BAB II

LANDASAN TEORI

2.1 YouTube Sebagai Media Sosial

YouTube merupakan salah satu platform berbagi video terbesar di dunia yang tidak hanya berfungsi sebagai hiburan, tetapi juga sebagai sarana edukasi dan komunikasi. YouTube adalah salah satu platform berbagi video terbaik dan menakjubkan secara global karena memiliki lebih dari 2 miliar pengguna aktif setiap bulannya (Dean, 2024). Jumlah tersebut menunjukkan bahwa ini telah menjadi bagian penting dari kehidupan masyarakat dan bisnis digital saat ini.

Pada platform ini, pengguna dapat berbagi dan menonton berbagai jenis video, serta saling berinteraksi satu sama lain. Hal ini menjadikan YouTube sebagai salah satu platform media sosial yang populer di dunia, dengan peringkat kedua dalam jumlah pengguna aktif internet global (Novie Rahmawati, 2023).

Fitur interaktif seperti komentar memungkinkan terjadinya komunikasi dua arah antara kreator dan penonton, sehingga menjadikan YouTube sebagai platform yang bersifat sosial. Namun, keterbukaan fitur-fitur tersebut juga membuka peluang masuknya konten negatif seperti ujaran kebencian, hoaks dan *spam* (Novie Rahmawati, 2023).

Beberapa fitur utama yang menjadikan YouTube sebagai platform media sosial adalah:

Tabel 2.1 Fitur YouTube

Fitur	**Deskrisi**
Suka dan tidak suka (*Like and Dislike*)	Pemirsa dapat mengutarakan pendapatnya terhadap video dengan menggunakan tombol suka dan tidak suka. Mekanisme masukan ini membantu pembuat konten memahami preferensi penonton dan mengukur penerimaan konten mereka (YouTube, 2020)
Berlangganan (*Subscribe*)	Pengguna atau calon penonton dapat berlangganan saluran untuk menerima pembaruan setiap kali video baru diunggah. Namun, berlangganan suatu saluran memungkinkan pengguna membangun jaringan pembuat konten yang mereka sukai dan tetap terhubung dengan saluran favorit mereka(YouTube, 2020).
Komentar (*Comment*)	Media sosial YouTube juga memungkinkan calon audiens bisnis untuk memberikan komentar pada video yang mereka tonton. Selain itu, ini juga memungkinkan pengguna atau bisnis untuk terlibat dalam diskusi, mengajukan pertanyaan dan memberikan umpan balik pada video tertentu di YouTube. Namun, hal ini juga dimanfaatkan oleh situs-situs judi online untuk melakukan *spam* promosi situs mereka (YouTube, 2020)

2.2 Komentar *Spam* di YouTube

Komentar *spam* didefinisikan sebagai komentar yang dikirim secara massal, berulang dan tidak relevan dengan isi video (Oh, 2021). Biasanya komentar *spam* berada di vidio yang sedang ramai, tetapi juga ada beberapa channel yang para *spam*mer suka menjalankan komentar *spam*nya, mungkin pemilik channel tidak mengerti cara membatasi kata-kata maupun kalimat atau lebih memilih tidak memperdulikan komentar *spam*. Berikut ciri khas seperti komentar *spam*:

1. promosi produk,
2. tautan ke situs eksternal,
3. isi yang tidak berkaitan dengan konteks video .

Terpapar iklan judi online pun terbukti memiliki pengaruh yang cukup kuat terhadap peningkatan minat bermain judi online. Hasil ini konsisten dengan teori Strong Effects, yang menyatakan bahwa terpaan iklan yang intens dan berulang dapat mempengaruhi perilaku individu. Responden yang sering terpapar iklan judi online cenderung menunjukkan minat yang lebih tinggi untuk mencoba permainan judi tersebut (Ilmu et al., 2024).

Berikut adalah tabel yang merangkum jenis *spam*, contoh dan motif di kolom YouTube :

Tabel 2.2 Jenis-Jenis *Spam*

Jenis *Spam*	**Contoh Komentar**	**Motif**
Promosi Produk/Layanan (Situs Judi Online)	"Terbaik ❤ memang kak,salam **PLUTO88**"	Mendapatkan keuntungan finansial dari situs yang dipromosikan.

Link Berbahaya	“Klik link ini untuk hack game gratis: bit.ly/scam456"	Mencuri data pengguna
Komentar Bot	"Great video! Subscribe to my channel!" (di-posting massal)	Menigkatkan subscribe/likes secara artifial”
Clickbait	“ketik ‘AMIN’ jika ingin masuk surga”	Memanipulasi interaksi (komentar/s) untuk meningkatkan visibilitas.
Plagiarisme	Menyalin komentar pengguna lain dan memposting ulang.	Menghindari deteksi *spam* dengan menyamar sebagai pengguna asli.
Komentar Provokatif	“like dan share komentar ini kalau tidak kami akan sial dinia akhirat”	Memanfaatkan psiologi pengguna untuk viralitty palsu
Spam Tagging	“@*spam*1, @*spam*2, @*spam*3 cek profil aku yaa”	Menyebarkan promosi kebanyak orang sekaligus
Random Text	“ fyuefjefue &%$d”	Meningkatkan jumlah komentar untuk manipulasi algoritma.

Dalam konteks penelitian ini, promosi situs judi online merupakan salah satu bentuk *spam* yang sering ditemukan. Komentar semacam ini melanggar kebijakan komunitas YouTube dan dapat menurunkan kredibilitas kanal (YouTube, 2022).

2.3 Judi Online Sebagai Ancaman Nasional

Judi online merupakan bentuk perjudian yang dilakukan melalui internet dan dilarang di banyak negara, termasuk Indonesia. Selain ilegal secara hukum, aktivitas ini membahayakan psikologi pengguna, terutama remaja dan kelompok rentan lainnya. Pelaku bisnis judi online sering memanfaatkan platform media sosial seperti YouTube sebagai sarana penyebaran link promosi, baik melalui komentar bot maupun akun palsu. Fenomena ini menjadikan komentar promosi judi online sebagai bagian dari kejahatan siber yang perlu ditanggulangi secara sistematis dan multidisiplin (Tasya Jadidah et al., 2023).

Judi online bukan hanya sekadar aktivitas ilegal, namun juga berdampak luas terhadap aspek psikologis, sosial, ekonomi, hingga keamanan nasional. Fenomena ini telah berkembang pesat, terutama melalui platform digital seperti YouTube, dimana *spam* promosi dilakukan secara massal oleh bot maupun akun palsu. Kerugian bukan hanya dialami pengguna tetapi juga orang disekitarnya karena pelaku tidak sadar sudah mengalami kerugian, tidak hanya ekonomi, kesehatan mental dan bersosial juga terganggu. Perilaku berjudi juga sudah melanggar hukum yang ada serta kejahatan siber yang akan mengancam.

2.3.1 Ancaman Terhadap Kesehatan Mental

Berikut adalah tabel yang menjelaskan mengenai ancaman judi online terhadap kesehatan mental :

Tabel 2.3 Kesehatan Mental

Penyakit Mental	Dampak
Kecanduan (Gambling Disorder)	1. Kehilangan kontrol atas frekuensi bermain. 2. Mengabaikan tanggung jawab pekerjaan, keluarga dan social. 3. Terus bermain meski sudah mengalami kerugian besar (chasing losses).
Gangguan kecemasan dan depresi	1. Stres akut akibat utang menumpuk. 2. Rasa malu dan bersalah karena telah membohongi keluarga. 3. Isolasi social karena menarik diri dari lingkungan.
Gangguan tidur dan konsentrasi	1. Insomnia karena terlalu lama bermain di malam hari 2. Penurunan produktivitas akibat kurang fokus 3. Gangguan emosi seperti mudah marah dan frustasi
Perilaku implusif dan agresif	1. Pengambilan keputusan implusif (misalnya: meminjam uang tanpa pertimbangan) 2. Perilaku agresif saat kalah atau ditegur keluarga 3. Resiko penyalah gunaan alcohol/narkoba sebagai pelarian

Fenomena ini tidak hanya mencerminkan adopsi teknologi baru yang diterima oleh generasi muda tetapi juga menyoroti kebutuhan mendesak untuk mengatasi aspek-aspek negatif yang berpotensi mengarah pada gambling disorder, yang dapat merusak secara sosial dan individu.(Pratama et al., 2025)

2.3.2 Dampak Sosial

Berikut adalah tabel yang menjelaskan mengenai dampak social dari judi online:

Tabel 2.4 Dampak Sosial

Kerusakan Sosial	Dampak
Keretakan Hubungan Keluarga	1. Konflik rumah tangga akibat kebohongan dan utang judi. 2. Perceraian meningkat karena kepercayaan hancur. 3. Pengabaian tanggung jawab sebai orang tua, pasangan, atau anak. 4. Tidak lagi dipercaya omongannya karena sudah sering sekali melakukan kebohongan.
Isolasi social dan stigma negatif	1. Pemain judi online cenderung menjauh dari lingkungan social karena malu. 2. Dikucilkan masyarakat karena dianggap pemboros dan tidak bertanggung jawab. 3. Afirmasi public berlebih dikarenakan merasa dirinya lihai dalam bermain judi online.
Peningkatan kriminalitas	1. Pencurian dan penipuan untuk menitupi kerugian judi 2. Kekerasan dalam rumah tangga (KDRT) akibat tekanan finansial.

Interaksi yang terjadi dalam media sosial dan platform judi online menciptakan realitas sosial di mana judi online dilihat sebagai aktivitas yang normal dan kadang- kadang diinginkan (Pratama et al., 2025).

2.3.3 Dampak Ekonomi

Berikut adalah tabel yang menjelaskan mengenai dampak ekonomi dari judi online:

Tabel 2.5 Dampak Ekonomi

Dampak Ekonomi	Dampak
Kerugian finansial individu dan keluarga	1. Utang menumpuk karena pemain terus "kejar rugi" *(chasing losses).* 2. Kebangkrutan akibat menjual atau menggadaikan asset (rumah, kendaraan, dll). 3. Meminjam uang dengan bunga yang tidak bisa dibayar.
Prokdutivitas kerja menurun	1. Kinerja menurun karena kecanduan dan kurang tidur sehingga gaji tidak dibayarkan 2. Pemutusan hubungan kerja (PHK) akibat bolos kerja atau menggunakan uang perusahaan untuk judi.
Kerugian Negara (pencucian uang, pajak hilang dan daya beli masyarakat menurun)	1. Transaksi judi online tidak kena pajak potensi pendapatan Negara hilang 2. Aliran dana illegal keluar negri (biasanya melalui Fintech atau dompet digital) 3. Daya beli masyarakat menurun diakibatkan tidak ada lagi uang untuk berbelanja kebutuhan dan perputaran ekonomi terputus.

Salah satunya adalah faktor ekonomi, di mana responden dari latar belakang ekonomi yang lebih rendah cenderung lebih tertarik pada judi online sebagai cara cepat untuk memperoleh keuntungan finansial (Ilmu et al., 2024).

2.3.4 Ancaman Kejahatan Siber

Berikut adalah tabel yang menjelaskan mengenai ancaman kejahatan siber:

Tabel 2.6 Ancaman Kejahatan Siber

Jenis Ancaman Siber	**Dampak**
Penipuan dan *phising*	1. Banyak situs judi online palsu yang dirancang untuk mencuri data dan keuangan pengguna. 2. Penipuan melalui chat WhatsApp atau SMS yang mengatas namakan platform judi resmi untuk mengelabui korban.
Peretasan Akun (*Hacking*)	1. Akun pemain bisa diretas jika menggunakan kata sandi lemah atau terjebak malware. 2. Peretas dapat mencuri saldo atau menggunakan akun untuk transaksi illegal.
Kebocoran data pribadi	1. Pada saat mendaftar akun judi kita di suruh mengisi data pribadi. 2. Platform judi illegal sering menjual data pengguna (nama, rekening bank, KTP, nomer Hp) ke pihak ketiga.

	3. Data ini bisa digunakan untuk kejahatan lain seperti pemalsuan identitas atau pinjaman online illegal.
Malware dan *ransomware*	1. Aplikasi atau link judi bisa mengandung malware yang menginfeksi perangkat. 2. Beberapa kasus ransomwere mengunci perangkar dan meminta tebusan.
Pencucian Uang(*Money Laundering*)	1. Transaksi di situs judi online sering digunakan untuk menyamarkan dana haram. 2. Pemain yang tidak sadar terlibat dalam jaringan kejahatan finansial.
Manipulasi permainan	1. Beberapa platform menggunakan algoritma curang agar pemain selalu kalah 2. Bot atau system otomatis dipakai untuk memanipilasi hasil taruhan.

Tidak dapat dipungkiri, bermain judi online juga berisiko menimbulkan masalah hukum. Seperti diketahui, judi online adalah permainan ilegal di Indonesia. Seseorang yang terlibat dalam judi online bisa terjerat masalah hukum dan harus menghadapi denda, tuntutan hukum, atau konsekuensi serius lainnya yang dapat merusak reputasi dan masa depannya.(Susanto et al., 2024)

2.3.5 Ancaman Hukum

Berikut adalah tabel yang menjelaskan mengenai ancaman hukum judi online:

Tabel 2.7 Ancaman Hukum

Undang-Undang	**Keterangan**	**Ancaman Pidana**
KUHP (Kitab Undang-Undang Hukum Pidana) Pasal 303	Melakukan atau memfasilitasi perjudian, baik secara langsung maupun online.	Penjara maksimal 10 tahun dan denda hingga Rp 25 miliar.
UU ITE (Undang-Undang informasi dan transaksi elektronik) Pasal 27 ayat 2	Setiap orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya informasi elektronik yang memiliki muatan perjudian	Penjara maksimal 6 tahun dan/atau denda maksimal Rp 1 miliar
UU Pencucian Uang (UU No. 8 Tahun 2010)	Transaksi judi online bisa dianggap sebagai tindakan pencucian uang, dengan ancaman	Ancaman hukuman 5-15 tahun penjara

Dengan diaturnya tindak pidana perjudian dalam KUHP, UU ITE dan UU Pencucian Uang maka jelaslah bahwa perjudian adalah salah satu jenis kejahatan dan bagi pemain maupun bandarnya sama-sama dikenakan ancaman pidana. Seiring perkembangan zaman, dimana saat ini segala sesuatunya dilakukan

berdasarkan teknologi, hal ini pun berdampak terhadap perubahan mekanisme perjudian(Juhara et al., 2025)

2.3.6 Modus Judi Online

Judi online terus berkembang dengan berbagai trik baru untuk menjerat korban, situs judi menggunaan *"near-miss effect"* (hampir menang) dan bonus palsu untuk memicu kecanduan. Berikut 10 modus operandi yang paling sering digunakan berdasarkan laporan kepolisian :

Tabel 2.8 Modus Judi Online

Modus	**Trik**	**Kenyataan**
Bonus Deposit Menggiurkan	Menawarkan bonus 100-300% untuk deposit pertama melalui *spam* chat, email, dll	Dana tidak bisa ditarik sebelum mencapai *turnover* (putaran) tertentu
Aplikasi Tertutup	Mengundang calon korban untuk join grup yang dibuat oleh situs judi	Grup langsung ditutup setelah korban kalah besar
Judi Berkedok Game	Menggunakan permainan seperti slot, poker, fish hunter, roulete, tebak mangkok dan visual gambar dibuat sangat menarik seperti karakter game (Zeus, Princes,	Memanipulasi algoritma agar pemain kalah di menit-menit akhir, Tampak menggiurkan karena suara dari game

	Gatot Kaca, dll). Suara game yang dibuat sangat menarik	
Investasi bodong	Mengklaim *"investasi sportbook"* dengan imbalan 20%/ Bulan, juga ada pada treding saham yang menawarkan bahwasannya pola-polanya bisa dipelajari	Uang hangus saat Bandar kabur (mirip *skena Ponzi*)
Prediksi Bola/Pacuan Kuda	Menjual prediksi pertandingan dengan akurasi 99% dan iming-iming racikan parlay, ods yang menggiurkan dari tim kemenangan	Prediksi palsu, tapi pemain tetap diminta bayar
P2P (Peer-to-peer) judi	Permainan jadi Bandar via aplikasi seperti Doker atau sakuku	Rekening dibekukan karena masuk laporan PPATK.
Judi Live Casino Online	Dealer canti,tampan mengajak main *baccarat* atau *raoulet* juga bisa berinterasi dengan Bandar	Streaming direkam uang untuk memanipulasi hasil.
Money Games	Gabung VIP, dapatkan 5% referral + profit harian	Hanya 1% member level atas yang untung.
Judi E-Sport (Laga Mobile Legend/Dota)	Taruhan pada turnamen game (hasilnya bisa diatur) dan tim bisa ditebak	Tim bayaran sengaja kalah untuk tipu penonton.
Modus "Kawin Tikung"	Bandar berpura-pura kalah diawal, lalu menghilang saat permainan deposit besar.	Memanfaatkan rasa percaya diri korban.

Perjudian online memiliki berbagai macam permainan yang dapat diakses oleh pemain melalui platform online. Berbagai jenis perjudian menawarkan variasi dan hiburan kepada pemain. Dengan memiliki banyak pilihan permainan, pemain dapat mencoba berbagai pengalaman perjudian yang berbeda dan tetap terhibur dalam jangka waktu yang lebih lama. Persaingan antar operator perjudian mendorong inovasi dan diversifikasi dalam jenis perjudian yang ditawarkan.(Hendarto & Handayani, 2024)

2.4 Deteksi *Spam* Secara Otomatis

Deteksi *spam* secara otomatis merupakan proses sistematis yang bertujuan untuk mengklasifikasikan komentar, pesan, atau email menjadi dua kategori utama: *spam* dan bukan *spam* (ham). Proses ini sangat penting dalam menjaga kualitas konten di platform digital seperti YouTube, terutama untuk mencegah penyebaran konten ilegal seperti promosi judi online yang sering dilakukan melalui komentar bot maupun akun palsu(Ifriza & Sam, 2021).

Secara teknis, deteksi *spam* menggunakan metode analisis teks (*text mining*) dan algoritma pembelajaran mesin (*machine learning*), yang memungkinkan sistem belajar dari data pelatihan untuk mengenali pola-pola karakteristik dari komentar *spam*. Penerapan sistem deteksi *spam* otomatis dalam pengembangan perangkat

lunak memiliki manfaat besar, yaitu:

1. Meningkatkan pengalaman pengguna,
2. Mengurangi risiko kejahatan siber seperti *phishing*,
3. Membantu moderator dalam menyaring ribuan komentar setiap harinya.

2.4.1 Pengertian *Spam*

Spam juga dikenal sebagai *unsolicited commercial email* atau *unsolicited bulk email*, adalah bentuk pesan elektronik yang dikirim secara massal tanpa izin penerima. Dalam konteks media sosial seperti YouTube, *spam* biasanya berupa komentar yang tidak relevan dengan isi video, sering kali berisi promosi ilegal, tautan berbahaya, atau upaya manipulasi interaksi pengguna (Sam'an & Imaddudin, 2024). Beberapa dampak negatif *spam* meliputi:

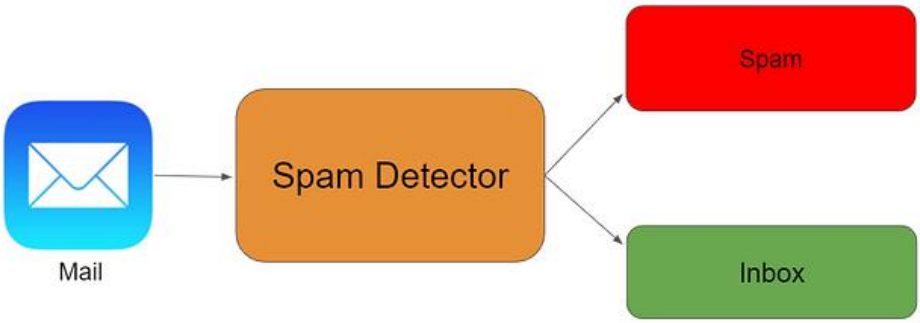
1. Memboroskan bandwidth jaringan,
2. Mengganggu pengalaman menonton,
3. Menyebarkan malware atau *scam,*
4. Merusak reputasi saluran YouTube.

2.4.2 Cara Kerja Sistem Deteksi *Spam*

Sistem deteksi *spam* bekerja dengan menggunakan kombinasi pendekatan *rule-based* dan algoritma machine learning. Algoritma yang umum digunakan dalam sistem ini antara lain:

1. *Naive bayes*
2. Decision Trees
3. Random Forests
4. Support Vector Machine (SVM)
5. Deep Learning (CNN, RNN, LSTM) untuk analisis semantik lebih kompleks

Ilustrasi sederhana tentang cara kerja sistem deteksi *spam* dapat dilihat pada Gambar berikut:



Gambar 2.1 Proses Deteksi *Spam* Otomatis

Sistem filter *spam* menganalisis beberapa elemen dalam komentar/email, seperti:

1. Alamat pengirim,
2. Bahasa yang digunakan,
3. Format dan struktur teks
4. Jenis konten

Dengan menggunakan data pelatihan yang valid, algoritma machine learning dapat belajar pola-pola yang biasanya terdapat pada konten *spam* dan membedakannya dari konten yang sah.

2.4.3 Faktor Utama dalam Klasifikasi *Spam*

Dalam sistem deteksi *spam*, terdapat sejumlah faktor utama yang digunakan sebagai fitur (features) untuk membedakan antara pesan/komentar *spam* dan bukan *spam* (ham). Fitur-fitur ini memainkan peran penting dalam proses klasifikasi, baik yang berbasis aturan (*rule-based*) maupun pendekatan pembelajaran mesin (machine learning). Berikut adalah enam faktor utama yang sering digunakan:

1. Kata-Kata atau Istilah Tertentu (Keywords)

Pesan *spam* sering kali mengandung kata-kata atau frasa tertentu yang muncul lebih sering dibandingkan pesan yang sah. Contohnya adalah kata-kata seperti "gratis", "diskon", "klik di sini", atau frasa promosi lainnya. frekuensi kemunculan kata-kata ini dapat menjadi fitur penting dalam model pembelajaran mesin untuk deteksi *spam* (Rahma et al., 2021).

2. Struktur dan Format Pesan

Karakteristik format pesan seperti penggunaan huruf kapital berlebihan (misalnya: “CEPAT DAFTAR GRATIS!!!”), penggunaan tanda baca tidak wajar, atau adanya tautan mencurigakan merupakan indikator kuat keberadaan *spam*. Penelitian oleh AISYAH et al., (2020) menunjukkan bahwa deteksi pola visual ini dapat meningkatkan performa klasifikasi ketika dikombinasikan dengan analisis tekstual.

3. Metadata Pesan

Analisis metadata seperti informasi waktu, IP address, atau akun pengguna dapat membantu mengidentifikasi pola distribusi *spam*. Dalam konteks email, ketidaksesuaian antara domain pengirim dan alamat IP sering menjadi ciri *spam*. Meskipun dalam komentar YouTube tidak ada header seperti pada email, atribut akun seperti usia channel, frekuensi komentar dan waktu posting bisa menjadi indikator perilaku mencurigakan.

4. Penggunaan Gambar, Emoji dan Teknik Obfuscation

Teknik obfuscation seperti penyisipan karakter Unicode atau emoji untuk menyamarkan tautan sering digunakan dalam komentar *spam* untuk menghindari filter otomatis.

5. Analisis Statistik dan Pembelajaran Mesin

Pendekatan statistik seperti Term Frequency-Inverse Document Frequency (TF-IDF) serta algoritma klasifikasi seperti *Naive bayes*, Support Vector Machine (SVM) dan Random Forest telah banyak digunakan dalam klasifikasi *spam*. Penelitian oleh (Rahma et al., 2021) menunjukkan bahwa model *Naive bayes* mampu mencapai akurasi tinggi dalam mendeteksi *spam*. Model deep learning seperti CNN dan LSTM belakangan ini digunakan untuk menangkap pola kompleks dan mengurangi tingkat false positive.

6. Perilaku Pengguna (User *Behavior*)

Faktor interaksi pengguna seperti laporan *spam*, jumlah likes/dislikes pada komentar, atau pola balasan bisa menjadi indikator tambahan dalam sistem klasifikasi adaptif. Sistem crowdsourcing untuk pelaporan *spam* terbukti meningkatkan akurasi deteksi. Fitur perilaku ini bersifat dinamis dan dapat disesuaikan berdasarkan konteks platform.

2.4.4 Kelebihan dan Kekurangan Pendekatan Otomatis

Pendekatan *hybrid* yang menggabungkan *rule-based filte*ring dan *Naive bayes* dipilih dalam skripsi ini karena kemampuannya untuk meningkatkan akurasi sekaligus menjaga kecepatan respons sistem.

Tabel 2.9 Kelebihan dan Kekurangan Pendekatan Otomatis

Metode	Kelebihan	Kekurangan
Rule-based Filter	Cepat, mudah diterapkan, efektif untuk *spam* jelas	Tidak adaptif, rentan diakali *spam*mer
Machine Learning	Adaptif, mampu deteksi pola baru	Butuh data pelatihan berkualitas
Hybrid Approach	Kombinasi kecepatan dan akurasi	Lebih kompleks dalam implementasi

2.5 Sistem Berbasis Aturan (*Rule-based* Filter)

Sistem berbasis aturan (*rule-based filter*) metode deteksi spam yang mengandalkan seperangkat aturan eksplisit yang dirancang secara manual untuk mengenali komentar mencurigakan.. Dalam konteks komentar *spam* di YouTube, Dalam penelitian ini, sistem ini digunakan untuk menyaring komentar spam di YouTube, terutama yang bermuatan promosi judi online.

Aturan dalam sistem ini umumnya berbentuk:

2.5.1 Daftar Kata Terlarang (Bloked Words)

Pada filter daftar kata terlarang ini jika isi teks pada komentar bermuatan kata-kata yang sudah di masukan pada daftar kata terlarang maka akan langsung di anggap *spam* tanpa pengecualian, berikut contoh daftar kata terlarang yang bermuatan judi online:

"slot", “gacor", "jepe", "jp", "maxwin", dan nama-nama situs judi online.

2.5.2 *Normalization Check* dalam *Rule-based Filter*

Sebelum tahap deteksi *spam* dilakukan, sangat penting untuk melakukan normalisasi teks *(text normalization*) agar semua bentuk penulisan yang tidak standar dapat disederhanakan menjadi format yang mudah dikenali oleh sistem *rule-based*. Proses ini disebut normalization check dan bertujuan untuk:

1. Menyederhanakan variasi penulisan agar semua bentuk dari suatu kata dapat dikenali sebagai entitas yang sama.
2. Jika terdapat *unicode* pada komentar maka akan dianggap *spam*.
3. Meminimalkan upaya penyamaran *spam*mer dengan manipulasi format teks.

Dalam penelitian ini, berikut normalisasi dilakukan melalui beberapa langkah utama dalam bentuk tabel:

Tabel 2.10 Langkah Utama Normalisasi Teks

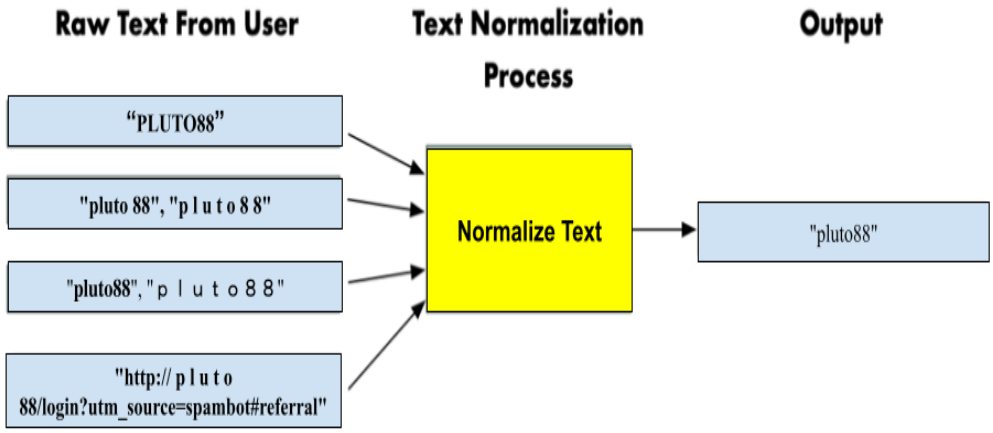
Tahap Normalisasi	**Keterangan**	**Contoh**	
		Sebelum	**Sesudah**
Lowercasing	Seluruh teks dikonversi ke huruf kecil untuk menghindari perbedaan sensitif besar-kecil huruf.	"CEPAT DAFTAR DI PLUTO88"	"cepat daftar di pluto88"
Penghapusan Spasi Tambahan & Simbol	Spasi tambahan dan simbol tidak relevan dihapus untuk membongkar teknik penyembunyian kata kunci.	"pluto 88", "p l u t o 8 8"	"pluto88"
Unicode Transformation	Karakter Unicode yang digunakan untuk menyembunyikan teks diubah ke bentuk standar ASCII jika memungkinkan.	"**pluto88**", "ｐｌｕｔｏ８８"	"pluto88"

URL Normalization	Tautan yang dimasukkan dalam komentar dinormalisasi untuk mendeteksi domain-domain mencurigakan terkait judi online.	"http:// p l u t o 88 . top /login?utm_source=*spam*bot#referral"	"pluto88.top "
Emoji *Ignoring*	Mengabaikan emoji untuk fokus pada isi teks	“Segera daftar 🔥🔥🔥 di sini pluto88.top"	"segera daftar [emoji] pluto88.top"

Setelah melewati tahapan ini, komentar tersebut siap diproses lebih lanjut untuk:

1. Jika di temukan ada unicode maka akan langsung ditandai spam
2. Klasifikasi lebih teliti dengan *Naive bayes* .

Jika dibuat kedalam bentuk gambar menjadi seperti ini :



Gambar 2. 2 Normalisasi Teks

2.6 Klasifikasi Teks dan *Naive bayes*

Klasifikasi teks merupakan salah satu tugas penting dalam pengolahan bahasa alami (*Natural Language Processing,* NLP), yaitu proses mengelompokkan dokumen atau potongan teks ke dalam kategori tertentu berdasarkan isi informasi yang terkandung di dalamnya. Dalam konteks deteksi komentar *spam* di YouTube, klasifikasi teks digunakan untuk menentukan apakah suatu komentar termasuk dalam kategori *spam* (promosi ilegal, judi online, dll.) atau bukan *spam* (ham)(Rahma et al., 2021).

Salah satu algoritma paling populer dan efektif untuk tugas ini adalah *Naive bayes* Classifier, sebuah metode pembelajaran mesin (*machine learning*) berbasis probabilitas. Algoritma ini bekerja menggunakan Teorema Bayes dan mengasumsikan bahwa setiap fitur (kata dalam teks) saling bebas secara statistik — asumsi sederhana namun cukup efektif dalam praktik klasifikasi teks berskala besar(Mukhtar et al., 2022).

2.6.1 Prinsip Kerja *Naive bayes* dalam Klasifikasi Teks

Naive bayes menghitung kemungkinan suatu komentar termasuk ke dalam kelas tertentu (misalnya *spam* atau *ham*) berdasarkan frekuensi kata-kata yang muncul dalam data pelatihan. Rumus dasar Klasifikasi *Teorema Bayes* yang digunakan adalah sebagai berikut:

$$P(c|x) = \frac{P(x|c)P(c)}{P(x)}$$

Keterangan:

C: Kelas (misalnya: *spam* atau *ham*)
x: Fitur atau data teks yang dianalisis
P(*C*|*x*): Probabilitas teks *x* termasuk kelas *C*
P(*C*): Probabilitas awal kelas *C* dalam data pelatihan
P(*x*|*C*): Probabilitas teks *x* muncul di kelas *C*
P(*x*): Probabilitas total dari teks *x*
Dalam implementasinya, model akan mengklasifikasikan sebuah komentar sebagai *spam* jika:

$$P(spam|x) > P(\text{ham}|x)$$

Model memilih kelas dengan probabilitas tertinggi sebagai hasil akhir klasifikasi.

2.6.2 Jenis-Jenis *Naive bayes*

Beberapa variasi dari algoritma *Naive bayes* digunakan dalam klasifikasi teks, antara lain:

1. Multinomial *Naive bayes*

   Cocok untuk data teks diskrit seperti frekuensi kata. Ini adalah varian yang paling umum digunakan dalam klasifikasi *spam* karena memperhitungkan berapa kali sebuah kata muncul dalam komentar.

2. Bernoulli *Naive bayes*

   Menggunakan representasi biner (kata ada/tidak ada) dalam dokumen. Cocok untuk teks pendek dan sederhana.

3. Gaussian *Naive bayes*

Digunakan untuk data kontinu, kurang cocok untuk klasifikasi teks.

Dalam penelitian ini, model *Multinomial Naive bayes* digunakan karena sesuai untuk menangani komentar YouTube yang berbasis frekuensi kata.

2.6.3 Proses Pelatihan dan Pengklasifikasian

Untuk menerapkan algoritma *Naive bayes* dalam sistem deteksi *spam*, diperlukan beberapa tahapan penting sebagai berikut:

1. Pengumpulan Data

   Langkah pertama adalah menghimpun data berupa komentar yang diambil dari YouTube. Setiap komentar kemudian diberi label secara manual, yaitu sebagai *spam* (komentar tidak relevan atau promosi) atau *ham* (komentar yang sah dan bermanfaat).

2. Praproses Teks

   Sebelum analisis lebih lanjut, teks komentar perlu diproses agar siap untuk dianalisis. Tahapan praproses meliputi:

   a. Tokenisasi : membagi kalimat menjadi kata-kata terpisah.

   b. Stopword removal : menghilangkan kata-kata umum yang tidak bermakna seperti “dan”, “di”, “yang”, dll.

   c. Stemming : mengubah kata ke bentuk dasarnya (misalnya “berikan” menjadi “beri”).

   d. Normalisasi : menyamakan format penulisan teks seperti penghapusan karakter khusus dan angka (lihat pada subbab 2.5.1).

3. Ekstraksi Fitur

   Setelah teks dibersihkan, dilakukan proses transformasi teks menjadi bentuk numerik agar dapat diproses oleh algoritma (Rahma et al., 2021). Metode yang sering digunakan antara lain:

   a. Bag of Words (BoW) : merepresentasikan frekuensi kemunculan kata dalam dokumen.

   b. TF-IDF (*Term Frequency - Inverse Document Frequency*) : memberikan bobot pada kata berdasarkan seberapa penting kata tersebut dalam konteks seluruh dokumen.

4. Pelatihan Model

   Model *Naive bayes* dilatih menggunakan data yang sudah diberi label (*spam* atau *ham*) dan fitur yang telah diekstraksi. Dalam proses ini, model akan belajar pola dari data sehingga mampu mengenali ciri-ciri komentar *spam* maupun ham.

5. Pengujian dan Evaluasi

   Setelah model selesai dilatih, model digunakan untuk melakukan prediksi terhadap data baru (komentar yang belum diketahui labelnya). Hasil prediksi kemudian dibandingkan dengan label asli untuk mengevaluasi performa model. Beberapa metrik evaluasi yang umum digunakan seperti akurasi, presisi, recall dan F1-Score

2.6.4 Kelebihan dan Kelemahan *Naive bayes*

Tabel 2.11 Kelebihan dan kelemahan *Naive bayes*

Kelebihan	Kekurangan
Cepat dan efisien dalam proses pelatihan	Asumsi independensi kata yang tidak realistis
Cocok untuk data teks besar	Kurang akurat jika kata-kata saling tergantung
Tidak membutuhkan banyak parameter	Sensitif terhadap kata yang jarang muncul (rare)
Mudah diimplementasikan dan dipahami	Performa bisa lebih rendah dari model kompleks lain

Model *Naive bayes* mampu mencapai akurasi deteksi *spam* hingga 90% jika didukung dengan data pelatihan yang bersih dan fitur yang representative (Rahma et al., 2021).

2.6.5 Relevansi *Naive bayes* dengan Penelitian Ini

Dalam penelitian ini, *Naive bayes* digunakan sebagai komponen klasifikasi dalam sistem deteksi *spam hybrid*. Model ini menangani komentar-komentar yang tidak teridentifikasi sebagai *spam* melalui *rule-based* filter, tetapi masih memiliki potensi mengandung promosi judi online.

Pendekatan ini membantu sistem untuk:

1. Mendeteksi komentar *spam* yang tidak eksplisit (ambigu),
2. Meningkatkan akurasi deteksi dengan pembelajaran dari pola bahasa *spam*,

3. Mengurangi false negative dari *rule-based* filter.

Dengan demikian, *Naive bayes* memperkuat sistem dengan kapabilitas pembelajaran otomatis dari data yang terus diperbarui.

2.7 Pendekatan *Hybrid* dalam Deteksi *Spam*

Pendekatan *hybrid* dalam sistem deteksi *spam* merujuk pada strategi penggabungan dua atau lebih metode yang berbeda untuk memperoleh hasil klasifikasi yang lebih akurat. Pendekatan ini bertujuan untuk memanfaatkan keunggulan masing-masing metode dan menutupi kelemahan yang mungkin dimiliki jika hanya menggunakan satu pendekatan secara tunggal.

Dalam kasus deteksi komentar *spam* di platform YouTube, pendekatan *hybrid* umumnya mengombinasikan:

1. Metode berbasis aturan (*rule-based*),
   seperti pencocokan kata kunci terlarang, analisis struktur komentar, atau jumlah kemunculan tautan mencurigakan
2. Metode berbasis machine learning,
   seperti *Naive bayes*, *Support Vector Machine* (SVM), atau Random Forest;
3. Model pembelajaran mendalam (deep learning),
   seperti *Convolutional Neural* Network (CNN) atau Long Short-Term Memory (LSTM), untuk memahami konteks dan makna dalam teks
4. Analisis perilaku pengguna,
   termasuk frekuensi komentar, waktu posting, serta ciri-ciri akun pengguna.

2.7.1 Implementasi Umum Pendekatan *Hybrid*

Beberapa contoh implementasi nyata dari pendekatan *hybrid* antara lain:

1. Kombinasi *Rule-based* dan Machine Learning,

   Komentar yang secara eksplisit mengandung kata-kata atau pola *spam* akan disaring lebih dahulu menggunakan aturan statis. Selanjutnya, komentar yang tidak terdeteksi oleh *rule-based* akan dianalisis lebih lanjut menggunakan algoritma klasifikasi seperti *Naive bayes*.

2. Machine Learning dan Analisis Sentimen,

   Selain mengklasifikasikan komentar sebagai *spam* atau bukan, sistem juga menganalisis sentimen dari komentar. Komentar dengan muatan negatif yang tidak relevan atau bersifat provokatif dapat dikategorikan sebagai *spam* atau komentar berbahaya.

3. Deep Learning dan Feature Engineering,

   Model deep learning seperti LSTM digunakan untuk menangkap konteks semantik komentar, dikombinasikan dengan fitur manual seperti jumlah karakter, panjang kata rata-rata, jumlah emoji, atau banyaknya tautan.

4. Model Ensemble,

   Beberapa model machine learning seperti *Naive bayes*, Decision Tree, SVM dijalankan secara parallel dan hasil klasifikasi digabungkan melalui teknik seperti voting mayoritas atau metode *stacking* untuk menghasilkan keputusan akhir yang lebih kuat.

2.7.2 Keunggulan Pendekatan *Hybrid*

Pendekatan *hybrid* menawarkan beberapa keuntungan, antara lain:

1. Peningkatan akurasi deteksi,

   Kombinasi teknik memungkinkan sistem untuk mengenali *spam* dengan presisi lebih tinggi, terutama pada kasus ambigu yang sulit dideteksi oleh satu metode saja.

2. Kemampuan menangani kasus kompleks,

   Beberapa komentar *spam* disusun dengan pola dan gaya bahasa yang kompleks. Dengan pendekatan campuran, sistem lebih siap menangani variasi ini.

3. Adaptif terhadap perubahan pola *spam,*

   Karakteristik komentar *spam* terus berkembang. Sistem *hybrid* lebih fleksibel dan dapat diperbarui untuk mengikuti tren baru dalam teknik penyamaran *spam*.

2.7.3 Tantangan Pendekatan *Hybrid*

Meskipun menawarkan banyak keunggulan, penerapan pendekatan *hybrid* juga menghadirkan sejumlah tantangan:

1. Kompleksitas arsitektur sistem meningkat

   Integrasi berbagai metode memerlukan desain sistem yang lebih rumit dan pengujian menyeluruh.

2. Kebutuhan sumber daya komputasi lebih tinggi

   Penggunaan banyak model, terutama jika melibatkan deep learning, membutuhkan waktu pelatihan dan proses inferensi yang lebih berat.

3. Diperlukan data pelatihan yang lebih beragam dan kaya

Agar sistem dapat bekerja optimal, setiap komponen dalam model *hybrid* membutuhkan data yang cukup untuk dilatih dan divalidasi.

2.7.4 Relevansi Pendekatan *Hybrid* dengan Penelitian Ini

Dalam penelitian ini, pendekatan *hybrid* diimplementasikan dengan menggabungkan metode *rule-based* dan klasifikasi *Naive bayes*. *Rule-based* digunakan untuk secara cepat menyaring komentar *spam* eksplisit yang mengandung kata atau pola mencurigakan, sedangkan *Naive bayes* digunakan untuk mengevaluasi komentar yang secara kasat mata tidak terindikasi sebagai *spam* tetapi memiliki potensi sebagai promosi judi online.

Model ini dirancang untuk:

1. Meningkatkan ketelitian dalam deteksi *spam*,
2. Meminimalkan false positive dan false negative,
3. Menyediakan sistem yang efisien dan dapat diandalkan untuk kebutuhan moderasi komentar di YouTube.

2.8 Integrasi YouTube API

YouTube API merupakan serangkaian antarmuka pemrograman aplikasi (Application Programming Interface) yang disediakan oleh Google guna memungkinkan pengembang mengakses dan memanipulasi berbagai data yang tersedia di platform YouTube secara otomatis. API ini dapat digunakan untuk mengambil informasi terkait video, channel, playlist dan komentar pengguna (YouTube, 2023).

Berikut adalah gambar dari operasi yang didukung oleh YouTube Data API :

Tabel 2.12 Integrasi YouTube API

Resource	list	insert	update	delete
activity	✓	✗	✗	✗
caption	✓	✗	✓	✓
channel	✓	✗	✗	✗
channelBanner	✗	✗	✓	✗
channelSection	✓	✓	✓	✓
comment	✓	✓	✓	✓
commentThread	✓	✓	✓	✗
guideCategory	✗	✗	✗	✗
i18nLanguage	✓	✗	✗	✗
i18nRegion	✓	✗	✗	✗
playlist	✓	✓	✓	✓
playlistItem	✓	✓	✓	✓
search result	✓	✗	✗	✗
subscription	✓	✓	✗	✓
thumbnail	✗	✗	✓	✗
video	✓	✓	✓	✓
videoCategory	✓	✗	✗	✗
watermark	✗	✓	✓	✗

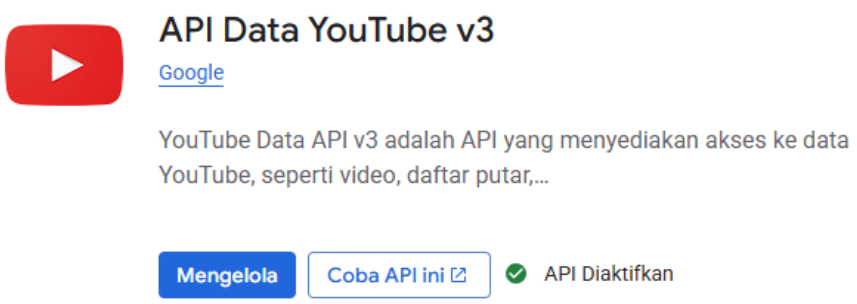
Dalam penelitian ini fokus utama penggunaan API adalah untuk mengakses komentar-komentar pada video sebagai bagian dari proses deteksi *spam* secara otomatis

2.8.1 Tujuan Integrasi API dalam Sistem Deteksi *Spam*

Integrasi YouTube API dalam sistem deteksi *spam* bertujuan untuk mengotomatisasi proses pengambilan data komentar, yang kemudian dianalisis untuk mengidentifikasi apakah komentar tersebut tergolong *spam* atau tidak. Selain itu, sistem juga dapat menampilkan hasil analisis dalam bentuk visualisasi data dan, apabila diperlukan, menjalankan tindakan lanjutan seperti menyembunyikan komentar yang terindikasi sebagai *spam*.

2.8.2 Jenis API yang Digunakan

Penelitian ini menggunakan *YouTube Data API v3*, sebuah layanan API publik dari Google yang memungkinkan akses terstruktur terhadap data YouTube.



Gambar 2.3 YouTube Data API v3

Beberapa endpoint penting yang digunakan antara lain:

1. commentThreads.list:

   digunakan untuk mengambil daftar komentar dari video tertentu beserta balasan (replies) jika tersedia.

   2. videos.list:

   berguna untuk mengambil informasi tambahan terkait video berdasarkan ID, seperti judul, deskripsi, atau statistik.

2.8.3 Tahapan Integrasi YouTube API

Berikut adalah langkah-langkah umum dalam proses integrasi API:

1. Pembuatan Proyek di Google Cloud Console,

   Pengembang terlebih dahulu membuat proyek pada platform Google Cloud dan mengaktifkan layanan YouTube Data API v3.

2. Konfigurasi Autentikasi,

   API Key digunakan untuk akses publik, sedangkan OAuth 2.0 diperlukan jika sistem membutuhkan izin khusus dari pengguna (misalnya untuk menghapus atau menyembunyikan komentar).

3. Pengambilan Data Komentar,

   Permintaan HTTP dikirim ke endpoint commentThreads.list dengan parameter video ID untuk memperoleh komentar-komentar yang ingin dianalisis.

4. Proses Analisis Komentar,

   Setelah komentar diambil, dilakukan preprocessing dan klasifikasi menggunakan model deteksi *spam*, seperti sistem *hybrid* (*rule-based* dan *Naive bayes*).

5. Penanganan Hasil Analisis,

   Hasil klasifikasi dapat ditampilkan melalui antarmuka pengguna atau, dalam implementasi lanjutan, digunakan untuk melakukan tindakan seperti menyembunyikan komentar secara otomatis.

2.8.4 Biaya Penggunaan YouTube Data API

Dalam penggunaan YouTube Data API, Google menerapkan sistem kuota berbasis "unit", bukan berbasis uang secara langsung. Namun, penggunaan unit ini berdampak pada biaya jika kamu menggunakan layanan Google Cloud berbayar atau melebihi kuota gratis.

YouTube Data API (Mode Gratis) memiliki batas kuota sebamyak 10.000 unit perhari untuk setiap permintaan, setiap jenis permintaan ke API mengonsumsi

jumlah unit tertentu (YouTube, 2023). Berikut tabel lengkap konsumsi Biaya (unit) untuk setiap permintaan:

Tabel 2.13 Biaya (unit) YouTube Data API v3

Resource	**Method**	**Biaya (unit)**	**Keterangan**
Activities	list	1	Aktivitas user seperti upload atau like
Captions	list	50	Ambil daftar caption
	insert	400	Upload caption
	update	450	Perbarui caption
	delete	50	Hapus caption
channelBanners	insert	50	Upload banner channel
Channels	list	1	Ambil info channel
	update	50	Update info channel
channelSections	list	1	Ambil section channel
	insert	50	Tambah section
	update	50	Update section
	delete	50	Hapus section
Comments	list	1	Ambil komentar
	insert	50	Tambah komentar
	update	50	Edit komentar
	setModerationStatus	50	Set status moderasi komentar
	delete	50	Hapus komentar

commentThreads	list	1	Ambil thread komentar utama
	insert	50	Tambah komentar utama
	update	50	Update komentar utama
guideCategories	list	1	Ambil kategori YouTube
i18nLanguages	list	1	Ambil daftar bahasa lokal
i18nRegions	list	1	Ambil daftar region
Members	list	1	Ambil daftar membership
membershipsLevels	list	1	Ambil level membership
playlistItems	list	1	Ambil item playlist
	insert	50	Tambah item ke playlist
	update	50	Update item playlist
	delete	50	Hapus item playlist
Playlists	list	1	Ambil daftar playlist
	insert	50	Tambah playlist
	update	50	Update playlist
	delete	50	Hapus playlist
Search	list	100	Cari video, channel, playlist, dsb
Subscriptions	list	1	Ambil daftar langganan
	insert	50	Subscribe channel
	delete	50	Unsubscribe channel
Thumbnails	set	50	Set thumbnail video
videoAbuseReportReasons	list	1	Ambil alasan report
videoCategories	list	1	Ambil kategori video

Videos	list	1	Ambil info video
	insert	1600	Upload video baru
	update	50	Update metadata video
	rate	50	Like/dislike video
	getRating	1	Ambil rating video
	reportAbuse	50	Laporkan penyalahgunaan
	delete	50	Hapus video
watermarks	set	50	Pasang watermark channel
	unset	50	Hapus watermark

Contoh jika menjalankan programnya, biaya (unit) penelitian ini jika ingin mengambil 1 vidio YouTube dengan total 50 komentar dan 10 komentar yang teridentifikasi *spam*, berikut estimasi biaya (unit):

1. Ambil video: *videos.list* = 1 vidio × 1 unit = 1 unit
2. Ambil komentar: *commentThreads.list* = 50 komentar × 1 unit = 50 unit
3. Hapus *spam*: *comments.update* = 10 komentar × 50 unit = 500 unit

Jadi biaya (unit) per menjalankannya = 1 unit + 50 unit + 500 unit = 551 unit

2.8.5 Manfaat Integrasi API

Integrasi YouTube API memberikan sejumlah keuntungan, antara lain:

1. Menghemat waktu dengan mengotomatisasi proses pengambilan komentar secara langsung dari YouTube.
2. Memungkinkan analisis terhadap data komentar yang nyata dan aktual.

3. Meningkatkan efisiensi sistem karena alur kerja deteksi *spam* dapat berjalan tanpa campur tangan manual.

2.8.6 Tantangan Integrasi API

Meskipun bermanfaat, integrasi YouTube API juga memiliki beberapa tantangan teknis, seperti:

1. Rate Limit: Google membatasi jumlah permintaan API per hari atau per menit, sehingga sistem harus dioptimalkan agar tidak melebihi kuota.
2. Kompleksitas Autentikasi: Penggunaan OAuth 2.0 memerlukan proses autentikasi tambahan dan pengelolaan token akses.
3. Ketergantungan Koneksi Internet: Karena data diakses secara real-time dari server YouTube, sistem sangat bergantung pada kestabilan jaringan.

2.9 Ekspor Data Menggunakan ExcelJS

ExcelJS merupakan pustaka (library) JavaScript yang digunakan untuk membuat, membaca dan memodifikasi file Microsoft Excel (format .xlsx) secara terprogram. Library ini sangat cocok digunakan dalam lingkungan Node.js maupun aplikasi berbasis web, karena menyediakan antarmuka yang fleksibel untuk menangani file spreadsheet. Dalam konteks sistem deteksi komentar *spam*, ExcelJS digunakan untuk menyimpan hasil klasifikasi ke dalam file Excel agar dapat ditinjau lebih lanjut oleh pengguna, baik untuk keperluan dokumentasi, validasi, maupun pelaporan (NPM, 2023).

2.9.1 Tujuan Ekspor Data ke Excel

Ekspor data hasil klasifikasi *spam* memiliki peran penting dalam sistem, antara lain:

1. Menyediakan laporan dalam format yang mudah dibaca dan familiar, yaitu Excel.
2. Menyimpan informasi hasil klasifikasi (*spam*/ham) secara sistematis untuk keperluan audit atau verifikasi manual.
3. Mempermudah distribusi data hasil analisis kepada pihak terkait, seperti admin channel atau dosen pembimbing dalam konteks penelitian.

2.9.2 Struktur Data yang Diekspor

Pada penelitian saya, struktur data yang dituliskan ke dalam file Excel mencakup:

1. Vidio ID, Contoh: “GvoG8kGtfr0”
2. Author, Contoh: “@muhammaddimas5958”
3. Comment, Contoh: “izin share bang $\mathcal{PULAUWIN}$”
4. *Spam*, Contoh “YA”
5. Detection Method, Contoh “*Naive bayes*”

2.9.3 Langkah-Langkah Penggunaan ExcelJS

Proses pembuatan dan penulisan data ke Excel menggunakan ExcelJS melibatkan beberapa tahapan sebagai berikut:

1. Menyiapkan Data

   Data komentar beserta hasil analisis dikumpulkan dalam struktur array atau objek di dalam aplikasi.

2. Membuat Workbook dan Worksheet

   Menggunakan method Workbook dari ExcelJS untuk membuat file Excel baru dan menambahkan worksheet.

3. Mendefinisikan Header dan Kolom

   Header kolom seperti “Vidio ID”, “Author”, “Comment”, “*Spam*”, “Detection Method”, ditentukan agar data tertata dengan baik.

4. Menuliskan Data ke Baris

   Melalui perulangan (looping), setiap hasil klasifikasi ditambahkan sebagai baris baru ke worksheet.

5. Menyimpan atau Mengunduh File

   File disimpan ke dalam server (pada aplikasi backend) atau dapat diunduh langsung oleh pengguna melalui browser.

6. (Opsional) Format Tampilan

   ExcelJS juga mendukung fitur pemformatan seperti pengaturan lebar kolom, warna latar sel, gaya huruf, hingga penambahan grafik visual.

2.9.4 Keunggulan Menggunakan ExcelJS

1. Mudah digunakan oleh pengguna umum, karena format Excel sangat dikenal.
2. Fleksibel dalam integrasi dengan berbagai sistem berbasis JavaScript.
3. Dapat disesuaikan format dan tampilannya sesuai kebutuhan pengguna.
4. Portabel, karena file Excel dapat dibuka dan dibagikan secara luas tanpa memerlukan aplikasi khusus.

2.9.5 Kendala dan Tantangan ExelJS

1. File Excel berukuran besar jika jumlah komentar sangat banyak, yang dapat memengaruhi kecepatan pemrosesan.
2. Dibutuhkan pengelolaan memori yang baik saat mengekspor data dalam jumlah besar.
3. Ketergantungan terhadap library eksternal, sehingga perlu memastikan kompatibilitas versi library dan lingkungan aplikasi.

2.10 Penelitian sebelumnya

Penelitian mengenai deteksi komentar *spam*, khususnya pada media sosial seperti YouTube, telah dilakukan oleh berbagai peneliti dengan pendekatan yang beragam. Pendekatan-pendekatan tersebut mencakup metode berbasis aturan (*rule-based*), machine learning klasik seperti *Naive bayes* dan Support Vector Machine (SVM), hingga metode deep learning. Penelitian-penelitian terdahulu ini menjadi referensi penting dalam merancang sistem deteksi komentar *spam* yang efektif. Berikut tebel yang menjelaskan penelitian sebelumnya:

Tabel 2.14 Penelitian Sebelumnya

Nama Peneliti	Judul Penelitian	Metode	Hasil Utama	Perbedaan Penelitian
(Krishna et al., 2025)	*YouTube Comments Sentiment*	YouTube Data API, Sentiment Analysis	Menganalisis sentimen komentar YouTube dan	Fokus Anda adalah *spam* promosi judi online, bukan

	Analysis – IJRASET	(VADER, TextBlob), Output Excel	menampilkan hasil dalam dashboard berbasis HTML.	hanya sentimen umum; serta menggunakan pendekatan *rule-based + Naive bayes*.
(AISYAH et al., 2020)	*Klasifikasi Spam pada Email* – Universitas Sriwijaya	SVM, Isolation Forest, SMOTE	SVM mencapai akurasi 96.8% dalam deteksi email *spam* setelah balancing data.	Berbeda konteks (email vs YouTube); Anda memakai *Naive bayes* dan *rule-based hybrid*.
(Lavindi et al., 2019)	*Aplikasi Hybrid Filtering dan Naïve Bayes untuk Rekomendasi Laptop* – JOINS UDINUS	*Hybrid* Filtering + *Naive bayes*	Sistem rekomendasi produk laptop berbasis web dengan akurasi klasifikasi 80%.	Fokus Anda pada *spam* detection, bukan sistem rekomendasi. Namun pendekatan *hybrid* dan implementasi web serupa.
(Rachmat Chrismanto et al., 2018)	*Instagram Spam Detector for*	*Naive bayes*, SVM, K-	Sistem deteksi *spam* komentar Instagram	Fokus platform berbeda (Instagram),

	Indonesian Language – iSemantic	NN, REST API	berbasis REST API. Akurasi tertinggi K-NN: 88.4%.	namun penggunaan komentar berbahasa Indonesia dan pendekatan supervised sangat relevan.
(Sam'an & Imaddudin, 2024)	*Hybrid Deep Learning Model for YouTube Spam Detection* – IJECE	CNN, LSTM, biLSTM, CNN-biLSTM, CNN-GRU	Akurasi tertinggi CNN-biLSTM: 96.94%. Deteksi *spam* komentar YouTube menggunakan dataset publik (UCI) dan preprocessing NLP.	Anda menggunakan pendekatan yang lebih ringan (*rule-based* + *Naive bayes*), sehingga cocok untuk deployment ringan seperti Node.js + ExcelJS. Model Anda juga fokus pada *spam* bermuatan judi, bukan umum.