosial	BiLSTM, CNN-BiLSTM, BiLSTM-GRU, ANN	BiLSTM mencapai akurasi 91%	Berbasis konten, bukan trafik terenkripsi

Nilai 95,8% dan 98,5% tidak dipertahankan dalam pembahasan utama karena konteks dataset, metode, dan kondisi pengujiannya belum dapat dikaitkan secara memadai dengan sumber utama yang digunakan. Penghapusan angka tersebut dilakukan untuk menghindari generalisasi lintas penelitian yang tidak sebanding. SDN dalam arsitektur ini diposisikan sebagai mekanisme orkestrasi kebijakan jaringan, bukan sebagai komponen deteksi utama. SDN controller dapat menerima keluaran dari modul penilaian risiko, tetapi tidak secara otomatis memblokir pengguna hanya berdasarkan satu skor ETA. Tindakan harus didasarkan pada mekanisme validasi, tingkat kepercayaan, dan kebijakan operasional yang mempertimbangkan risiko false positive..

3.3 Federated Learning dan Batas Perlindungan Privasi

FL memungkinkan pelatihan model dilakukan secara terdistribusi tanpa memusatkan data mentah pengguna [8]. Dalam mekanisme ini, perangkat pengguna melakukan pembaruan model secara lokal dan mengirimkan parameter atau model updates kepada agregator. Meskipun demikian, FL tidak menjamin privasi secara penuh. Parameter atau gradien yang dikirimkan tetap dapat mengandung informasi yang berpotensi dimanfaatkan melalui serangan inferensi atau rekonstruksi. Oleh karena itu, FL dalam kajian ini diposisikan sebagai mekanisme untuk mengurangi sentralisasi data, bukan sebagai jaminan absolut terhadap kebocoran informasi. Teknologi seperti secure aggregation, differential privacy, homomorphic encryption (HE), dan Secure Multi-Party Computation (SMPC) dapat digunakan sebagai mekanisme tambahan untuk meningkatkan perlindungan pembaruan model. Namun, HE dan SMPC bukan komponen inti yang wajib ada dalam arsitektur, melainkan opsi penguatan keamanan yang dapat diterapkan sesuai kebutuhan, kapasitas komputasi, dan persyaratan privasi. Dengan pembatasan tersebut, arsitektur konseptual tetap

Jurnal Komputer dan Elektro Sains, Vol.4 No.1, Maret 2026, 80-90
https://ejournal.sultanpublisher.com/komets

Received : 27 Juli 2026; Revision: 18 Agustus 2026; Accepted: 18 Agustus 2026; Publication: 21 Agustus 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.718

sederhana: FL bertugas melakukan pembelajaran terdistribusi, sedangkan mekanisme kriptografi tambahan hanya berfungsi sebagai lapisan proteksi terhadap proses pertukaran pembaruan model.

3.4 Analisis Model Deep Learning untuk Deteksi Cyberbullying

Hasil sintesis menunjukkan bahwa metode deteksi cyberbullying telah berkembang dari pendekatan ML konvensional menuju deep learning. Metode seperti SVM, Naïve Bayes, dan Random Forest relatif ringan, tetapi memiliki keterbatasan dalam menangkap hubungan semantik dan urutan bahasa [3], [13]. Model LSTM, BiLSTM, CNN-BiLSTM, dan arsitektur berbasis Transformer mampu memodelkan hubungan kontekstual yang lebih kompleks. Akter et al. [13], misalnya, menggunakan dataset berbahasa Bangla yang diperoleh dari media sosial dan terdiri atas kategori neutral, threat, troll, political, dan sexual. Pada kondisi pengujian tersebut, model LSTM mencapai akurasi 99,80%. Nilai tersebut hanya merepresentasikan performa pada dataset dan konfigurasi penelitian yang digunakan.

Jaradat et al. [4], [24] memperoleh hasil berbeda ketika membandingkan BiLSTM, CNN-BiLSTM, BiLSTM-GRU, dan ANN pada klasifikasi multikelas, dengan performa terbaik sekitar 91% pada BiLSTM. Perbedaan ini menunjukkan bahwa performa model sangat dipengaruhi bahasa, ukuran dataset, distribusi kelas, proses prapemrosesan, dan konfigurasi algoritma.

Dengan demikian, nilai performa dari penelitian yang berbeda tidak dibandingkan secara langsung sebagai indikator model terbaik. Dalam arsitektur yang diusulkan, model berbasis teks diposisikan untuk menangkap informasi semantik, sedangkan ETA menangkap karakteristik trafik. Kedua kelompok analisis tersebut memiliki fungsi yang berbeda dan bersifat komplementer.

3.5 Arsitektur Konseptual MEC–ETA–FL

Berdasarkan sintesis literatur, arsitektur yang diusulkan mengikuti urutan proses teknis yang jelas.

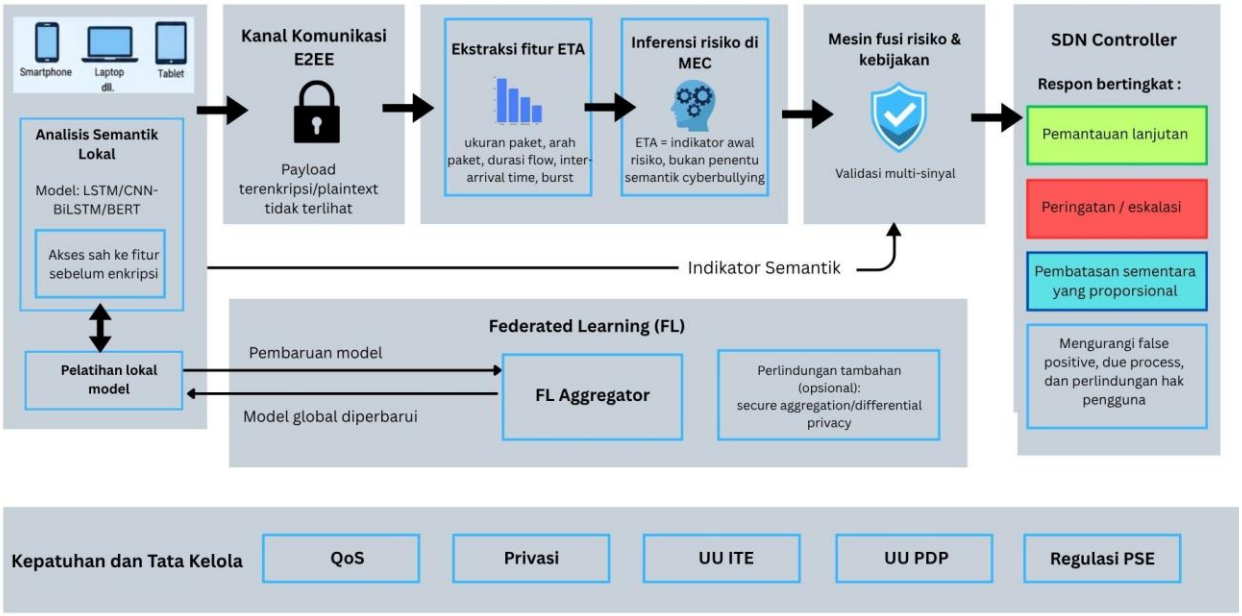
1. Tahap pertama, pada User Equipment (UE), fitur semantik yang tersedia secara sah dapat dianalisis oleh model lokal sebelum komunikasi masuk ke kanal E2EE. Model ini berfungsi mengidentifikasi karakteristik linguistik yang tidak dapat diperoleh oleh jaringan setelah pesan dienkripsi.
2. Tahap kedua, setelah komunikasi memasuki kanal E2EE, jaringan tidak memiliki akses terhadap plaintext. Pada tahap ini, modul ETA mengekstraksi fitur non-payload, seperti ukuran paket, arah paket, durasi flow, dan inter-arrival time.
3. Tahap ketiga, fitur ETA diproses pada lingkungan MEC untuk menghasilkan skor risiko jaringan. Skor ini tidak merepresentasikan kepastian bahwa suatu komunikasi merupakan cyberbullying, tetapi hanya indikator awal yang perlu dikombinasikan dengan informasi lain.
4. Tahap keempat, FL digunakan untuk memperbarui model secara terdistribusi. UE atau node yang berpartisipasi melakukan pelatihan lokal dan mengirimkan pembaruan model ke FL aggregator. Data mentah tetap berada pada sumbernya.
5. Tahap kelima, hasil analisis semantik, skor ETA, dan kebijakan operasional dapat digabungkan dalam risk fusion/policy engine. Pada tahap ini dilakukan validasi sebelum tindakan jaringan dijalankan.
6. Tahap keenam, apabila suatu kondisi memenuhi kebijakan dan ambang risiko yang ditetapkan, SDN controller dapat menjalankan respons teknis yang proporsional, seperti peningkatan pemantauan, pembatasan sementara, atau pengalihan untuk evaluasi lebih lanjut. Tindakan yang berdampak signifikan terhadap hak pengguna tidak didasarkan pada skor probabilistik tunggal.

UE dan analisis semantik lokal → E2EE → ekstraksi fitur ETA → inferensi pada MEC → fusi risiko/kebijakan → SDN controller → respons, dengan FL aggregator menjalankan pembaruan model secara terpisah dan terdistribusi.

Jurnal Komputer dan Elektro Sains, Vol.4 No.1, Maret 2026, 80-90
https://ejournal.sultanpublisher.com/komets

Received : 27 Juli 2026; Revision: 18 Agustus 2026; Accepted: 18 Agustus 2026; Publication: 21 Agustus 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.718



Gambar 1. Arsitektur Konseptual MEC–ETA–FL untuk Mendukung Mitigasi Cyberbullying pada Komunikasi E2EE

Dalam arsitektur tersebut, ETA hanya menjadi indikator awal, bukan alat deteksi cyberbullying secara langsung. SDN berfungsi sebagai pelaksana kebijakan jaringan, sedangkan HE atau SMPC merupakan mekanisme keamanan tambahan dan tidak ditempatkan sebagai komponen wajib dalam alur inti. Pembatasan fungsi ini dilakukan agar arsitektur tetap dapat dipahami, diimplementasikan, dan dievaluasi secara konseptual.

3.6 Analisis Regulasi, Hak Pengguna, dan Kewenangan ISP

Analisis regulasi dipisahkan dari analisis kemampuan teknis arsitektur. Kemampuan sistem dalam menghasilkan skor risiko tidak secara otomatis memberikan kewenangan hukum kepada ISP untuk menyatakan suatu komunikasi sebagai pelanggaran atau melakukan pemutusan akses permanen. UU No. 1 Tahun 2024 tentang perubahan kedua UU ITE [9], UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi [10], serta Permenkominfo No. 5 Tahun 2020 sebagaimana diubah dengan Permenkominfo No. 10 Tahun 2021 [11], [12] memberikan kerangka hukum terkait informasi elektronik, perlindungan data, serta kewajiban PSE. Namun, penerapan aturan tersebut tetap memerlukan prosedur hukum dan administratif yang sesuai.

Hubungan antara E2EE, metadata trafik, dan perlindungan data juga perlu diperhatikan. Walaupun ETA tidak membaca isi pesan, metadata trafik tetap dapat berkaitan dengan aktivitas pengguna dan dalam kondisi tertentu dapat memiliki implikasi terhadap privasi. Oleh karena itu, pengumpulan dan pemrosesan metadata harus mengikuti prinsip tujuan yang jelas, proporsionalitas, minimisasi data, pembatasan retensi, keamanan pemrosesan, dan akuntabilitas. Kewenangan ISP dalam menggunakan hasil analisis jaringan juga tidak bersifat tidak terbatas. Skor probabilistik, termasuk confidence score, tidak dapat digunakan sebagai satu-satunya dasar untuk melakukan take down, pemblokiran permanen, atau pembatasan hak pengguna. Risiko false positive dapat menyebabkan komunikasi normal diklasifikasikan sebagai aktivitas berisiko. Oleh karena itu, arsitektur yang diusulkan menerapkan prinsip respons bertingkat. Risiko rendah dapat menghasilkan peningkatan pemantauan teknis tanpa intervensi terhadap pengguna. Risiko menengah dapat memerlukan verifikasi tambahan. Tindakan dengan dampak signifikan harus memiliki validasi yang lebih kuat, pencatatan keputusan, mekanisme audit, dan apabila diperlukan, tinjauan manusia. Dengan demikian, arsitektur MEC–ETA–FL tidak dinyatakan sebagai sistem yang secara otomatis memenuhi seluruh kewajiban hukum atau mekanisme Safe Harbor. Arsitektur tersebut lebih tepat diposisikan sebagai kerangka teknis yang berpotensi mendukung tata kelola dan mitigasi risiko, sementara keputusan hukum, moderasi, dan pemutusan akses tetap harus dilaksanakan sesuai kewenangan serta prosedur yang berlaku. Secara

Received : 27 Juli 2026; Revision: 18 Agustus 2026; Accepted: 18 Agustus 2026; Publication: 21 Agustus 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.718

keseluruhan, hasil sintesis menunjukkan bahwa nilai utama arsitektur yang diusulkan terletak pada pembagian fungsi yang tegas antara analisis semantik pada titik yang memiliki akses sah terhadap fitur, ETA sebagai indikator risiko jaringan, MEC sebagai lingkungan pemrosesan berlatensi rendah, FL sebagai mekanisme pembelajaran terdistribusi, serta SDN sebagai orkestrator respons jaringan. Arsitektur ini masih bersifat konseptual dan memerlukan validasi eksperimental untuk mengukur akurasi, latensi, false positive rate, beban komputasi, dampak terhadap QoS, keamanan pembaruan FL, serta kesesuaian implementasinya dengan prosedur hukum dan perlindungan hak pengguna.

4 KESIMPULAN

Hasil Systematic Literature Review (SLR) menunjukkan bahwa deteksi cyberbullying, Encrypted Traffic Analysis (ETA), Mobile Edge Computing (MEC), dan Federated Learning (FL) memiliki fungsi yang berbeda tetapi dapat disintesis dalam suatu arsitektur konseptual jaringan telekomunikasi cerdas. Berdasarkan literatur yang ditinjau, MEC berpotensi mendukung pemrosesan berlatensi rendah melalui penempatan fungsi komputasi lebih dekat dengan pengguna, sedangkan ETA memungkinkan analisis karakteristik non-payload pada trafik terenkripsi tanpa melakukan dekripsi terhadap isi komunikasi. Namun, ETA tidak dapat secara langsung menentukan konteks semantik cyberbullying dan hanya diposisikan sebagai indikator awal risiko atau anomali jaringan. Analisis semantik tetap memerlukan model seperti LSTM, CNN-BiLSTM, atau BERT pada lingkungan yang memiliki akses sah terhadap fitur sebelum proses enkripsi. FL selanjutnya memungkinkan pembelajaran model secara terdistribusi tanpa memusatkan data mentah, meskipun pembaruan model tetap memiliki potensi risiko kebocoran informasi dan memerlukan mekanisme perlindungan tambahan.

Kontribusi utama kajian ini adalah perumusan arsitektur konseptual MEC–ETA–FL yang memisahkan fungsi analisis semantik, analisis trafik terenkripsi, pemrosesan edge, pembelajaran terdistribusi, dan orkestrasi respons jaringan. Arsitektur tersebut belum dapat dinyatakan efektif dalam melakukan mitigasi cyberbullying karena penelitian ini tidak melakukan implementasi maupun pengujian eksperimental. Keterbatasan penelitian terletak pada ketergantungan terhadap hasil studi terdahulu yang menggunakan dataset, metode, dan kondisi pengujian yang berbeda serta masih terbatasnya bukti empiris yang secara langsung menghubungkan karakteristik trafik terenkripsi dengan perilaku cyberbullying. Penelitian selanjutnya perlu mengembangkan prototipe MEC–ETA–FL dan melakukan validasi menggunakan dataset trafik terenkripsi yang representatif untuk mengukur akurasi, false positive rate, false negative rate, latensi, computational overhead, dampak terhadap QoS, keamanan pembaruan FL, serta kesesuaian implementasinya dengan perlindungan data pribadi dan regulasi PSE di Indonesia.

5 DAFTAR PUSTAKA

[1] G. Akwa, “Technological transitions in artificial intelligence-driven cyberbullying mitigation on social media: A systematic review,” AI and Ethics, vol. 6, art. no. 221, 2026, doi: 10.1007/s43681-026-01054-x.

[2] D. Villar Onrubia, M. Barreda Angeles, R. Cachia, A. Economou, and M. Lopez Cobo, Cyberbullying: Insights from Science, Policy and Legislation. Luxembourg: Publications Office of the European Union, 2025, JRC144335, doi: 10.2760/0941861.

[3] A. Abdullah, F. Ullah, N. Hafeez, I. Latif, G. Sidorov, E. Felipe-Riveron, and A. Gelbukh, “Cyberbull ying detection on social media using machine learning techniques,” Computación y Sistemas, vol. 29, no. 3, pp. 1567–1586, 2025, doi: 10.13053/cys-29-3-5481.

[4] G. Jaradat, M. Shehab, D. Ibrahim, S. Najdawi, and R. Sihwail, “Deep learning approaches for detecting cyberbullying on social media,” Journal of Computational and Cognitive Engineering, vol. 4, no. 4, pp. 451–465, 2025, doi: 10.47852 /bonviewJCCE52024162.

[5] R. Wang, T. Lu, P. Zhang, and N. Gu, “Role identification-based method for cyberbullying analysis in social edge computing,” Tsinghua Science and Technology, vol. 30, no. 4, pp. 1659–1684, 2025,
doi: 10.26599/TST.2024.9010066.

[6] M. Shen, K. Ye, X. Liu, L. Zhu, J. Kang, S. Yu, Q. Li, and K. Xu, “Machine learning-powered encrypted network traffic analysis: A comprehensive survey,” IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 791–824, 2023, doi: 10.1109/COMST.2022.3208196.

[7] European Telecommunications Standards Institute, Multi-access Edge Computing (MEC); Use Cases and Requirements, ETSI GS MEC 002 V4.2.1, May 2026.

[8] International Telecommunication Union, Management Requirements for Federated Machine Learning Systems, Recommendation ITU-T M.3387, Mar. 2024.

[9] Republik Indonesia, “Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik,” *Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1*, Jan. 2, 2024.

Received : 27 Juli 2026; Revision: 18 Agustus 2026; Accepted: 18 Agustus 2026; Publication: 21 Agustus 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.718

[10] Republik Indonesia, "Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi," Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Oct. 17, 2022.

[11] Kementerian Komunikasi dan Informatika Republik Indonesia, "Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat," Berita Negara Republik Indonesia Tahun 2020 Nomor 1376, Nov. 24, 2020.

[12] Kementerian Komunikasi dan Informatika Republik Indonesia, "Peraturan Menteri Komunikasi dan Informatika Nomor 10 Tahun 2021 tentang Perubahan atas Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat," Berita Negara Republik Indonesia Tahun 2021 Nomor 544, May 21, 2021.

[13] F. Akter, M. U. F. Jahangir, M. F. Rabbi, and R. R. Chowdhury, "Cyberbullying detection on social media platforms utilizing different machine learning approaches," International Journal of Computer Applications, vol. 186, no. 61, pp. 40–50, 2025, doi: 10.5120/ijca2025924395.

[14] F. Alserhani, "Advanced social media crime prevention via deep learning and cryptographic data encryption," The Computer Journal, vol. 68, no. 9, pp. 1150–1162, 2025, doi: 10.1093/comjnl/bxaf028.

[15] H. K. Haqyar, R. Faizi, and M. Muhib, "The influence of social media usage on student anxiety levels," Nangarhar University Social Science Journal, vol. 2, no. 2, pp. 57–62, 2025, doi: 10.70436/nussj. v2i02.41.

[16] M. Harini, M. Logashri, T. Sarmila, and P. Revathi, "Smart cyberbullying detection using machine learning: A comprehensive review of methods, datasets, and challenges," International Journal of Engineering Development and Research, vol. 14, no. 1, pp. 179–185, 2026.

[17] P. Kalpana, K. Malleboina, M. Nikhitha, P. Saikiran, and S. N. Kumar, "Predicting cyberbullying on social media in the big data era using machine learning algorithm," in Proc. 2024 International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, 2024, pp. 1–7, doi: 10.1109/ICD SNS62112.2024.10691297.

[18] K. Oladipo, J. N. Zeyeum, J. Ogedegbe, P. E. Olufemi, and V. Onaji, "Self-optimizing AI agents for real-time security enforcement in dynamic broadband infrastructures," International Journal of Computer Applications Technology and Research, vol. 14, no. 6, pp. 51–82, 2025, doi: 10.7753/IJCATR1406.1004.

[19] C. Pereira, A. Marto, R. Ribeiro, A. Gonçalves, N. Rodrigues, C. Rabadão, R. L. de C. Costa, and L. Santos, "Security and privacy in physical–digital environments: Trends and opportunities," Future Internet, vol. 17, no. 2, art. no. 83, 2025, doi: 10.3390/fi17020083.

[20] J. Rotter and W. Bailkoski, "AI adoption in NGOs: A systematic literature review," ACM Journal on Computing and Sustainable Societies, vol. 4, no. 2, art. no. 8, pp. 1–33, 2026, doi: 10.1145/3803556.

[21] Siberkreasi, Anak Aman di Ruang Digital: Modul Literasi Digital—Pilar Aman Digital #4, 2024.

[22] S. Hamama, "Etika komunikasi dalam media sosial: Tantangan dan solusinya," Selasar KPI: Referensi Media Komunikasi dan Dakwah, vol. 4, no. 2, pp. 182–197, 2024, doi: 10.33507/selasar.v4i2.2608.

[23] A. K. Yadav and H. O. Patel, "Cyberbullying detection using machine learning," *AIP Conference Proceedings, vol. 3224, no. 1, art. no. 020062, 2025, doi: 10.1063/5.0253658.

[24] S. Windasari, A. Abdurohman, A. A. Ratib, A. Frihadi, and K. Montazi, "Optimization model of IoT and machine learning for renewable energy-powered aeroponic systems," International Journal of Engineering Continuity, vol. 4, no. 2, pp. 40–56, Oct. 2025, doi: 10.58291/ijec.v4i2.426.