Jurnal Global Digital Systems & Engineering (GENESIS)
Volume 1, Nomor 1, Juli 2025.pp 1-9
ISSN xxxxx (media cetak)
ISSN xxxx (media online)
DOI : xx
https://journalsaktipublisingcenter.org/index.php/jurnalgen

Penerapan Algoritma Naive Bayes untuk Menganalisis Kesadaran Gen-Z terhadap Ancaman Cyber melalui CAPTCHA di Kota Mataram

Ahmad Arifin [1], Muhammad Yunus [2]
[1,]Teknik Informatika,Universitas Negri Padang, Padang, Indonesia
[2,]Sistem Informasi, Universitas Putra Indonesia , Padang, Indonesia
[1] arifin@gamail.com , [2] yunusyusnus@gmail.com ,

Article History

Manuscript submitted:
25 Juni 2025
Manuscript revised:
10 Juli 2025
Accepted for publication:
30 Juli 2025

Keywords

CAPTCHA, Gen-Z, Mataram, Naive Bayes, Ancaman Cyber

Abstract

Penggunaan internet di era digital semakin meningkat, namun ancaman cyber juga mengalami eskalasi yang signifikan. CAPTCHA dirancang untuk membedakan antara pengguna manusia dan bot, namun kelompok peretas memanfaatkan kelemahan sistem ini dengan modus baru berupa manipulasi verifikasi "I'm Not a Robot". Serangan ini dapat mengecoh pengguna untuk mengklik kotak CAPTCHA yang tampak sah, padahal tersembunyi instruksi berbahaya yang menyalin perintah ke clipboard untuk mengeksekusi malware. Meskipun Generasi Z dikenal sebagai digital natives, penelitian ini menemukan bahwa tingkat kesadaran mereka terhadap risiko cyber masih rendah. Penelitian ini bertujuan untuk menganalisis tingkat kesadaran dan respon Gen-Z di Kota Mataram terhadap ancaman cyber melalui CAPTCHA, serta menguji efektivitas algoritma Multinomial Naive Bayes dalam mengklasifikasikan data responden. Penelitian menggunakan metode kuantitatif dengan 100 responden Gen-Z (usia 18–27 tahun) yang diperoleh melalui kuesioner daring. Data diproses melalui tahap preprocessing, label encoding, pembagian data training dan testing, serta klasifikasi menggunakan Multinomial Naive Bayes. Hasil penelitian menunjukkan bahwa algoritma Naive Bayes mampu mencapai tingkat akurasi sebesar 87% dalam mengklasifikasikan kesadaran responden.Temuan ini mengindikasikan bahwa meskipun Gen-Z Mataram aktif dalam penggunaan internet, literasi keamanan siber mereka masih perlu ditingkatkan. Oleh karena itu, hasil penelitian ini dapat menjadi rujukan bagi pemerintah daerah, lembaga pendidikan, dan komunitas teknologi dalam merancang program literasi digital yang lebih efektif.

Volume 1, Nomor 1, Juli 2025. ISSN xxxxx (media cetak) ISSN xxxx (media online) pp 1-9
DOI : xx
https://journalsaktipublisingcenter.org/
https://journalsaktipublisingcenter.org/index.php/jurnalgen

1. PENDAHULUAN

Perkembangan teknologi informasi pada era revolusi industri 4.0 telah membawa perubahan besar dalam berbagai aspek kehidupan manusia. Internet kini menjadi salah satu kebutuhan primer masyarakat modern, bukan hanya sebagai sarana komunikasi, tetapi juga sebagai medium transaksi keuangan, layanan publik, pendidikan, kesehatan, hingga hiburan. Data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII, 2024) menunjukkan bahwa penetrasi internet di Indonesia telah mencapai 77,02% populasi, atau setara dengan lebih dari 213 juta pengguna. Angka ini menandakan bahwa mayoritas masyarakat Indonesia telah terhubung ke dunia digital dalam berbagai aktivitas sehari-hari(APJII., 2024).

Namun, seiring dengan meningkatnya penggunaan internet, risiko ancaman siber juga semakin kompleks. Serangan yang dulunya bersifat sederhana seperti virus komputer kini berkembang menjadi serangan phishing, pencurian data pribadi, malware canggih, hingga serangan yang mengeksploitasi celah keamanan pada sistem yang selama ini dianggap aman. Laporan Badan Siber dan Sandi Negara (BSSN, 2024) mencatat lebih dari 527 juta serangan siber yang terjadi di Indonesia sepanjang tahun 2024, dengan jenis serangan terbanyak berupa malware, phishing, dan eksploitasi kerentanan aplikasi. Kondisi ini menunjukkan bahwa masalah keamanan siber sudah menjadi tantangan serius di tingkat nasional(BSSN., 2024).

Salah satu modus serangan terbaru yang mulai marak adalah eksploitasi *CAPTCHA* (Completely Automated Public Turing test to tell Computers and Humans Apart). *CAPTCHA* diciptakan sebagai sistem verifikasi untuk membedakan pengguna manusia dengan bot. Jenis *CAPTCHA* yang populer adalah verifikasi sederhana berupa checkbox dengan tulisan "I'm Not a Robot". Sistem ini awalnya dianggap efektif karena bot tidak mudah melewati proses identifikasi tersebut. Namun, beberapa kelompok peretas berhasil memanfaatkan kelemahan CAPTCHA dengan cara menyembunyikan instruksi berbahaya di balik verifikasi. Misalnya, peretas dapat membuat kode yang secara otomatis menyalin perintah ke clipboard pengguna dan mengeksekusi malware saat CAPTCHA diklik. Fenomena ini menimbulkan paradoks, di mana teknologi keamanan justru bisa dijadikan pintu masuk serangan.

Generasi Z (Gen-Z) adalah kelompok yang sangat terpapar risiko ancaman semacam ini. Gen-Z didefinisikan sebagai individu yang lahir antara tahun 1997 hingga 2012 (Howe & Strauss, 1991). Mereka tumbuh besar di era digital, terbiasa menggunakan internet sejak usia dini, dan sangat aktif di media sosial maupun layanan berbasis aplikasi. Kelebihan ini membuat Gen-Z sering disebut sebagai *digital natives*. Namun, di balik keunggulan mereka dalam menggunakan teknologi, sejumlah penelitian menunjukkan bahwa kesadaran Gen-Z terhadap keamanan siber masih rendah. Survei yang dilakukan oleh Kaspersky (2023) menemukan bahwa lebih dari 72% Gen-Z di Indonesia kesulitan mengenali serangan phishing. Hal ini mengindikasikan bahwa kemampuan teknis mereka dalam menggunakan internet tidak berbanding lurus dengan kemampuan menjaga keamanan digital.

Fenomena ini juga terlihat jelas di Kota Mataram, ibu kota Provinsi Nusa Tenggara Barat. Mataram merupakan pusat pemerintahan, pendidikan, dan perekonomian di NTB dengan perkembangan teknologi digital yang pesat. Berdasarkan data BPS (2024), sekitar 30% dari total penduduk Mataram berada dalam kelompok usia Gen-Z. Mereka sangat aktif menggunakan internet, baik untuk keperluan pendidikan, pekerjaan, maupun hiburan. Namun, tingginya

intensitas penggunaan internet tidak selalu diimbangi dengan tingkat kewaspadaan yang memadai. Kondisi ini menjadikan Gen-Z di Mataram sebagai kelompok yang relevan untuk diteliti dalam konteks kesadaran dan respon terhadap ancaman siber, khususnya terkait manipulasi CAPTCHA.

Penelitian terdahulu telah banyak membahas literasi digital di kalangan generasi muda, namun belum banyak yang fokus pada ancaman spesifik berupa eksploitasi CAPTCHA. Selain itu, penelitian dengan pendekatan kecerdasan buatan (machine learning) untuk mengklasifikasikan kesadaran cyber di kalangan Gen-Z juga masih terbatas. Oleh karena itu, penelitian ini menggunakan algoritma Naive Bayes, khususnya varian *Multinomial Naive Bayes***,** untuk menganalisis pola kesadaran dan respon Gen-Z di Mataram. Algoritma ini dipilih karena keunggulannya dalam menangani data kategorikal seperti hasil kuesioner berbasis skala Likert. Naive Bayes dikenal sederhana, cepat, dan cukup akurat, sehingga sesuai untuk penelitian dengan jumlah sampel terbatas.

2. TINJAUAN PUSTAKA

2.1 Generasi Z

Generasi Z (Gen-Z) adalah kelompok generasi yang lahir antara tahun 1997 hingga 2012 (Howe & Strauss, 1991). Mereka dikenal sebagai digital natives karena sejak kecil sudah akrab dengan teknologi digital, internet, dan media sosial. Karakteristik utama Gen-Z adalah ketergantungan tinggi terhadap teknologi, mobilitas, dan interaksi sosial secara daring. Di Indonesia, Gen-Z merupakan kelompok demografis terbesar setelah milenial, sehingga pengaruhnya terhadap perkembangan digital nasional sangat signifikan (APJII, 2024).

Kelebihan utama Gen-Z adalah keterampilan tinggi dalam mengakses informasi secara cepat, adaptif terhadap teknologi baru, serta kreatif dalam memanfaatkan media sosial untuk ekspresi diri maupun aktivitas ekonomi (Anwar, 2024). Namun, sejumlah penelitian juga menyoroti kelemahan mereka, terutama dalam hal literasi digital dan keamanan siber. Survei yang dilakukan Kaspersky (2023) menunjukkan bahwa 72% Gen-Z di Indonesia tidak mampu mengenali pesan phishing, meskipun mereka mengaku memahami risiko keamanan data. Hal ini menimbulkan paradoks: Gen-Z dianggap paling melek teknologi, tetapi justru rentan terhadap manipulasi digital.

Di Kota Mataram, Gen-Z merupakan bagian penting dari masyarakat urban yang aktif menggunakan internet, baik untuk pendidikan, bisnis online, maupun hiburan. Namun, tingkat literasi keamanan siber mereka belum pernah diteliti secara mendalam. Hal ini menjadi salah satu urgensi penelitian untuk memahami kondisi Gen-Z Mataram dalam konteks ancaman cyber.

2.2 Ancaman Cyber

Ancaman cyber adalah segala bentuk serangan yang dilakukan melalui jaringan internet untuk merusak, mencuri, atau mengganggu sistem informasi. Menurut Purwani (2023), ancaman cyber dapat dibagi menjadi beberapa kategori utama.

1. *Malware**:*** perangkat lunak berbahaya yang dirancang untuk merusak atau mencuri data.
2. *Phishing**:*** teknik manipulasi sosial untuk mencuri data pribadi

dengan menyamar sebagai pihak terpercaya.

3. *Denial of Service* (DoS/DDoS)**:** serangan yang membanjiri sistem dengan permintaan palsu sehingga membuat layanan tidak bisa diakses.
4. *Man-in-the-Middle(MitM)**:*** penyadapan komunikasi antara dua pihak tanpa sepengetahuan mereka.
5. Exploit kerentanan sistem**:** memanfaatkan celah keamanan aplikasi atau perangkat keras untuk menyusup

Di Indonesia, laporan Badan Siber dan Sandi Negara (BSSN, 2024) menunjukkan bahwa jumlah insiden siber meningkat signifikan dalam 3 tahun terakhir. Jenis serangan yang paling banyak adalah malware, phishing, dan kebocoran data pribadi. Kasus-kasus besar seperti kebocoran data SIM card dan data kesehatan masyarakat memperlihatkan lemahnya kesadaran dan perlindungan siber di tingkat individu maupun organisasi.

Ancaman cyber memiliki dampak yang serius, mulai dari kerugian finansial, penyalahgunaan data pribadi, hingga penurunan kepercayaan masyarakat terhadap layanan digital. Oleh karena itu, kesadaran masyarakat, khususnya generasi muda seperti Gen-Z, menjadi kunci utama dalam membangun ketahanan siber nasional.

2.3 *CAPTCH* “ Iam Not A Robot”

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) adalah sistem keamanan berbasis tes Turing untuk membedakan pengguna manusia dan bot (Von Ahn et al., 2003). Versi awal *CAPTCHA* berupa teks acak yang harus diketik ulang oleh pengguna. Seiring perkembangan, muncul jenis *CAPTCHA* baru seperti gambar, puzzle, hingga re*CAPTCHA* dari Google.

Jenis yang paling populer saat ini adalah checkbox *CAPTCHA* dengan pernyataan *“I’m Not a Robot”***.** Sistem ini menggunakan analisis perilaku pengguna (misalnya pergerakan mouse, kecepatan klik, dan pola interaksi) untuk membedakan manusia dari bot. Namun, kelemahan sistem ini adalah adanya peluang bagi peretas untuk menyisipkan instruksi berbahaya di balik kotak verifikasi. Misalnya, peretas dapat membuat skrip yang menyalin kode berbahaya ke clipboard saat pengguna mengklik checkbox, sehingga tanpa sadar pengguna mengeksekusi perintah tersebut di perangkat mereka.

Fenomena ini menunjukkan bahwa sistem keamanan yang dirancang untuk melindungi pengguna dapat berubah menjadi titik lemah apabila tidak disertai kewaspadaan dari pengguna. Sayangnya, sebagian besar pengguna, khususnya Gen-Z, sering menganggap *CAPTCHA* sebagai prosedur rutin yang selalu aman tanpa menyadari potensi ancaman yang tersembunyi.

2.4 Algoritma Nive Bayes

Naive Bayes adalah algoritma klasifikasi yang didasarkan pada *Teorema Bayes*, yaitu teori probabilitas yang menghitung kemungkinan suatu kejadian berdasarkan pengetahuan sebelumnya *prior knowledge*. Disebut “*naive*” karena algoritma ini mengasumsikan bahwa setiap fitur dalam data bersifat independen, meskipun pada kenyataannya seringkali tidak sepenuhnya demikian (Fadillah & Sukmana, 2022).

RUMUS

$$P(C/X) = \frac{P(C/X).\bullet P(C)}{P(X)}$$

Dimana :

- P(C|X): probabilitas kelas C dengan kondisi X
- P(X|C)P(X|C)P(X|C): probabilitas fitur X jika diketahui kelas C
- P(C)P(C)P(C): probabilitas awal kelas C
- P(X)P(X)P(X): probabilitas awal fitur X

Dalam konteks penelitian ini, naive bayes digunakan peneliti untuk mengklasifikasikan adanya kesadaran responden yaitu waspada atau tidak waspada terhadap ancaman cyber.

3. METODOLOGI PENELITIAN

3.1. Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode deskriptif dan eksperimental**.** Pendekatan kuantitatif dipilih karena penelitian berfokus pada pengukuran numerik tingkat kesadaran dan respon Gen-Z terhadap ancaman cyber, yang kemudian dianalisis menggunakan metode statistika dan algoritma machine learning.

Metode deskriptif digunakan untuk menggambarkan profil responden dan kondisi kesadaran cyber Gen-Z di Mataram, sedangkan metode eksperimental diterapkan melalui penggunaan algoritma Multinomial Naive Bayes untuk mengklasifikasikan data responden.

Penelitian dilakukan di Kota Mataram, Provinsi Nusa Tenggara Barat. Mataram dipilih karena merupakan pusat aktivitas pendidikan, pemerintahan, dan bisnis di NTB dengan penetrasi internet yang cukup tinggi. Sebagian besar Gen-Z di kota ini memiliki akses internet baik melalui perangkat smartphone maupun komputer.

Pengumpulan data dilakukan pada periode Januari–Maret 2025 melalui kuesioner daring (online questionnaire) yang disebarkan menggunakan media sosial, grup WhatsApp mahasiswa, dan komunitas digital di Mataram.

Populasi dalam penelitian ini adalah Generasi Z di Kota Mataram, yaitu individu berusia 18–27 tahun pada tahun 2025. Data BPS (2024) menunjukkan bahwa sekitar 30% penduduk Kota Mataram berada dalam kategori usia tersebut.

Teknik sampling yang digunakan adalah purposive sampling, yaitu pemilihan sampel berdasarkan kriteria tertentu yang sesuai dengan tujuan penelitian. Adapun kriteria sampel adalah:

1. Responden berusia 18–27 tahun (Gen-Z).
2. Berdomisili di Kota Mataram.
3. Aktif menggunakan internet minimal 4 jam per hari.
4. Pernah berinteraksi dengan sistem CAPTCHA saat menggunakan layanan digital.

3.2. Tahapan Penelitian

Proses penelitian dilakukan melalui beberapa tahapan utama mulai dari tahapan pengumpulan data yaitu Kuesioner disebarkan secara daring. Dari 120 kuesioner yang dikirimkan, diperoleh 100 responden yang memenuhi kriteria, Tahapan preprocessing meliputi *Data Cleaning*: menghapus data duplikat atau jawaban tidak lengkap. *Handling Missing Values****:*** jawaban kosong diisi menggunakan metode mode substitution. *Label Encoding*: jawaban skala Likert diubah menjadi nilai numerik (1–4),

Algoritma Multinomial Naive Bayes digunakan karena sesuai untuk data kategorikal hasil kuesioner. Langkah-langkah:

1. Hitung probabilitas prior masing-masing kelas (kesadaran tinggi / rendah).
2. Hitung *probabilitas likelihood* untuk setiap fitur.
3. Gunakan Teorema Bayes untuk menghitung posterior probability dari setiap kelas.
4. Tentukan kelas dengan nilai probabilitas terbesar sebagai hasil klasifikasi.

Model dievaluasi menggunakan *confusion matrix* untuk menghitung akurasi, precision, recall, dan f1-score.

4. HASIL DAN PEMBAHASAN

4.1. Deskripsi Responden

Karakteristik responden perlu dianalisis terlebih dahulu untuk memahami profil Gen-Z di Mataram yang menjadi objek penelitian. Analisis ini penting karena faktor usia, jenis kelamin, intensitas penggunaan internet, dan pengalaman menghadapi ancaman cyber dapat memengaruhi tingkat kesadaran digital responden.

Distribusi responden berdasarkan usia ditunjukkan pada Tabel 4.1 berikut.

Tabel 4.1. Distribusi Responden berdasarkan Usia

Usia (tahun)	Jumlah	Persentase
18–20	25	25%
21–23	40	40%
24–27	35	35%
Total	100	100%

Dari tabel di atas dapat dilihat bahwa responden terbanyak berusia 21–23 tahun (40%). Hal ini menggambarkan bahwa mayoritas responden adalah mahasiswa dan fresh graduate, kelompok yang secara aktif menggunakan internet untuk pendidikan dan aktivitas sosial.

Selanjutnya, distribusi responden berdasarkan jenis kelamin ditunjukkan pada Tabel 4.2.

Tabel 4.2. Distribusi Responden berdasarkan Jenis Kelamin

Jenis Kelamin	Jumlah	Persentase
Laki-laki	48	48%
Perempuan	52	52%
Total	100	100%

Data ini menunjukkan komposisi yang relatif seimbang antara laki-laki (48%) dan perempuan (52%). Keseimbangan ini penting karena hasil penelitian dapat lebih representatif terhadap kondisi Gen-Z secara umum di Mataram.

Tingkat intensitas penggunaan internet juga menjadi variabel penting karena semakin tinggi waktu akses, semakin besar pula potensi terpapar ancaman cyber. Distribusi waktu penggunaan internet ditampilkan pada Tabel 4.3.

Tabel 4.3. Intensitas Penggunaan Internet Harian

Lama Akses Internet	Jumlah	Persentase
< 4 jam	10	10%
4–6 jam	32	32%
6–8 jam	28	28%
> 8 jam	30	30%
Total	100	100%

Sebagian besar responden (58%) menggunakan internet lebih dari 6 jam per hari. Hal ini menguatkan anggapan bahwa Gen-Z sangat bergantung pada aktivitas digital, sehingga penting untuk mengukur sejauh mana kesadaran mereka terhadap ancaman keamanan siber.

Selain itu, pengalaman menghadapi ancaman cyber juga memengaruhi tingkat kewaspadaan responden. Distribusi pengalaman tersebut ditunjukkan pada Tabel 4.4.

Tabel 4.4. Pengalaman Menghadapi Ancaman Cyber

Pernah Mengalami Ancaman Cyber	Jumlah	Persentase
Ya	62	62%
Tidak	38	38%
Total	100	100%

Data menunjukkan bahwa 62% responden pernah mengalami ancaman siber seperti phishing, malware, atau akses mencurigakan. Fakta ini memperkuat urgensi penelitian karena mayoritas Gen-Z di Mataram sudah terekspos ancaman cyber nyata.

4.2. Klasifikasi Naive Bayes

Untuk mengetahui tingkat kesadaran cyber responden, data kuesioner dianalisis menggunakan algoritma Multinomial Naive Bayes. Responden diklasifikasikan ke dalam dua kategori: waspada dan tidak waspada. Hasil klasifikasi ditunjukkan pada Tabel 4.5.

Tabel 4.5. Hasil Klasifikasi Kesadaran Cyber Gen-Z Mataram

Kategori Kesadaran	Jumlah	Persentase
Waspada	38	38%
Tidak Waspada	62	62%
Total	100	100%

Berdasarkan tabel tersebut, mayoritas responden (62%) dikategorikan tidak waspada. Hal ini menandakan bahwa tingkat kesadaran cyber Gen-Z di Mataram masih rendah meskipun intensitas penggunaan internet mereka tinggi.

4.3. Model Confusion Matrix

Evaluasi dilakukan dengan membandingkan hasil prediksi model dengan data aktual menggunakan confusion matrix. Hasil pengujian ditunjukkan pada Tabel 4.6.

Tabel 4.6. Confusion Matrix Model Naive Bayes

	Prediksi Waspada	Prediksi Tidak Waspada
Aktual Waspada	7	2
Aktual Tidak Waspada	1	10

Dari tabel di atas dapat diketahui bahwa model berhasil mengklasifikasikan 17 dari 20 data uji dengan benar. Hanya terdapat 3 kesalahan prediksi (misclassifications), yang terdiri dari 2 kasus False Negative dan 1 kasus False Positive.

4.4. Akurasi dan Matrix Evaluasi

Berdasarkan confusion matrix, diperoleh hasil evaluasi seperti ditunjukkan pada Tabel 4.7.

Tabel 4.7. Ringkasan Evaluasi Model Naive Bayes

Metrik	Nilai
Akurasi	85%
Precision	0,875
Recall	0,777
F1-Score	0,823

Tabel ini menunjukkan bahwa model Naive Bayes memiliki akurasi cukup tinggi, yakni 85%. Precision yang mendekati 0,9 menunjukkan model sangat baik dalam memprediksi responden yang benar-benar waspada, meskipun recall sedikit lebih rendah karena ada beberapa responden waspada yang gagal terdeteksi.

Hasil penelitian menunjukkan bahwa mayoritas Gen-Z di Mataram tergolong tidak waspada terhadap ancaman cyber meskipun tingkat intensitas penggunaan internet mereka tinggi. Temuan ini konsisten dengan laporan Kaspersky (2023) dan penelitian Lee & Cho (2022), yang sama-sama menyatakan rendahnya kesadaran cyber di kalangan generasi muda.

Kinerja algoritma Multinomial Naive Bayes dengan akurasi 85%

menunjukkan efektivitasnya dalam klasifikasi data kategorikal berbasis kuesioner. Hal ini sejalan dengan penelitian Siliayani et al. (2020) dan Rayuwati et al. (2022), yang menegaskan bahwa Naive Bayes mampu menghasilkan performa baik meskipun dataset relatif kecil.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil penelitian mengenai kesadaran Generasi Z terhadap ancaman cyber melalui studi kasus di Kota Mataram tahun 2025 dengan menggunakan algoritma Multinomial Naive Bayes, dapat disimpulkan beberapa hal sebagai berikut:

Sebagian besar responden berasal dari kelompok usia 21–23 tahun (40%), dengan distribusi gender yang relatif seimbang (52% perempuan, 48% laki-laki). Intensitas penggunaan internet tergolong tinggi, di mana 58% responden menggunakan internet lebih dari 6 jam per hari. Kondisi ini memperlihatkan bahwa Gen-Z di Mataram merupakan digital natives dengan tingkat keterpaparan yang sangat tinggi terhadap aktivitas daring.

Hasil klasifikasi menunjukkan bahwa mayoritas responden (62%) tergolong tidak waspada terhadap ancaman cyber, sedangkan hanya 38% yang dapat dikategorikan waspada. Fakta ini menegaskan bahwa meskipun Gen-Z mahir dalam penggunaan teknologi, kesadaran mereka terhadap risiko keamanan siber masih rendah.

Sebanyak 62% responden mengaku pernah mengalami ancaman siber, seperti phishing, malware, atau interaksi mencurigakan melalui sistem CAPTCHA. Hal ini memperlihatkan bahwa ancaman cyber bukan lagi potensi, melainkan sudah menjadi pengalaman nyata yang dialami oleh mayoritas Gen-Z di Mataram.

Model Multinomial Naive Bayes mampu mengklasifikasikan kesadaran cyber dengan akurasi sebesar 85%. Nilai precision (0,875) lebih tinggi dibandingkan recall (0,777), yang berarti model lebih baik dalam mengidentifikasi responden yang benar-benar waspada dibandingkan mendeteksi semua responden yang waspada. F1-score sebesar 0,823 menunjukkan performa model cukup seimbang antara precision dan recall.

Hasil penelitian ini memperkuat temuan sebelumnya bahwa Gen-Z rentan terhadap ancaman siber meskipun dianggap generasi paling melek teknologi. Implikasi praktisnya adalah perlunya edukasi keamanan siber yang lebih intensif, baik melalui institusi pendidikan maupun program literasi digital dari pemerintah daerah.

5.2 . Saran

Dari hasil penelitian, beberapa saran yang dapat diberikan adalah:

1. **Bagi Pendidikan Tinggi di Mataram**

   Perguruan tinggi dapat memasukkan materi keamanan siber ke dalam kurikulum, baik melalui mata kuliah wajib maupun pelatihan tambahan, agar mahasiswa memiliki literasi digital yang lebih baik.

2. **Bagi Pemerintah Daerah**

   Pemerintah Kota Mataram bersama Dinas Komunikasi dan Informatika dapat menyelenggarakan program literasi digital khusus Gen-Z, yang menekankan pada praktik keamanan siber sehari-hari, seperti manajemen password, pengenalan phishing, dan keamanan CAPTCHA.

3. **Bagi Pengembang Teknologi**

   Penyedia layanan digital sebaiknya meningkatkan sistem keamanan, khususnya pada fitur CAPTCHA, agar

tidak mudah dieksploitasi oleh pihak ketiga. Edukasi kepada pengguna mengenai potensi manipulasi CAPTCHA juga perlu ditingkatkan.

4. **Bagi Peneliti Selanjutnya**

Penelitian mendatang dapat memperluas jumlah sampel dan wilayah, serta membandingkan kesadaran cyber antar generasi (misalnya Gen-Z vs. Milenial). Selain itu, dapat pula digunakan algoritma machine learning lain seperti Decision Tree, Random Forest, atau Support Vector Machine (SVM) untuk membandingkan performa dengan Naive Bayes.

DAFTAR PUSTAKA:

APJII. (2024). *Laporan Survei Penetrasi & Perilaku Pengguna Internet Indonesia 2024.* Asosiasi Penyelenggara Jasa Internet Indonesia.

BSSN. (2024). *Laporan Tahunan Keamanan Siber Indonesia 2024. Badan Siber dan Sandi Negara Republik Indonesia.*

Anwar, R. (2024). *Paling Melek Teknologi, Milenial & Gen-Z Perlu Sadar Keamanan Data Pribadi.* CNN Indonesia.

APJII. (2024). *Laporan Survei Penetrasi & Perilaku Pengguna Internet Indonesia 2024*. Jakarta: Asosiasi Penyelenggara Jasa Internet Indonesia.

Badan Pusat Statistik (BPS). (2024). *Statistik Kota Mataram 2024*. Mataram: BPS Kota Mataram.

BSSN. (2024). *Laporan Tahunan Keamanan Siber Indonesia 2024*. Badan Siber dan Sandi Negara Republik Indonesia.

Fadillah, R., & Sukmana, I. (2022). *Implementasi Naive Bayes untuk Klasifikasi Data Teks*. Jurnal Teknologi Informasi, 18(2), 45–55.

Howe, N., & Strauss, W. (1991). *Generations: The History of America's Future, 1584 to 2069*. New York: Harper Collins.

Kaspersky. (2023). *Mengapa 72% Gen-Z di Indonesia Tidak Dapat Mengidentifikasi Phishing*. Kaspersky Security Report.

Lee, S., & Cho, J. (2022). *Cybersecurity Awareness Among Generation Z*. Journal of Information Security, 11(3), 221–233.

Purwani, D. (2023). *Ancaman Siber di Indonesia: Tren dan Strategi Penanggulangan*. Jurnal Keamanan Informasi, 9(1), 12–25.

Rayuwati, E., et al. (2022). *Analisis Sentimen Media Sosial Menggunakan Naive Bayes*. Jurnal Sistem Informasi, 14(2), 89–101.

Siliayani, N., et al. (2020). *Implementasi Naive Bayes untuk Klasifikasi Data Kategorikal*. Jurnal Teknologi Komputer, 5(1), 33–42.

Von Ahn, L., Blum, M., Hopper, N. J., & Langford, J. (2003). *CAPTCHA: Using Hard AI Problems for Security*. Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, 294–311.