

**27/S/TEKKOM-KCBR/PK.03.08/16/AGUSTUS/2024**

**APLIKASI FILTRASI SPAM DAN PHISING PESAN WHATSAPP  
DENGAN METODE TF - IDF DAN MACHINE LEARNING**

**SKRIPSI**

diajukan untuk memenuhi sebagian syarat  
dalam memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer



Oleh

**Ferdinand Aprillian Manurung**

**NIM 2004930**

**PROGRAM STUDI S1 TEKNIK KOMPUTER**

**KAMPUS UPI DI CIBIRU**

**UNIVERSITAS PENDIDIKAN INDONESIA**

**2024**

**HALAMAN HAK CIPTA**  
**APLIKASI FILTRASI SPAM DAN PHISING PESAN WHATSAPP**  
**DENGAN METODE TF - IDF DAN MACHINE LEARNING**

Oleh  
Ferdinand Aprillian Manurung  
NIM 2004930

diajukan untuk memenuhi sebagian syarat dalam memperoleh gelar Sarjana  
Teknik pada Program Studi Teknik Komputer

© Ferdinand Aprillian Manurung  
Universitas Pendidikan Indonesia  
2024

Hak cipta dilindungi undang-undang Skripsi ini tidak boleh diperbanyak  
seluruhnya atau Sebagian dengan cetak ulang, difotokopi, atau cara lainnya tanpa  
ijin dari penulis

**HALAMAN PENGESAHAN**

**FERDINAND APRILLIAN MANURUNG**

**APLIKASI FILTRASI SPAM DAN PHISING PESAN WHATSAPP  
DENGAN METODE TF – IDF DAN MACHINE LEARNING**

Disetujui dan disahkan oleh pembimbing:

Pembimbing I



Dr. Eng. Munawir, S.Kom., M.T.

NIP. 920200819851205101

Pembimbing II

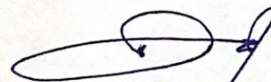


Deden Pradeka, S.T., M.Kom.

NIP. 920200419890816101

Mengetahui

Ketua Program Studi Teknik Komputer



Deden Pradeka, S.T., M.Kom.

NIP. 920200419890816101

## **PERNYATAAN KEASLIAN SKRIPSI DAN BEBAS PLAGIARISME**

Dengan ini saya menyatakan bahwa skripsi dengan judul “Aplikasi Filtrasi Spam dan *Phising* Pesan Whatsapp dengan Metode TF – IDF dan Machine Learning” ini beserta seluruh isinya adalah benar-benar karya sendiri. Saya tidak melakukan tindakan penjiplakan atau pengutipan dengan cara yang tidak sesuai dengan etika yang berlaku. Atas pernyataan ini, saya siap menanggung resiko apabila dikemudian hari ditemukan adanya pelanggaran etika keilmuan atau klaim dari pihak terhadap karya saya.

Bandung, 16 Agustus 2024

Yang membuat pernyataan

Ferdinand Aprillian Manurung

NIM 2004930

## UCAPAN TERIMA KASIH

*Bismillahirrahmanirrahim*, segala puji dan syukur bagi Allah SWT yang telah melimpahkan rahmat dan karunia-Nya kepada kita. Shalawat serta salam semoga tercurah limpahkan kepada Nabi Muhammad SAW, kepada keluarganya, sahabatnya, serta kita selaku umatnya hingga akhir zaman. Berkat rahmat dan karunia-Nya penulis dapat menyelesaikan skripsi dengan judul “Aplikasi Filtrasi Spam Dan *Phising* Pesan Whatsapp Dengan Metode TF – IDF Dan Machine Learning” dengan baik. Bimbingan, kritikan, dan masukan sangat berarti bagi penulis untuk menyempurnakan dan memperbaiki skripsi ini menjadi lebih baik.

Dalam penyusunan skripsi ini tentu tidak terlepas dari bantuan dan dukungan dari berbagai pihak. Dengan ini penulis mengucapkan terima kasih kepada:

1. Orang tua dan keluarga yang telah memuliakan penulis dan selalu memberikan dukungan dan pengertian;
2. Dr. Eng. Munawir, S.Kom., M.T. selaku dosen pembimbing I yang selalu meluangkan waktu, tenaga, dan pikirannya dalam membimbing;
3. Deden Pradeka, S.T., M.Kom. selaku dosen pembimbing II dan Ketua Program Studi Teknik Komputer yang selalu meluangkan waktu, tenaga, dan pikirannya dalam membimbing;
4. Ana Rahma Yuniarti, S.T., M.Eng. selaku Dosen Pembimbing Akademik yang selalu memberikan arahan dan bimbingan selama perkuliahan;
5. Prof. Dr. H. M. Solehuddin, M.Pd., MA. selaku Rektor Universitas Pendidikan Indonesia;
6. Prof. Dr. Deni Darmawan, M.Si., M.Kom., MCE selaku Direktur Universitas Pendidikan Indonesia Kampus Cibiru;
7. Bapak dan Ibu Dosen Teknik Komputer yang telah memberikan ilmu pengetahuannya;
8. Seluruh tenaga kependidikan Universitas Pendidikan Indonesia Kampus Cibiru;
9. Teman-teman seangkatan yang telah berjuang bersama-sama untuk kemajuan program studi Teknik Komputer dengan nama Taufik Hanafi Asnan, Dastin Aryo Atmanto, Rizki Nuriman, Ivan Rajwa Naufal, Rifty Pradana Gunawan, M. Dzulfikar Alhakim, M. Aksyal B. S., *The three musketeers*, Ihsan Naufal Munif,

Rahmawati, Anisa Nur Syafia, dan teman – teman lainnya yang tidak bisa disebutkan.

10. Kakak Tingkat dari program studi lain yang membimbing penulis selama menjalani kehidupan perkuliahan dengan nama Rizki Priutama, S.Pd., Riyadi Rafiki, S.Pd., Gumilang Pawitan, S.Pd., Rafif Raihansyah, S.Pd., dan Kakak – kakak lainnya yang tidak bisa disebutkan.
11. Himpunan Mahasiswa Teknik Komputer UPI Kampus di Cibiru yang menjadi tempat beristirahat dan berkembang penulis selama perkuliahan.
12. Ketua BE Himpunan Mahasiswa Teknik Komputer UPI Kampus Cibiru, saudara Farhan Naufal dan saudara Fatih Nurrobbil yang telah menjaga tempat penulis dengan sangat baik
13. Rekan – rekan kerja penulis di PT. Reka Cipta Solusi atas nama Oriza Naufal Harish, Yadhika Rizky F., Sani Ratna Aprillia, Gradiyanto Putera Husein, Ranis Aryanti, M. Luthfi Riyanto, M. Ikshan, Yudo H, Arif Hanafiah, M. Diaztando, Puji Adam Rizki, Zainun Amal Huda dan rekan – rekan kerja lainnya yang selalu mendukung penulis untuk menyediakan lingkungan yang nyaman untuk bekerja dan mengerjakan tugas akhir penulis dengan baik.

Penulis mengucapkan terima kasih atas segala bimbingan, arahan, masukan, nasihat, dan motivasi yang diberikan oleh semua pihak kepada peneliti. Semoga menjadi amal yang diberkahi oleh Allah SWT dan semoga Allah SWT membalas semua kebaikan yang telah diberikan. Aamiin.

Bandung, 16 Agustus 2024

Penulis

# APLIKASI FILTRASI SPAM DAN PHISING PESAN WHATSAPP DENGAN METODE TF – IDF DAN MACHINE LEARNING

Ferdinand Aprillian Manurung

2004930

## ABSTRAK

Pesatnya perkembangan teknologi komunikasi telah menyebabkan peningkatan jumlah pesan yang tidak diinginkan, seperti Spam dan *Phising*. Perkembangan tersebut masih belum dibarengi dengan adanya kesadaran pengguna akan dasar – dasar penggunaan teknologi. Ditambah penerapan hukum terhadap kejahatan melalui jaringan internet yang masih simpang siur menambah resiko pengguna menjadi korban dari kejahatan yang dilakukan melalui jaringan internet. Sebagai salah satu media Spam dan *Phising*, Penelitian ini bertujuan untuk mengembangkan aplikasi yang mampu memfilter pesan Spam dan *Phishing* pada WhatsApp menggunakan metode Term Frequency-Inverse Document Frequency (TF-IDF) dan *machine learning* dengan algoritma Random Forest. Aplikasi ini dikembangkan menggunakan arsitektur Model-View-ViewModel (MVVM), yang memungkinkan pemisahan logika bisnis dari antarmuka pengguna, sehingga meningkatkan efisiensi pengembangan dan pemeliharaan. Hasil penelitian menunjukkan bahwa kombinasi TF-IDF dan Random Forest memberikan tingkat akurasi yang tinggi dalam klasifikasi pesan Spam dan *Phishing*. Pengukuran menggunakan *confusion matrix* menunjukkan bahwa model memiliki akurasi sebesar 92 %. Dengan presisi, *recall*, dan F1 – *score* masing – masing 89%, 95%, 92 %, untuk kelas pesan yang aman dan 95%, 88%, 92%, untuk kelas pesan yang berbahaya. Integrasi antara model dan aplikasi juga berjalan dengan sangat baik terbukti dengan hasil pengujian dengan metode *black – box* yang semua skenarionya terpenuhi dan berhasil melakukan deteksi terhadap pesan pengujian dengan akurasi 98%. Diharapkan aplikasi yang dikembangkan mampu memberikan perlindungan yang lebih baik bagi pengguna WhatsApp dari ancaman digital.

**Kata Kunci** : Spam, Phishing, TF-IDF, Machine Learning, Random Forest, Arsitektur MVVM

# WHATSAPP MESSAGE SPAM FILTRATION AND PHISING APPLICATION USING TF – IDF AND MACHINE LEARNING METHOD

Ferdinand Aprillian Manurung

2004930

## ABSTRACT

*The rapid development of communication technology has led to an increase in the number of unwanted messages, such as Spam and Phishing. This development is still not accompanied by user awareness of the basics of using technology. In addition, the application of law regarding crimes via internet networks is still confusing, adding to the risk of internet network technology users falling victim to crimes via internet networks. As one of the Spam and Phishing media, this research aims to develop an application that is able to filter spam and phishing messages on WhatsApp using the TF-IDF (Term Frequency-Inverse Document Frequency) method and machine learning with the Random Forest model. The application is developed using the MVVM (Model-View-ViewModel) architecture, which allows separating business logic from the user interface, thereby increasing development and maintenance efficiency. The research results show that the combination of TF-IDF and Random Forest provides a high level of accuracy in classifying spam and phishing messages. Measurements using the confusion matrix show that the model has an accuracy of 92%. With precision, recall, and F1 – scores of 89%, 95%, 92%, respectively, for the safe message class and 95%, 88%, 92%, for the dangerous message class. The integration between the model and application also went very well as proven by the results of testing using the black-box method where all scenarios were met and successfully detected the test message with an accuracy of 98%. So, the application developed is able to provide better protection for WhatsApp users from digital threats.*

**Keyword :** *Spam, Phishing, TF-IDF, Machine Learning, Random Forest, MVVM Architecture*



## DAFTAR ISI

<b>HALAMAN HAK CIPTA</b> .....	i
<b>HALAMAN PENGESAHAN</b> .....	ii
<b>PERNYATAAN KEASLIAN SKRIPSI DAN BEBAS PLAGIARISME</b> .....	iii
<b>UCAPAN TERIMA KASIH</b> .....	iv
<b>ABSTRAK</b> .....	vi
<b>ABSTRACT</b> .....	vii
<b>DAFTAR ISI</b> .....	viii
<b>DAFTAR TABEL</b> .....	x
<b>DAFTAR GAMBAR</b> .....	xi
<b>DAFTAR PERSAMAAN</b> .....	xii
<b>DAFTAR LAMPIRAN</b> .....	i
<b>BAB I PENDAHULUAN</b> .....	2
<b>1.1 Latar Belakang Penelitian</b> .....	2
<b>1.2 Rumusan Masalah Penelitian</b> .....	7
<b>1.3 Tujuan Penelitian</b> .....	7
<b>1.4 Manfaat Penelitian</b> .....	7
1.4.1. Manfaat Teoritis .....	7
1.4.2. Manfaat Praktis .....	8
<b>1.5 Batasan Penelitian</b> .....	8
<b>1.6 Struktur Organisasi Skripsi</b> .....	9
<b>BAB II KAJIAN PUSTAKA DAN KERANGKA PEMIKIRAN</b> .....	11
<b>2.1 Kajian Pustaka</b> .....	11
2.1.1 Machine Learning .....	11
2.1.2 Pemanfaatan Metode Feature Extraction TF – IDF Data Teks.....	12
2.1.3 Implementasi Random Forest Sebagai Algoritma Klasifikasi.....	15
2.1.4 Implementasi Arsitektur MVVM Pada Aplikasi Android .....	16
2.1.5 Spam .....	19
2.1.6 Phising .....	20
2.1.7 Aplikasi Whatsapp .....	22
<b>2.2 Kerangka Pemikiran</b> .....	23
<b>2.3 Penelitian Terdahulu</b> .....	25

<b>BAB III METODE PENELITIAN .....</b>	<b>26</b>
<b>3.1 Metode Penelitian.....</b>	<b>26</b>
3.1.1 Analisis Kebutuhan Sistem.....	26
3.1.2 Perancangan Sistem.....	27
3.1.3 Pengembangan Sistem.....	31
3.1.4 Evaluasi Sistem.....	33
3.1.5 Penulisan Laporan .....	36
<b>3.2 Perangkat Penunjang Penelitian .....</b>	<b>36</b>
<b>BAB IV HASIL DAN PEMBAHASAN.....</b>	<b>38</b>
<b>4.1 Hasil Perancangan Model .....</b>	<b>38</b>
4.1.1 Model Filtrasi Spam dan Phising.....	38
4.1.2 Hasil Pengujian Model.....	40
<b>4.2 Hasil Perancangan aplikasi.....</b>	<b>43</b>
4.2.1 Aplikasi Filtrasi Spam dan Phising Android DOSA.....	43
4.2.2 Hasil Pengujian Aplikasi.....	50
<b>BAB V SIMPULAN, IMPLIKASI, DAN REKOMENDASI .....</b>	<b>57</b>
<b>5.1 Simpulan .....</b>	<b>57</b>
<b>5.2 Implikasi .....</b>	<b>57</b>
<b>5.3 Rekomendasi .....</b>	<b>57</b>
<b>DAFTAR PUSTAKA.....</b>	<b>58</b>
<b>LAMPIRAN.....</b>	<b>62</b>

## DAFTAR TABEL

Tabel 2. 1 Penelitian Terkait.....	25
tabel 4. 1 Hasil Pengukuran Performa Model .....	42
Tabel 4. 2 Hasil Pengujian Fungsional Aplikasi Dosa Menggunakan Teknik Equivalence Partitions .....	51
Tabel 4. 3 Hasil Pengujian Aplikasi Dosa Terhadap 100 Data Pesan Dalam Dataset.....	55
Tabel 4. 4 Hasil Pengujian Aplikasi Dosa Terhadap 40 Data Pesan Di Luar Dataset.....	56

## DAFTAR GAMBAR

Gambar 3. 1 Metode Penelitian .....	26
Gambar 3. 2 Diagram Sistem Aplikasi Filtrasi Pesan Spam Dan Phising .....	27
Gambar 3. 3 Metode Pengembangan Ai Project Cycle.....	28
Gambar 3. 4 Diagram Alir Aplikasi .....	30
Gambar 3. 5 Desain Antarmuka Pengguna A. Halaman Utama Aplikasi B. Halaman Detail Pesan Aplikasi.....	31
Gambar 4. 1 Kode Untuk Regex Pembersihan Karakter Pada Dataset .....	38
Gambar 4. 2 Kode Untuk Pembagian Data Menggunakan Method Train_Test_Split.....	39
Gambar 4. 3 Kode Konversi Model Scikit – Learn Menjadi Format .Onnx.....	40
Gambar 4. 14 Kode Confusion Matrix Model Machine Learning Filtrasi Spam Dan Phising .....	40
Gambar 4. 15 3 Grafik Confusion Matrix Model Filtrasi Spam Dan Phising .....	41
Gambar 4. 16 Grafik Nilai ROC .....	42
Gambar 4. 4 Kode Model Pada Aplikasi Dosa .....	44
Gambar 4. 5 Tampilan Aplikasi Dosa, Dari Kiri Tampilan Pesan Aman, Pesan – Pesan Yang Berasal Dari Pengirim Yang Sama, Dan Pesan Berbahaya .....	44
Gambar 4. 6 Fungsi Addsafenotification Pada Viewmodel Aplikasi Dosa.....	46
Gambar 4. 7 Fungsi Updatespamnotifications Pada Viewmodel Aplikasi Dosa ...	46
Gambar 4. 8 Kode Fetchlatestnotificationbytag .....	46
Gambar 4. 9 Kode Fetchnotificationsbytag .....	47
Gambar 4. 10 Kelas Notificationservice Dan Fungsi Override Fun Onnotificationposted.....	47
Gambar 4. 11 Fungsi Createortsession Dan Runprediction Untuk Melakukan Filtrasi Pesan.....	48
Gambar 4. 12 Fungsi Onnewnotification dan Onspamnewnotification.....	49
Gambar 4. 13 Fungsi Postnotification Pada Notificationservice .....	49
Gambar 4. 17 Kode Script Pengujian Integrasi Aplikasi Dosa Dan Model.....	53
Gambar 4. 18 Confusion Matrix Hasil Pengujian Aplikasi Terhadap 100 Data Dalam Dataset.....	54
Gambar 4. 19 Confusion Matrix Hasil Pengujian Aplikasi Terhadap 40 Data Di Luar Dataset .....	55

## DAFTAR PERSAMAAN

Persamaan 2. 1 Persamaan Matematika Term Frequency Inverse Document .....	13
Persamaan 2. 2 Persamaan Matematika Term Frequency .....	13
Persamaan 2. 3 Persamaan Matematika Inverse Document Frequency.....	13
Persamaan 3. 1 Persamaan Untuk Menghitung Nilai Presisi.....	34
Persamaan 3. 2 Persamaan Untuk Menghitung Nilai Recall .....	34
Persamaan 3. 3 Persamaan Untuk Menghitung Nilai Akurasi.....	35
Persamaan 3. 4 Persamaan Untuk Menghitung F1-Score.....	35

## DAFTAR LAMPIRAN

Lampiran 1 100 Data Pesan Dari Dataset Untuk Pengujian Integrasi Model Dan Aplikasi .....	62
Lampiran 2 50 Data Pesan Dari Dataset Untuk Pengujian Integrasi Model Dan Aplikasi .....	70
Lampiran 3 Dokumentasi Hasil Pengujian Aplikasi DOSA .....	81
Lampiran 4 Kode Training Machine Learning Model Filtrasi Spam Dan Phising	82
Lampiran 5 Source Kode Aplikasi DOSA .....	86
Lampiran 6 Dataset Model Machine Learning Filtrasi Spam Dan Phising .....	86

## DAFTAR PUSTAKA

- Alazab, M., & Broadhurst, R. (2014). SPAM and criminal activity. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2467423>
- Amir Sjarif, N. N., Mohd Azmi, N. F., Chuprat, S., Sarkan, H. M., Yahya, Y., & Sam, S. M. (2019). SMS SPAM message detection using term frequency-inverse document frequency and random forest algorithm. *Procedia Computer Science*, *161*, 509–515. <https://doi.org/10.1016/j.procs.2019.11.150>
- Azimah, F., & Rizky Nova Wardani, K. (2022). Klasifikasi Deteksi Gejala Awal Covid-19 Dengan metode logistic regression, random forest classifier Dan Support Vector Machine. *Jurnal Locus Penelitian Dan Pengabdian*, *1(6)*, 405–418. <https://doi.org/10.58344/locus.v1i6.135>
- Aziziyah, T., Purwoleksono, D. E., & Rachman, T. (2023). Sniffing cybercrimes in M-banking via WhatsApp: Comparative Legal Framework and implications. *Rechtsidee*, *11(2)*. <https://doi.org/10.21070/jihr.v12i2.985>
- Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. *International Journal of Computer Applications*, *182(33)*, 27–29. <https://doi.org/10.5120/ijca2018918286>
- Breiman, L. (2001). *Machine Learning*, *45(1)*, 5–32. <https://doi.org/10.1023/a:1010933404324>
- Catal, C., Giray, G., Tekinerdogan, B., Kumar, S., & Shukla, S. (2022). Applications of deep learning for phishing detection: A systematic literature review. *Knowledge and Information Systems*, *64(6)*, 1457–1500. <https://doi.org/10.1007/s10115-022-01672-x>
- Chirzah, D., & Wardhana, Y. A. (2023). Analisis Dampak Pandemi Covid-19 Ditinjau Dari Sudut Pandang Keamanan Siber, *01(01)*.

Danilo Dessí, Rim Helaoui, Vivek Kumar, Diego Reforgiato Recupero, & Daniele Riboni. (2020). TF-IDF vs Word Embeddings for Morbidity Identification in Clinical Notes: An Initial Study. CEUR Proceedings of the First Workshop on Smart Personal Health Interfaces Co-located with 25th International Conference on Intelligent User Interfaces (IUI 2020), 1–12. <https://doi.org/10.5281/zenodo.4777594>

Dave, B., Bhat, S., & Majumder, P. (2021, April). IRNLP\_DAIICT@DravidianLangTech-EACL2021:Offensive Language identification in Dravidian Languages using TF-IDF Char N-grams and MuRIL. In B. R. Chakravarthi, R. Priyadharshini, A. Kumar M, P. Krishnamurthy, & E. Sherly (Eds.), *Proceedings of the First Workshop on Speech and Language Technologies for Dravidian Languages* (pp. 266–269). Retrieved from <https://aclanthology.org/2021.dravidianlangtech-1.37>

De Silva, D., & Alahakoon, D. (2022). An artificial intelligence life cycle: From conception to production. *Patterns*, 3(6), 100489. <https://doi.org/10.1016/j.patter.2022.100489>

EKİCİ, B., & TAKCI, H. (2021). Spam tespitinde word2vec ve tf-IDF Yöntemlerinin Karşılaştırılması ve Başarı Oranının Artırılması üzerine Bir çalışma. *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi*, 8(2), 646–655. <https://doi.org/10.35193/bseufbd.935247>

Hayati, P., Potdar, V., Talevski, A., Firoozeh, N., Sarenche, S., & Yeganeh, E. A. (2010a). Definition of spam 2.0: New spamming boom. 4th IEEE International Conference on Digital Ecosystems and Technologies. <https://doi.org/10.1109/dest.2010.5610590>

Iswanto, H., Seniwati, E., Astuti, Y., & Maulina, D. (2021). Comparison of algorithms on machine learning for Spam Email Classification. *IJISTECH (International Journal of Information System and Technology)*, 5(4), 446. <https://doi.org/10.30645/ijistech.v5i4.164>

Kouraklis, J. (2016a). *MVVM in Delphi: Architecting and building model view viewmodel applications* (1st ed.). Apress.



Liu, X., Lu, H., & Nayak, A. (2021). A spam transformer model for SMS spam detection. *IEEE Access*, 9, 80253–80263. <https://doi.org/10.1109/access.2021.3081479>

Lumba, E., & Waworuntu, A. (2022). Implementation of Model View Controller Architecture in Object Oriented Programming Learning. *IJNMT (International Journal of New Media Technology)*, 8(2), 102-108. <https://doi.org/https://doi.org/10.31937/ijnmt.v8i2.2429>

Nugraha, R. (2021). Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber di Indonesia. *Jurnal Ilmiah Hukum Dirgantara*, 11, 44–56.

Palefi Ma'ady, M. N., Zahra, A. N., Darmawan, M. Z., Abdillah, R., & Anaking, P. (n.d.-b). Analisis Modus Penipuan Digital Teknik Phising Melalui Aplikasi WhatsApp Menggunakan Metode BPMN (Studi Kasus Pada Peretasan E-Wallet). ISSN: 2598-0076

Rao, S., Verma, A. K., & Bhatia, T. (2021). A review on Social Spam Detection: Challenges, open issues, and Future Directions. *Expert Systems with Applications*, 186, 115742. <https://doi.org/10.1016/j.eswa.2021.115742>

Roihan, A., Sunarya, P. A., & Rafika, A. S. (2020). Pemanfaatan machine learning Dalam Berbagai Bidang: Review paper. *IJCIT (Indonesian Journal on Computer and Information Technology)*, 5(1). <https://doi.org/10.31294/ijcit.v5i1.7951>

Sukarsa, I. M. (2020). Penerapan Arsitektur MVP Dalam Pengembangan Aplikasi Pemesanan Tiket Seminar Berbasis Android, 4(03), 513–520.

Vijaywargi, A., & Boddapati, U. K. (2024). Architectural Patterns in android development: Comparing MVP, MVVM, and MVI. *International Journal for Research in Applied Science and Engineering Technology*, 12(4), 4611–4616. <https://doi.org/10.22214/ijraset.2024.60762>

Widhiyanti, K., & Atmani, A. K. (2021). Penerapan metode prototyping Dalam Perancangan interface Sistem Unggah portofolio Penerimaan mahasiswa Baru Diploma Isi Yogyakarta. *Teknika*, *10*(2), 88–95. <https://doi.org/10.34148/teknika.v10i2.308>

Yuan, H., Tang, Y., Sun, W., & Liu, L. (2020). A detection method for Android application security based on TF-IDF and Machine Learning. *PLOS ONE*, *15*(9). <https://doi.org/10.1371/journal.pone.0238694>

Zidan, M., Nur'aini, S., Wibowo, N. C., & Ulinuha, M. A. (2022). Black box testing pada aplikasi single sign on (SSO) Di Diskominfostandi Menggunakan Teknik equivalence partitions. *Walisongo Journal of Information Technology*, *4*(2), 127–137. <https://doi.org/10.21580/wjit.2022.4.2.12135>