Jurnal Minfo Polgan
Volume 12, Nomor 1, Maret 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12379
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Terbit : 30-Maret-2023

Aplikasi Deteksi Phising Berbasis Android Menggunakan Metode Pengembangan Perangkat Lunak DSRM

Rangga Gelar Guntara[1)*]
[1)]Universitas Pendidikan Indonesia, Indonesia
[1)]ranggagelar@upi.edu

Abstrak :
Penggunaan pesan spam atau phishing yang masuk melalui SMS semakin meningkat dalam beberapa tahun terakhir dan telah menjadi masalah keamanan yang serius bagi pengguna perangkat seluler. Untuk mengatasi masalah ini, dilakukan penelitian untuk mengembangkan aplikasi deteksi phishing SMS berbasis android menggunakan algoritma Naive Bayes dengan menggunakan metode penelitian pengembangan perangkat lunak DSRM. Model pengembangan perangkat lunak DSRM fokus pada pengembangan perangkat lunak yang cepat dan terus berubah sesuai dengan kebutuhan pelanggan yang berkembang. Penelitian ini dilakukan dengan menggunakan metode pengumpulan data SMS yang dilabeli phishing dan non-phishing, melakukan preprocessing data, pembuatan model Naive Bayes, serta desain dan implementasi aplikasi android. Pengujian dilakukan dengan menggunakan dataset yang berbeda-beda dan teknik cross validation. Hasil pengujian menunjukkan bahwa aplikasi dapat melakukan deteksi dengan akurasi yang baik, sensitivitas dan spesifisitas yang baik, serta waktu respons yang cepat. Aplikasi ini dapat membantu pengguna perangkat seluler dalam menghindari pesan phishing atau spam yang merugikan.

Kata kunci :
phising; android; naïve bayes; DSRM; preprocessing

PENDAHULUAN

Perkembangan aplikasi Android saat ini sangat pesat, seiring dengan pertumbuhan pengguna smartphone Android di seluruh dunia (Pohan et al., 2022). Dalam beberapa tahun terakhir, jumlah aplikasi Android yang tersedia di Google Play Store meningkat dengan pesat dan telah mencapai lebih dari 3,8 juta aplikasi pada akhir 2020 (Tapaningsih et al., 2022). Aplikasi Android telah menjadi bagian integral dari kehidupan sehari-hari dan digunakan untuk berbagai tujuan, mulai dari bisnis hingga hiburan dan Pendidikan (Guntara, 2022b).

Aplikasi Android menawarkan keuntungan yang luar biasa dalam hal kemudahan penggunaan, fleksibilitas, dan keterjangkauan (Guntara, 2022a). Selain itu, fitur-fitur canggih seperti AI, AR, VR, dan IoT juga semakin terintegrasi dalam aplikasi Android, membuka peluang baru bagi pengembang aplikasi untuk menciptakan pengalaman yang lebih menarik dan interaktif bagi pengguna (Agusriadi & Finot, 2022).

Perkembangan teknologi seperti 5G, AI, dan IoT juga memberikan peluang baru dalam pengembangan aplikasi Android, yang memungkinkan pengembang untuk mengembangkan aplikasi yang lebih kompleks dan inovatif (Lestari et al., 2022). Selain itu, model bisnis berbasis aplikasi seperti freemium, iklan dalam aplikasi, dan pembelian dalam aplikasi semakin populer dan menawarkan peluang bagi pengembang aplikasi untuk memperoleh penghasilan (Suryawirawan et al., 2022).

Namun, dalam mengembangkan aplikasi Android, penting untuk memperhatikan aspek keamanan dan privasi pengguna (Sari et al., 2022), mengikuti standar dan pedoman Android, dan terus memperbarui aplikasi agar tetap relevan dan sesuai dengan perkembangan teknologi. Salah satu kejahatan dalam aplikasi android adalah adanya teknik phising. Phishing SMS atau pesan teks phishing semakin sering terjadi dan semakin merugikan para pengguna ponsel. Phishing SMS adalah salah satu bentuk serangan siber yang dilakukan dengan mengirimkan pesan teks yang mengelabui pengguna agar memberikan informasi rahasia atau data pribadi mereka, seperti nomor kartu kredit, password, atau nomor identitas pribadi.

Untuk melindungi para pengguna ponsel dari serangan phishing SMS, perlu dilakukan deteksi otomatis terhadap pesan-pesan yang dicurigai sebagai phishing SMS. Salah satu cara untuk melakukan deteksi phishing SMS adalah dengan menggunakan algoritma Naive Bayes. Algoritma Naive Bayes digunakan dalam deteksi phishing SMS karena kemampuannya dalam mengklasifikasikan data ke dalam dua kategori yaitu phishing atau

*penulis korespondensi

Jurnal Minfo Polgan
Volume 12, Nomor 1, Maret 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12379
e-ISSN : 2797-3298
p-ISSN : 2089-9424

bukan phishing. Algoritma Naive Bayes memperhitungkan kemungkinan terjadinya setiap fitur pada setiap kelas target, dan kemudian menggabungkan probabilitas tersebut untuk menghitung probabilitas kelas target yang paling mungkin terjadi. Fitur-fitur yang digunakan dalam model Naive Bayes untuk deteksi phishing SMS meliputi panjang SMS, jumlah tautan dalam SMS, jumlah kata kunci dalam SMS, dan jarak Levenshtein antara SMS dan pesan phishing.

Dalam artikel ini, akan membahas bagaimana mengembangkan aplikasi Android untuk deteksi phising sms dan mengulas bagaimana pengembangan aplikasi Android menggunakan DSRM dapat membantu pengembang untuk membangun aplikasi yang lebih baik, efisien, dan efektif.

TINJAUAN PUSTAKA

Aplikasi Android

Berdasarkan penelitian (Nugroho et al., 2022) menyatakan bahwa aplikasi Android adalah perangkat lunak yang dirancang dan dikembangkan khusus untuk berjalan pada sistem operasi Android yang digunakan pada smartphone, tablet, dan perangkat mobile lainnya. Aplikasi Android dapat diunduh dan diinstal dari Google Play Store atau sumber lainnya.

Pengembangan aplikasi Android melibatkan proses perancangan, pengembangan, pengujian, dan penyebaran aplikasi ke pasar. Proses ini melibatkan pengembang yang menggunakan berbagai bahasa pemrograman dan platform pengembangan untuk membuat aplikasi yang sesuai dengan kebutuhan pengguna (Maliki, 2021).

Application Programming Interface (API)

API adalah singkatan dari Application Programming Interface, yaitu antarmuka atau sekumpulan protokol, aturan, dan instruksi yang digunakan oleh sebuah perangkat lunak untuk berkomunikasi dengan perangkat lunak lainnya (Rangga Gelar Guntara, 2022). API berfungsi sebagai penghubung antara aplikasi dengan sumber daya yang tersedia, seperti server, database, atau perangkat keras.

API memungkinkan pengembang aplikasi untuk mengakses fitur dan sumber daya yang tersedia pada perangkat lunak lainnya tanpa harus mengetahui bagaimana fitur tersebut dibuat atau bagaimana data dihasilkan. Dengan kata lain, API memungkinkan pengembang untuk menggunakan fungsionalitas yang sudah ada dan mengintegrasikannya ke dalam aplikasi mereka sendiri tanpa harus membangun fitur dari awal (Hasanuddin et al., 2022).

Phising

Phishing adalah suatu metode penipuan yang dilakukan oleh pelaku cybercrime untuk memperoleh informasi pribadi seperti username, password, nomor kartu kredit, atau data sensitif lainnya dengan cara membuat situs web atau halaman palsu yang meniru tampilan situs web asli (Jonathan et al., 2020).

Biasanya, pelaku phishing akan mengirimkan email palsu atau pesan teks yang mengatasnamakan perusahaan atau organisasi resmi untuk mengelabui korbannya agar mengklik tautan menuju situs web palsu. Situs web palsu tersebut dirancang sedemikian rupa sehingga sangat mirip dengan situs web asli, sehingga korban terkecoh dan memasukkan informasi pribadi mereka seperti nama pengguna dan kata sandi.

Algoritma Naïve Bayes

Naive Bayes adalah salah satu algoritma klasifikasi yang populer digunakan dalam bidang machine learning, terutama dalam klasifikasi teks dan data yang berkategori (Ferdi & Vina Ayumi, 2023). Algoritma ini didasarkan pada teorema Bayes dan menghitung probabilitas kelas target berdasarkan probabilitas fitur yang terkait dengan kelas target tersebut.

Secara umum, algoritma Naive Bayes bekerja dengan menghitung probabilitas kelas target yang akan diprediksi berdasarkan fitur-fitur yang terdapat pada data input. Naive Bayes memperhitungkan kemungkinan terjadinya setiap fitur pada setiap kelas target, dan kemudian menggabungkan probabilitas tersebut untuk menghitung probabilitas kelas target yang paling mungkin terjadi.

METODE PENELITIAN

Metode penelitian yang digunakan pada pengembangan aplikasi ini adalah DSRM. DSRM (Dynamic Systems Development Method) adalah salah satu model pengembangan perangkat lunak yang termasuk ke dalam kategori model pengembangan perangkat lunak Agile. Model pengembangan perangkat lunak DSRM fokus pada pengembangan perangkat lunak yang cepat dan terus berubah sesuai dengan kebutuhan pelanggan yang berkembang (Javdani Gandomani et al., 2022).

Berikut adalah tahapan pengembangan aplikasi Android menggunakan model DSRM:

*penulis korespondensi

Jurnal Minfo Polgan
Volume 12, Nomor 1, Maret 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12379
e-ISSN : 2797-3298
p-ISSN : 2089-9424

1. Tahap Pra-proyek
   a. Identifikasi kebutuhan bisnis: pada tahap ini, tim pengembang harus mengidentifikasi kebutuhan bisnis dari aplikasi Android yang akan dikembangkan, seperti tujuan aplikasi, target pengguna, fitur dan fungsionalitas yang diperlukan, serta batasan dan kendala proyek.
   b. Penentuan scope proyek: setelah kebutuhan bisnis diidentifikasi, tim pengembang harus menentukan scope proyek yang akan dikembangkan, termasuk batas waktu dan sumber daya yang tersedia.
   c. Analisis risiko: tim pengembang harus menganalisis risiko yang mungkin terjadi selama pengembangan aplikasi Android.
2. Tahap Fase Perencanaan
   a. Merencanakan pengembangan: pada tahap ini, tim pengembang membuat rencana pengembangan detail, termasuk penjadwalan proyek, alokasi sumber daya, dan definisi tujuan yang jelas.
   b. Penentuan kebutuhan: tim pengembang harus mengidentifikasi kebutuhan teknis untuk aplikasi Android, seperti platform, bahasa pemrograman, dan alat pengembangan yang akan digunakan.
   c. Pembuatan spesifikasi: pada tahap ini, tim pengembang membuat spesifikasi teknis dan fungsionalitas aplikasi yang akan dikembangkan.
3. Tahap Fase Model Iterasi
   a. Desain: pada tahap ini, tim pengembang merancang antarmuka pengguna dan arsitektur aplikasi Android yang akan dikembangkan.
   b. Implementasi: pada tahap ini, tim pengembang mulai mengimplementasikan fitur dan fungsionalitas aplikasi Android yang telah dirancang.
   c. Evaluasi: pada akhir setiap iterasi, tim pengembang melakukan evaluasi dan pengujian terhadap aplikasi yang telah dikembangkan.
4. Tahap Fase Evaluasi dan Pemeliharaan
   a. Evaluasi: pada tahap ini, tim pengembang melakukan evaluasi akhir terhadap aplikasi Android yang telah dikembangkan.
   b. Pemeliharaan: setelah aplikasi Android dirilis, tim pengembang akan melakukan pemeliharaan terhadap aplikasi dan memperbaiki bug atau masalah yang ditemukan.

Sedangkan tahapan dalam pengembangan aplikasi Android pendeteksi spam SMS, Anda dapat mengikuti langkah-langkah berikut:

1. Membuat UI (User Interface) untuk aplikasi Anda. Anda dapat menggunakan Android Studio untuk membuat UI yang menarik dan mudah digunakan. Pastikan Anda menyertakan fitur untuk memindai pesan masuk dan menampilkan hasil deteksi.
2. Membuat logika deteksi spam SMS. Anda dapat menggunakan teknik Machine Learning atau Artificial Intelligence untuk melatih model Anda agar dapat mengenali spam SMS. Ada banyak dataset spam SMS yang tersedia di internet yang dapat Anda gunakan untuk melatih model Anda.
3. Membuat kode untuk memindai pesan masuk. Anda perlu membuat kode untuk membaca pesan masuk dan memindainya untuk menentukan apakah itu spam atau tidak. Anda dapat menggunakan API SMS Android untuk membaca pesan masuk.
4. Menampilkan hasil deteksi. Setelah memindai pesan masuk, Anda dapat menampilkan hasil deteksi pada UI aplikasi Anda. Anda dapat menampilkan pesan masuk yang telah diklasifikasikan sebagai spam atau tidak spam, dan memberikan opsi kepada pengguna untuk memblokir atau menghapus pesan tersebut.
5. Meningkatkan aplikasi Anda. Setelah aplikasi Anda selesai dibuat, pastikan untuk menguji aplikasi Anda dengan cermat dan mengumpulkan umpan balik dari pengguna Anda. Anda dapat menggunakan umpan balik ini untuk meningkatkan aplikasi Anda dan membuatnya lebih efektif dalam mendeteksi spam SMS.

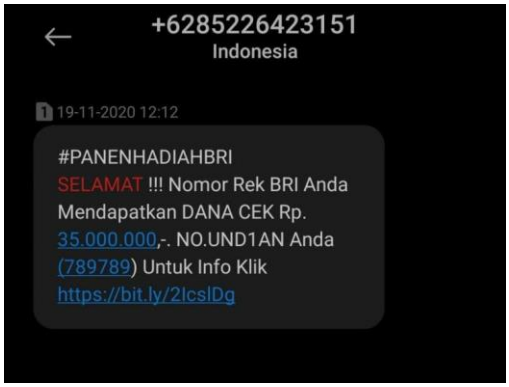
HASIL PENELITIAN DAN DISKUSI

Pengumpulan Data

Pertama-tama, perlu melakukan pengumpulan data berupa dataset SMS dengan label phishing atau tidak phishing. Dataset ini akan digunakan untuk melatih model Naive Bayes. Dataset dapat diperoleh dengan cara melakukan crawling SMS atau meminta kerjasama dengan pihak yang memiliki data SMS. Proses pengumpulan data sms pada penelitian ini dengan cara menggunakan sms reader yaitu membaca semua SMS yang masuk pada perangkat Android dan mengembalikan hasilnya dalam bentuk string.

*penulis korespondensi

Jurnal Minfo Polgan
Volume 12, Nomor 1, Maret 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12379
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 1. Contoh isi sms phising

Preprocessing Data

Setelah memperoleh dataset, langkah selanjutnya adalah melakukan preprocessing data. Preprocessing data dapat dilakukan dengan cara membersihkan data dari karakter-karakter yang tidak diperlukan, melakukan tokenisasi, menghapus stopword, dan melakukan stemming atau lemmatization. Preprocessing data bertujuan untuk memudahkan pengolahan data selanjutnya. Berikut adalah kode untuk melakukan preprocessing data:

```
public class Preprocessing {
    public static List<String> preprocess(String smsText) {
        // Menghapus karakter-karakter yang tidak diperlukan
        String cleanedText = smsText.replaceAll("[^a-zA-Z\\s]", "");

        // Konversi menjadi huruf kecil
        cleanedText = cleanedText.toLowerCase();

        // Tokenisasi
        String[] tokens = cleanedText.split("\\s+");

        // Menghapus stopword
        List<String> stopWords = Arrays.asList("dan", "atau", "yang", "di", "ke", "dari", "untuk", "dengan");
        List<String> filteredTokens = new ArrayList<>();
        for (String token : tokens) {
            if (!stopWords.contains(token)) {
                filteredTokens.add(token);
            }
        }

        // Stemming
        PorterStemmer stemmer = new PorterStemmer();
        List<String> stemmedTokens = new ArrayList<>();
        for (String token : filteredTokens) {
            stemmer.setCurrent(token);
            stemmer.stem();
            stemmedTokens.add(stemmer.getCurrent());
        }

        return stemmedTokens;
    }
}
```

Pembuatan Model Naïve Bayes

Setelah melakukan preprocessing data, langkah selanjutnya adalah membuat model Naive Bayes. Pada tahap ini, dataset yang telah diolah akan dibagi menjadi dua bagian, yaitu data latih (training data) dan data uji (test data).

*penulis korespondensi

Jurnal Minfo Polgan
Volume 12, Nomor 1, Maret 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12379
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Data latih akan digunakan untuk melatih model Naive Bayes, sedangkan data uji akan digunakan untuk menguji performa model.

```
private boolean isPhishing(String sms) {
    // Buat model Naive Bayes
    NaiveBayes nb = new NaiveBayes();

    // Definisikan atribut yang digunakan dalam model
    Attribute lengthAttr = new Attribute("length");
    Attribute linkCountAttr = new Attribute("linkCount");
    Attribute keywordCountAttr = new Attribute("keywordCount");
    Attribute levenshteinAttr = new Attribute("levenshteinDistance");
```

Integrasi Model dengan Aplikasi

Setelah model Naive Bayes berhasil dibuat, langkah selanjutnya adalah mengintegrasikan model dengan aplikasi Android. Pada tahap ini, model Naive Bayes akan diimplementasikan ke dalam aplikasi Android dan diuji coba dengan data uji.

Pengujian Aplikasi

Pada tahap ini, aplikasi akan diuji coba menggunakan data uji yang telah dipisahkan sebelumnya. Pengujian aplikasi bertujuan untuk mengevaluasi performa aplikasi dan memastikan aplikasi dapat mendeteksi phishing SMS dengan akurat.

Pelatihan Model

Jika hasil pengujian tidak memuaskan, langkah selanjutnya adalah melakukan pelatihan model ulang dengan dataset yang lebih banyak dan bervariasi. Setelah melakukan pelatihan model ulang, langkah selanjutnya adalah mengintegrasikan model baru ke dalam aplikasi dan menguji coba kembali.

Peningkatan Aplikasi

Setelah aplikasi berhasil memenuhi persyaratan performa yang diinginkan, langkah selanjutnya adalah melakukan peningkatan aplikasi agar lebih mudah digunakan dan lebih efektif dalam mendeteksi phishing SMS. Hal ini dapat dilakukan dengan menambahkan fitur-fitur tambahan yang relevan atau melakukan perbaikan pada antarmuka pengguna.

Perancangan UI/UX Aplikasi

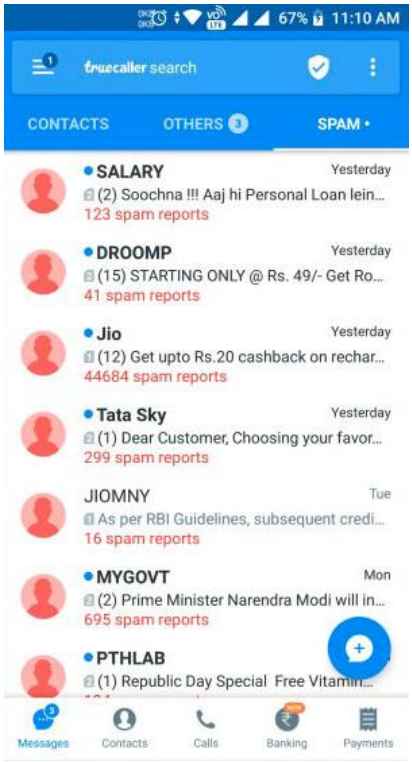
Perancangan UI/UX aplikasi deteksi phishing SMS di Android ini dilakukan dengan mempertimbangkan beberapa hal sebagai berikut:

1. Simplicity: Usahakan agar antarmuka aplikasi mudah dipahami dan sederhana, sehingga pengguna tidak merasa kesulitan atau bingung saat menggunakan aplikasi.
2. Clarity: Pastikan semua informasi yang disajikan di antarmuka aplikasi mudah dibaca dan dipahami, sehingga pengguna dapat mengetahui dengan jelas informasi yang ditampilkan.
3. Navigation: Susun antarmuka aplikasi dengan tata letak yang intuitif dan mudah dinavigasi, sehingga pengguna dapat dengan mudah menemukan fitur yang mereka butuhkan.
4. Consistency: Pastikan seluruh elemen desain aplikasi konsisten dan memiliki kesamaan dalam tampilan dan fungsinya.
5. Color scheme: Pilih skema warna yang sesuai dengan tujuan aplikasi dan membuatnya terlihat menarik bagi pengguna.
6. Typography: Pilih jenis huruf yang mudah dibaca dan tidak terlalu kecil, sehingga pengguna dapat membaca informasi dengan jelas.
7. Feedback: Berikan umpan balik yang jelas dan mudah dimengerti oleh pengguna, sehingga mereka dapat memahami apakah aplikasi sedang memproses informasi atau telah menyelesaikan tugas.

Dengan mempertimbangkan faktor-faktor di atas, maka antarmuka aplikasi deteksi phishing SMS di Android dapat dibuat dengan mudah dan user-friendly.

*penulis korespondensi

Jurnal Minfo Polgan
Volume 12, Nomor 1, Maret 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12379
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 2. Rancangan UI/UX Aplikasi

Hasil Pengujian Aplikasi

Pengujian aplikasi sangat penting untuk memastikan aplikasi deteksi phishing SMS di Android yang Anda kembangkan dapat bekerja dengan baik dan memberikan hasil yang akurat. Berikut adalah beberapa tahapan yang dapat dilakukan untuk melakukan pengujian aplikasi:

1. Pengujian Fungsional
   Pastikan semua fitur pada aplikasi berfungsi dengan baik. Coba masukkan pesan SMS yang termasuk dalam kategori phishing dan juga pesan SMS yang tidak termasuk dalam kategori phishing dan pastikan aplikasi memberikan hasil yang sesuai.
2. Pengujian Kinerja
   Uji kinerja aplikasi dengan memasukkan sejumlah pesan SMS untuk dianalisis. Pastikan aplikasi memberikan hasil deteksi dengan waktu respons yang cepat.
3. Pengujian Kecocokan
   Uji aplikasi dengan berbagai macam jenis pesan SMS dan pastikan hasil deteksi yang diberikan konsisten dan akurat.
4. Pengujian Keamanan
   Pastikan aplikasi aman dan tidak membahayakan pengguna. Uji aplikasi dengan memasukkan pesan SMS palsu dan pastikan aplikasi tidak memberikan hasil deteksi yang salah.
5. Pengujian Antarmuka
   Pastikan antarmuka pengguna aplikasi mudah digunakan dan intuitif. Uji aplikasi dengan beberapa pengguna dan minta feedback mengenai desain antarmuka pengguna.

Selain itu, pastikan juga untuk melakukan uji coba pada berbagai versi perangkat Android, mulai dari versi yang lebih lama hingga versi yang terbaru untuk memastikan aplikasi dapat berjalan dengan baik pada semua perangkat.

Dalam melakukan pengujian, juga dapat menggunakan metode seperti black box testing dan white box testing untuk memastikan semua aspek aplikasi telah diuji secara menyeluruh. Setelah semua pengujian selesai dilakukan, pastikan untuk membuat laporan pengujian dan mengidentifikasi bug atau masalah yang ditemukan untuk diperbaiki pada versi selanjutnya.

*penulis korespondensi

Jurnal Minfo Polgan
Volume 12, Nomor 1, Maret 2023
DOI : https://doi.org/10.33395/jmp.v12i1.12379
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Tabel 1
Hasil Pengujia blackbox

No	Aktivitas Pengujian	Realisasi yang Diharapkan	Hasil Pengujian	Kesimpulan
1	Tampilkan data sms	Tampilan list inbox sms	Menampilkan list inbox sms	Terpenuhi
2	Tampilkan keterangan phising	Tampilan keterangan label phising dan bukan phising	Menampilkan keterangan label phising dan bukan phising	Terpenuhi
3	Hapus SMS phising	Tampilan pesan hapus sms berhasil	Menampilkan pesan hapus sms berhasil	Terpenuhi
4	Latih Model	Tampilan pesan latih model	Menampilkan pesan latih model	Terpenuhi

KESIMPULAN

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa aplikasi deteksi phishing SMS berbasis android menggunakan algoritma Naive Bayes dapat digunakan untuk mendeteksi pesan SMS yang mengandung phishing dengan akurasi yang baik. Penggunaan metode preprocessing data dan pembuatan model Naive Bayes memberikan hasil yang baik dalam mengklasifikasikan pesan SMS. Selain itu, aplikasi ini juga memiliki waktu respons yang cepat dan dapat membantu pengguna perangkat seluler dalam menghindari pesan phishing atau spam yang merugikan. Oleh karena itu, pengembangan aplikasi ini dapat dijadikan alternatif untuk meningkatkan keamanan pengguna perangkat seluler dalam menghadapi ancaman pesan SMS yang tidak diinginkan. Namun, perlu dilakukan penelitian lebih lanjut untuk memperbaiki performa deteksi dan meningkatkan jumlah dataset untuk mendapatkan hasil yang lebih akurat dan lebih luas cakupannya.

REFERENSI

Agusriadi, E., & Finot. (2022). Sistem Pakar dalam Menganalisis Penyakit Organ dan Jaringan Tubuh dengan Metode Perceptron dan Fitur Augmented Reality. *Jurnal Informasi Dan Teknologi*, 39–45. https://doi.org/10.37034/jidt.v4i1.180

Ferdi, & Vina Ayumi. (2023). ANALISA SENTIMEN MENGENAI KENAIKAN HARGA BBM MENGGUNAKAN METODE NAÏVE BAYES DAN SUPPORT VECTOR MACHINE. *JSAI (Journal Scientific and Applied Informatics)*, *6*(1), 1–10. https://doi.org/10.36085/jsai.v6i1.4628

Guntara, R. G. (2022a). Ekstraksi Fitur Warna Citra Daun Untuk Klasifikasi Skala Klorofil dan Rekomendasi Pemupukan. *Jurnal Minfo Polgan*, *11*(1), 15–22. https://doi.org/10.33395/jmp.v11i1.11644

Guntara, R. G. (2022b). Aplikasi Pengenalan Citra Wajah di KTP Menggunakan Google Cloud Vision API dan Kairos API Berbasis Android. *ILKOMNIKA: Journal of Computer Science and Applied Informatics*, *4*(2), 198–207. https://doi.org/10.28926/ilkomnika.v4i2.504

Hasanuddin, Asgar, H., & Hartono, B. (2022). RANCANG BANGUN REST API APLIKASI WESHARE SEBAGAI UPAYA MEMPERMUDAH PELAYANAN DONASI KEMANUSIAAN. *Jurnal Informatika Teknologi Dan Sains*, *4*(1), 8–14. https://doi.org/10.51401/jinteks.v4i1.1474

Javdani Gandomani, T., Ziaei Nafchi, M., & M. Parizi, R. (2022). Empowering Software Startups with Agile Methods and Practices: A Design Science Approach. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4299858

Jonathan, K. M., Mulyawan, B., & Perdana, N. J. (2020). PERBANDINGAN KINERJA ALGORITMA NAÏVE BAYES DAN C4.5 UNTUK MENDETEKSI PENGELABUAN UNIFORM RESOURCE LOCATOR (PHISHING URL). *Jurnal Ilmu Komputer Dan Sistem Informasi*, *8*(1), 116. https://doi.org/10.24912/jiksi.v8i1.11479

Lestari, M. A., Ramli, A. M., & Ramli, T. S. (2022). TELAAH YURIDIS PENYELENGGARAAN TEKNOLOGI 5G DI INDONESIA: LANGKAH TRANSFORMASI MENUJU ERA SOCIETY 5.0. *Citizen : Jurnal Ilmiah Multidisiplin Indonesia*, *2*(1), 129–137. https://doi.org/10.53866/jimi.v2i1.49

Maliki, M. I. (2021). Rancang Bangun Aplikasi Penjualan Grosir Sembako Pada Toko LA-RIS. *Jurnal Informatika Dan Rekayasa Perangkat Lunak*, *2*(3), 304–311. https://doi.org/10.33365/jatika.v2i3.1222

Nugroho, S. A., Hadi, A. P., Rudjiono, R., & Zainudin, A. (2022). APLIKASI MOBILE LEARNING PEMBELAJARAN VIDEO EDITING BERBASIS ANDROID PADA PERSATUAN PEMUDA SANDYA

*penulis korespondensi

e-ISSN : 2797-3298
p-ISSN : 2089-9424

KARYA MUDA DESA REKSOSARI KEC SURUH KABUPATEN SEMARANG. *Pixel :Jurnal Ilmiah Komputer Grafis*, *15*(1), 196–205. https://doi.org/10.51903/pixel.v15i1.765

Pohan, A. B., Alfarobi, I., & Hadi, S. W. (2022). Pengembangan Idle Game "Havok Runner" Berbasis Android Menggunakan Metode Agile Game Development. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *6*(3), 1573. https://doi.org/10.30865/mib.v6i3.3994

Rangga Gelar Guntara. (2022). Aplikasi Pendeteksi Penyakit Telinga Berbasis Android menggunakan API Clarifai dan K-Nearest Neighbor. *Jurnal CoSciTech (Computer Science and Information Technology)*, *3*(2), 81–90. https://doi.org/10.37859/coscitech.v3i2.3862

Sari, M., Purnomo, H. D., & Sembiring, I. (2022). Review : Algoritma Kriptografi Sistem Keamanan SMS di Android. *Journal of Information Technology*, *2*(1), 11–15. https://doi.org/10.46229/jifotech.v2i1.292

Suryawirawan, O. A., Suhermin, S., & Shabrie, W. S. (2022). SERVICE QUALITY, SATISFACTION, CONTINUOUS USAGE INTENTION, AND PURCHASE INTENTION TOWARD FREEMIUM APPLICATIONS: THE MODERATING EFFECT OF PERCEIVED VALUE. *Jurnal Ekonomi Bisnis Dan Kewirausahaan*, *11*(3), 383. https://doi.org/10.26418/jebik.v11i3.57483

Tapaningsih, B. S., Esmawati, & Azzahra, F. (2022). Analisa Green Accounting pada Aplikasi GaloninAja dalam Upaya Mewujudkan SDGs. *Jurnal Akuntansi Dan Audit Syariah (JAAiS)*, *3*(2), 130–150. https://doi.org/10.28918/jaais.v3i2.5960

*penulis korespondensi