Jurnal Riset Multidisiplin Edukasi
https://journal.hasbaedukasi.co.id/index.php/jurmie
Halaman : 411 - 430

IMPLEMENTASI ALGORITMA LEVENSHTEIN DISTANCE PADA APLIKASI EDUKASI KEAMANAN DIGITAL DAN SIMULASI DETEKSI PENIPUAN ONLINE BERBASIS MOBILE: STUDI KASUS PADA IDOLA CAFE

Muhammad Rayhan Fadillah[1], Khairuddin Nasution[2], Tasliyah Haramaini[3]
Universitas Islam Sumatera Utara, Medan, Indonesia [1,2,3]
Email: muhammadrayhanfadillah9@gmail.com[1], khairuddin_nst@uisu.ac.id[2], tasliyah@ft.uisu.ac.id[3]

Informasi

Volume : 3
Nomor : 11
Bulan : November
Tahun : 2026
E-ISSN : 3062-9624

Abstract

Micro, small, and medium enterprises (MSMEs), including culinary businesses, increasingly rely on social media, instant messaging, and digital payments, which makes them vulnerable to online fraud such as fictitious orders, fake links or QRIS codes (phishing), and fake promotions. Available educational resources are generally passive and are not accompanied by simulations whose effectiveness can be measured. This study aims to design and build a mobile application for digital security education and online fraud detection simulation, named Scam Guard, for the owner and employees of Idola Cafe, and to apply the Levenshtein Distance algorithm in a link-checking feature to detect typosquatting. The application was developed using the Waterfall method with the Flutter framework, the Dart programming language, and Firebase Authentication and Cloud Firestore as backend services. Its main features include educational materials, case simulations, pre-test and post-test, score history, case studies, and link checking. The link checker compares a URL entered by the user against official domains using an edit distance threshold of 3, supported by risk indicators such as the use of the HTTP protocol, phishing keywords, and login requests. Black box testing of 16 scenarios showed that all of them passed (100%). The link-checking feature identified whatsappqr.com as similar to whatsapp.com with an edit distance of 2. User Acceptance Testing with four respondents produced an overall average score of 4.47 out of 5 (Very Good), while the average score increased from 57.5 on the pre-test to 97.5 on the post-test. These results indicate that the application is well accepted and helps improve users' understanding of online fraud, with limitations in the number of respondents and the sample URLs tested.

Keyword: *Levenshtein Distance, Digital Security, Online Fraud, Phishing, Typosquatting, Flutter, MSMEs*

Abstrak

Pelaku usaha mikro, kecil, dan menengah (UMKM), termasuk usaha kuliner, semakin bergantung pada media sosial, aplikasi pesan instan, dan pembayaran digital sehingga rentan terhadap penipuan online seperti pesanan fiktif, tautan atau QRIS palsu (phishing), dan promosi palsu. Sumber edukasi yang tersedia umumnya masih bersifat pasif dan belum dilengkapi simulasi yang efektivitasnya dapat diukur. Penelitian ini bertujuan merancang dan membangun aplikasi mobile edukasi keamanan digital dan simulasi deteksi penipuan online bernama Scam Guard bagi pemilik dan karyawan Idola Cafe, serta menerapkan algoritma Levenshtein Distance pada fitur pemeriksaan tautan untuk mendeteksi typosquatting. Aplikasi dikembangkan dengan metode Waterfall menggunakan framework Flutter, bahasa pemrograman Dart, serta Firebase Authentication dan Cloud Firestore sebagai layanan backend. Fitur utama aplikasi meliputi materi edukasi, simulasi kasus, pre-test dan post-test, riwayat skor, studi kasus, dan pemeriksaan tautan. Pemeriksaan tautan membandingkan URL yang dimasukkan

pengguna dengan domain resmi menggunakan ambang batas jarak edit 3, dilengkapi indikator risiko berupa penggunaan protokol HTTP, kata kunci phishing, dan permintaan login. Hasil pengujian black box terhadap 16 skenario menunjukkan seluruhnya berstatus Sesuai (100%). Fitur pemeriksaan tautan berhasil mengenali whatsappqr.com sebagai domain yang mirip dengan whatsapp.com dengan jarak edit 2. User Acceptance Test terhadap empat responden menghasilkan rata-rata skor 4,47 dari 5 dengan kategori Sangat Baik, sedangkan rata-rata skor pre-test meningkat dari 57,5 menjadi 97,5 pada post-test. Hasil tersebut menunjukkan bahwa aplikasi dapat diterima dengan baik dan membantu meningkatkan pemahaman pengguna dalam mengenali penipuan online, dengan keterbatasan pada jumlah responden dan contoh URL yang diuji.

Kata Kunci : *Levenshtein Distance, Keamanan Digital, Penipuan Online, Phishing, Typosquatting, Flutter, UMKM*

A. PENDAHULUAN

Perkembangan teknologi digital mendorong pelaku usaha mikro, kecil, dan menengah (UMKM), termasuk usaha kuliner seperti Idola Cafe, memanfaatkan media sosial, aplikasi pesan instan WhatsApp, dan pembayaran digital QRIS untuk promosi, penerimaan pesanan, serta transaksi. (Riandi dkk., 2023) Di sisi lain, meningkatnya aktivitas digital ini membuka celah bagi berbagai modus penipuan online, seperti pesanan fiktif yang disertai permintaan transfer dana atas nama kurir, tautan atau QRIS palsu (phishing), giveaway palsu yang mengatasnamakan usaha, serta klaim refund palsu yang mengarahkan korban ke tautan berbahaya. (Nugroho dkk., 2023)

Insiden keamanan siber pada dasarnya tidak semata-mata disebabkan oleh kelemahan teknologi, melainkan lebih sering dipicu oleh perilaku pengguna, dan penipuan online menjadi ancaman dominan karena memanfaatkan rendahnya literasi serta kewaspadaan pengguna (Pasaribu dkk., 2026). Keterbatasan anggaran dan rendahnya literasi keamanan menyebabkan UMKM rentan, sehingga edukasi dan pelatihan pengguna menjadi strategi pertahanan yang paling realistis dan terjangkau (Pasaribu dkk., 2026). Sebagian besar pelaku UMKM belum menerapkan praktik keamanan dasar seperti kata sandi yang kuat dan autentikasi dua faktor (Atika dkk., 2026). Pemahaman perilaku aman dalam beraktivitas dan bertransaksi online juga sangat penting bagi pelaku usaha kecil dan menengah (Riandi dkk., 2023). Pemilik dan karyawan Idola Cafe berpotensi menghadapi risiko serupa, sementara sumber edukasi yang tersedia umumnya masih pasif berupa artikel atau imbauan tanpa simulasi kasus yang dapat diukur efektivitasnya.

Pendekatan edukasi interaktif terbukti meningkatkan pemahaman. Penyuluhan interaktif kepada pelaku UMKM meningkatkan pemahaman dasar tentang modus penipuan online dari sekitar 20% menjadi 85% (Anan dkk., 2024). Edukasi keamanan digital juga efektif

menumbuhkan kewaspadaan terhadap tautan phishing (Nugroho dkk., 2023). Simulasi serangan phishing yang diukur melalui pre-test dan post-test juga meningkatkan pemahaman peserta dalam mengenali penipuan online (Holilah dkk., 2026). Temuan ini menunjukkan bahwa evaluasi berbasis pre-test dan post-test relevan untuk mengukur efektivitas edukasi. Selain itu, aplikasi mobile lebih sesuai dengan kebiasaan pelaku UMKM karena pesanan dan pembayaran digital umumnya dilakukan melalui perangkat mobile.

Salah satu modus yang sering ditemui adalah typosquatting, yaitu pembuatan domain palsu yang menyerupai tautan resmi dengan menambah, menghilangkan, atau mengganti satu-dua karakter. Salah eja domain semacam ini dapat dideteksi dengan mengukur jarak edit terhadap daftar domain tepercaya secara ringan di sisi pengguna (Tupsamudre dkk., 2021). Algoritma Levenshtein Distance sesuai untuk pendekatan tersebut karena menghitung jumlah minimum operasi penyisipan, penghapusan, atau penggantian karakter yang diperlukan untuk mengubah satu string menjadi string lainnya.

Berdasarkan uraian tersebut, dibutuhkan aplikasi mobile yang menyediakan materi edukasi keamanan digital, simulasi kasus penipuan online, dan pemeriksaan tautan berbasis algoritma Levenshtein Distance, disertai evaluasi pre-test dan post-test untuk mengukur peningkatan pemahaman pengguna.

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah bagaimana merancang dan membangun aplikasi edukasi keamanan digital dan simulasi deteksi penipuan online berbasis mobile yang menyajikan materi edukasi, simulasi kasus, serta kuis evaluasi sesuai dengan kebutuhan pemilik dan karyawan Idola Cafe. Selain itu, penelitian ini membahas bagaimana penerapan algoritma Levenshtein Distance pada fitur pemeriksaan tautan untuk mendeteksi kemiripan URL yang berpotensi menjadi tautan phishing terhadap domain resmi atau tepercaya. Selanjutnya, penelitian ini juga mengkaji bagaimana hasil pengujian aplikasi dari aspek fungsionalitas menggunakan metode Black-Box Testing, penerimaan pengguna melalui User Acceptance Test (UAT), serta peningkatan pemahaman pengguna Idola Cafe berdasarkan perbandingan hasil pre-test dan post-test.

Berdasarkan rumusan masalah yang telah diuraikan, penelitian ini bertujuan untuk merancang dan membangun aplikasi edukasi keamanan digital dan simulasi deteksi penipuan online berbasis mobile yang menyediakan materi edukasi, simulasi kasus, dan kuis evaluasi sesuai dengan kebutuhan pemilik dan karyawan Idola Cafe. Penelitian ini juga bertujuan untuk menerapkan algoritma Levenshtein Distance pada fitur pemeriksaan tautan guna mendeteksi kemiripan URL yang berpotensi merupakan tautan phishing terhadap domain resmi atau

tepercaya. Selain itu, penelitian ini bertujuan untuk mengetahui hasil pengujian fungsionalitas aplikasi menggunakan metode Black-Box Testing, mengukur penerimaan pengguna melalui User Acceptance Test (UAT), serta mengevaluasi efektivitas aplikasi dalam meningkatkan pemahaman pengguna Idola Cafe melalui perbandingan hasil pre-test dan post-test.

B. METODE PENELITIAN

Penelitian ini dilaksanakan di Idola Cafe, Desa Sidorejo, Kecamatan Medan Tembung, Kota Medan, pada Oktober hingga November 2026. Penelitian bertujuan mengembangkan aplikasi edukasi keamanan digital dan simulasi deteksi penipuan online berbasis mobile dengan menggunakan Flutter dan bahasa pemrograman Dart. Perancangan dan pengembangan aplikasi didukung oleh Visual Studio Code sebagai lingkungan pengembangan serta Firebase Authentication dan Cloud Firestore sebagai layanan autentikasi dan penyimpanan data. Metode pengembangan sistem yang digunakan adalah Waterfall, yang terdiri atas tahapan analisis kebutuhan, perancangan sistem, implementasi, integrasi, dan pengujian. Pengumpulan data dilakukan melalui studi literatur, observasi aktivitas digital Idola Cafe, serta wawancara dengan pemilik dan karyawan untuk mengetahui kebutuhan pengguna dan potensi ancaman penipuan online. Sistem dirancang menggunakan UML yang meliputi Use Case Diagram, Activity Diagram, Sequence Diagram, dan Class Diagram, serta dilengkapi dengan perancangan basis data dan antarmuka aplikasi.

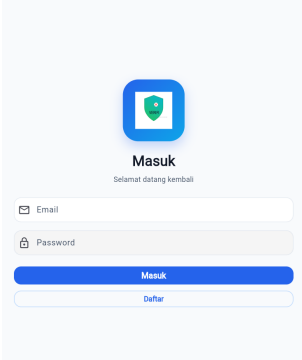
Aplikasi yang dikembangkan memiliki beberapa fitur utama, yaitu materi edukasi keamanan digital, simulasi kasus penipuan online, pre-test dan post-test, riwayat skor, serta pemeriksaan tautan (link checker). Fitur pemeriksaan tautan menerapkan algoritma Levenshtein Distance untuk membandingkan URL masukan pengguna dengan domain resmi atau tepercaya yang tersimpan dalam Cloud Firestore. Ambang batas jarak ditetapkan sebesar 3, yaitu jarak 0 menunjukkan kesamaan domain, jarak 1–3 menunjukkan potensi typosquatting, sedangkan jarak lebih dari 3 menunjukkan tidak ditemukan kemiripan. Pengujian dilakukan menggunakan Black-Box Testing untuk mengukur kesesuaian fungsi, User Acceptance Test (UAT) dengan skala Likert 1–5 untuk mengetahui penerimaan pengguna, serta perbandingan hasil pre-test dan post-test yang masing-masing terdiri atas 10 soal untuk mengukur perubahan pemahaman. Data hasil pengujian dianalisis secara deskriptif berdasarkan kesesuaian fungsi, kemampuan pemeriksaan tautan, tingkat penerimaan pengguna, dan peningkatan pemahaman terhadap ciri-ciri penipuan online.

C. HASIL DAN PEMBAHASAN

Implementasi Aplikasi

Implementasi Antarmuka dan Fitur

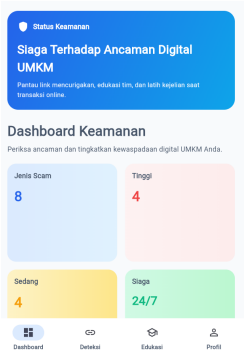
Halaman *Login*



Gambar 1 Halaman *Login*

Gambar 1 menunjukkan halaman *login* yang pertama kali tampil ketika aplikasi dibuka. Bagian atas halaman memuat logo aplikasi berupa perisai, judul Masuk, dan sapaan Selamat datang kembali. Di bawahnya terdapat kolom *Email* dan *Password* yang masing-masing dilengkapi ikon, tombol Masuk berwarna biru, dan tombol Daftar bagi pengguna yang belum memiliki akun. Proses autentikasi dilakukan melalui Firebase Authentication.

Halaman *Dashboard*



Gambar 2 a *Dashboard* (Bagian Atas)

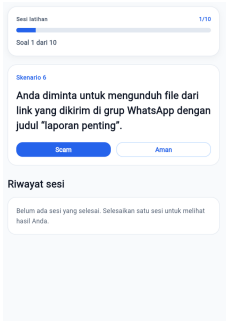


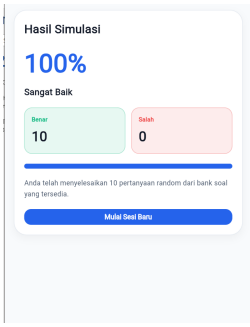
Gambar 2 b *Dashboard* (Bagian Bawah)

Gambar 2 a menunjukkan bagian atas *dashboard* pengguna yang tampil setelah *login* berhasil. Kartu biru Status Keamanan memuat pesan Siaga Terhadap Ancaman Digital UMKM sebagai pengingat untuk memantau tautan mencurigakan, mengedukasi tim, dan melatih kejelian saat transaksi *online*. Di bawahnya terdapat bagian *Dashboard* Keamanan yang menyajikan empat kartu ringkasan, yaitu jumlah Jenis *Scam* sebanyak 8, kategori risiko Tinggi sebanyak 4, kategori risiko Sedang sebanyak 4, dan keterangan Siaga 24/7. Jumlah jenis *scam* tersebut sesuai dengan jumlah materi pada panel admin

Gambar 2 b menunjukkan bagian bawah *dashboard*. Bagian Akses Cepat menyediakan pintasan ke Simulasi (latihan anti *scam*) dan Studi Kasus (contoh nyata). Bagian Peringatan Penting berwarna merah mengingatkan pengguna agar waspada terhadap tautan yang meminta *login*, OTP, atau pembayaran segera, karena penipu sering memakai kata-kata panik seperti akun diblokir, bonus akhir bulan, atau verifikasi mendadak. Bagian *Top Scam* yang Sering Ditemui menampilkan modus penipuan yang umum, misalnya *deepfake* dan *social engineering*. Perpindahan antarhalaman dilakukan melalui menu navigasi bawah yang terdiri dari *Dashboard*, Deteksi, Edukasi, dan Profil.

Halaman Simulasi, *Pre-test*, dan *Post-test*

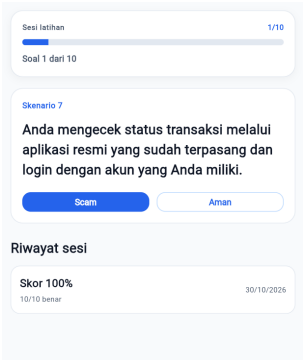




Gambar 3 a Halaman Simulasi Gambar 3 b Halaman Hasil Simulasi

Gambar 3 a menunjukkan halaman simulasi yang juga digunakan sebagai *pre-test* dan *post-test*. Bagian atas memuat kartu Sesi latihan dengan indikator 1/10 dan bilah progres yang menandakan setiap sesi terdiri dari 10 soal. Kartu skenario menampilkan cerita kasus penipuan, pada contoh ini Skenario 6 yang meminta pengguna mengunduh *file* dari tautan yang dikirim di grup WhatsApp dengan judul "laporan penting". Pengguna menentukan jawaban melalui dua tombol, yaitu *Scam* atau Aman. Nomor skenario dapat berbeda dengan urutan soal karena soal diambil secara acak dari bank soal. Bagian Riwayat sesi menampilkan keterangan bahwa belum ada sesi yang selesai apabila pengguna belum pernah menyelesaikan satu sesi.

Gambar 3 b menunjukkan halaman Hasil Simulasi yang tampil setelah seluruh soal dijawab. Halaman ini memuat persentase skor (100%), keterangan tingkat pemahaman (Sangat Baik), kartu jumlah jawaban Benar (10) dan Salah (0), bilah progres, serta keterangan bahwa pengguna telah menyelesaikan 10 pertanyaan acak dari bank soal. Tombol Mulai Sesi Baru digunakan untuk mengulang sesi. Skor inilah yang dibandingkan antara *pre-test* dan *post-test* untuk melihat perubahan pemahaman pengguna.



Gambar 3 c Halaman Simulasi dengan Riwayat Sesi

Gambar 3 c menunjukkan halaman simulasi setelah satu sesi diselesaikan. Sesi baru dimulai kembali dari soal 1/10 dengan skenario yang berbeda, yaitu Skenario 7 tentang pengecekan status transaksi melalui aplikasi resmi. Pada bagian Riwayat sesi, tampil kartu yang memuat Skor 100%, jumlah jawaban 10/10 benar, dan tanggal pengerjaan 30/10/2026. Data ini diambil dari koleksi riwayat_skor sehingga pengguna dapat memantau perkembangan hasil latihannya.

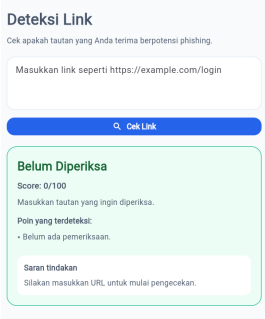
Halaman Studi Kasus



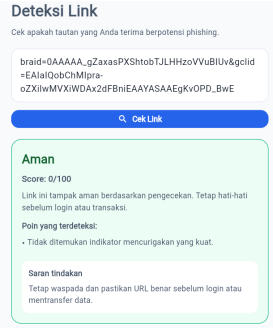
Gambar 4 Halaman Studi Kasus

Gambar 4 menunjukkan halaman Studi Kasus dengan judul Kejadian Nyata dan deskripsi bahwa halaman ini membantu pengguna mempelajari pola penipuan yang sering terjadi beserta cara mencegahnya. Setiap kasus disajikan dalam bentuk kartu yang memuat gambar ilustrasi, label kategori (pada contoh ini *Malware*), judul kasus Aplikasi Palsu untuk Pembukuan, dan ringkasan kejadian. Bagian Dampak menjelaskan akibat yang dialami korban, bagian Pembelajaran memuat langkah pencegahan, dan bagian Sumber mencantumkan rujukan kasus. Halaman ini melengkapi simulasi dengan contoh peristiwa nyata yang relevan dengan pelaku usaha.

Halaman Deteksi *Link Phishing*



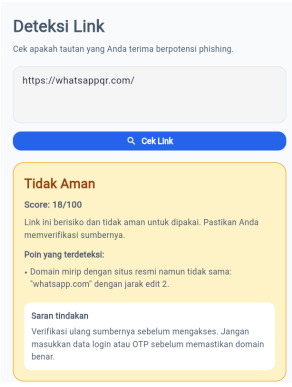
Gambar 5 a Deteksi *Link* (Kondisi Awal)



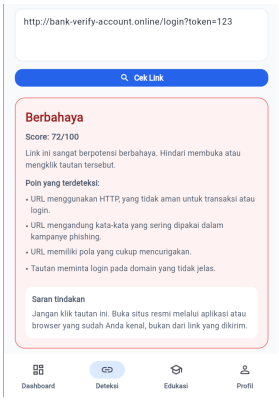
Gambar 5 b Hasil Pemeriksaan Status Aman

Gambar 5 a menunjukkan kondisi awal halaman Deteksi *Link*. Halaman memuat judul, deskripsi bahwa fitur ini digunakan untuk memeriksa apakah tautan yang diterima berpotensi *phishing*, kolom *input* URL dengan petunjuk Masukkan *link* seperti https://example.com/login, dan tombol Cek *Link*. Sebelum ada pemeriksaan, kartu hasil menampilkan status Belum Diperiksa dengan skor 0/100 serta saran tindakan untuk memasukkan URL terlebih dahulu.

Gambar 5 b menunjukkan hasil pemeriksaan terhadap URL berparameter yang berasal dari tautan iklan. Sistem menampilkan status Aman dengan skor 0/100 dan poin bahwa tidak ditemukan indikator mencurigakan yang kuat. Meskipun demikian, saran tindakan tetap mengingatkan pengguna untuk waspada dan memastikan URL benar sebelum *login* atau mentransfer data.



Gambar 5 c Hasil Pemeriksaan Status Tidak Aman



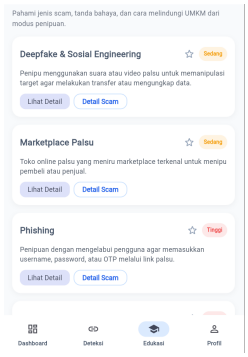
Gambar 5 d Hasil Pemeriksaan Status Berbahaya

Gambar 5 c menunjukkan hasil pemeriksaan terhadap URL https://whatsappqr.com/ yang dibuat menyerupai domain resmi. Sistem menampilkan status Tidak Aman dengan skor 18/100 pada kartu berwarna kuning. Poin yang terdeteksi menyebutkan bahwa domain mirip dengan situs resmi namun tidak sama, yaitu whatsapp.com dengan jarak edit 2. Saran tindakan meminta pengguna memverifikasi ulang sumber tautan dan tidak memasukkan data *login* atau

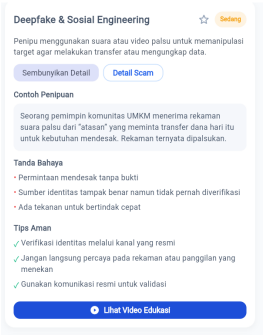
OTP.

Gambar 5 d menunjukkan hasil pemeriksaan terhadap URL http://bank-verify-account.online/login?token=123. Sistem menampilkan status Berbahaya dengan skor 72/100 pada kartu berwarna merah. Terdapat empat poin yang terdeteksi, yaitu URL menggunakan HTTP yang tidak aman untuk transaksi atau *login*, URL mengandung kata-kata yang sering dipakai dalam kampanye *phishing*, URL memiliki pola yang cukup mencurigakan, serta tautan meminta *login* pada domain yang tidak jelas. Saran tindakan meminta pengguna untuk tidak mengklik tautan tersebut dan membuka situs resmi melalui aplikasi atau *browser* yang sudah dikenal. Perbedaan warna kartu (hijau, kuning, merah) membantu pengguna memahami tingkat risiko dengan cepat.

Halaman Edukasi



Gambar 6 a Daftar Materi Edukasi



Gambar 6 b Detail Materi pada Kartu

Gambar 6 a menunjukkan halaman Edukasi yang berisi deskripsi untuk memahami jenis *scam*, tanda bahaya, dan cara melindungi UMKM dari modus penipuan. Materi ditampilkan dalam bentuk kartu, misalnya *Deepfake* & Sosial Engineering, *Marketplace* Palsu, dan *Phishing*. Setiap kartu memuat nama modus, ikon bintang, label tingkat risiko (Sedang atau Tinggi), ringkasan singkat, serta tombol Lihat Detail dan Detail *Scam*. Menu Edukasi pada navigasi bawah ditandai sebagai halaman yang sedang aktif.

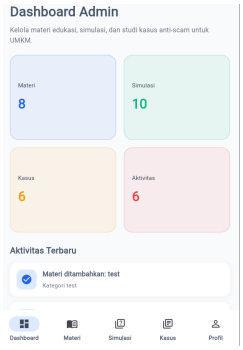
Gambar 6 b menunjukkan tampilan kartu setelah tombol Lihat Detail ditekan, ditandai dengan berubahnya tombol menjadi Sembunyikan Detail. Kartu memperlihatkan bagian Contoh Penipuan berupa ilustrasi kasus, Tanda Bahaya seperti permintaan mendesak tanpa bukti, serta Tips Aman seperti memverifikasi identitas melalui kanal resmi. Di bagian bawah tersedia tombol Lihat Video Edukasi.



Gambar 6 c Halaman Detail *Scam*

Gambar 6 c menunjukkan halaman Detail *Scam* yang tampil setelah tombol Detail *Scam* ditekan. Halaman ini memuat label kategori (Manipulasi Sosial), judul dan deskripsi modus, daftar Tanda Bahaya, Tips Aman, serta Contoh Penipuan. Pengguna juga dapat membuka video referensi melalui tombol Lihat Video Referensi dan membagikan materi kepada orang lain melalui tombol Share Edukasi.

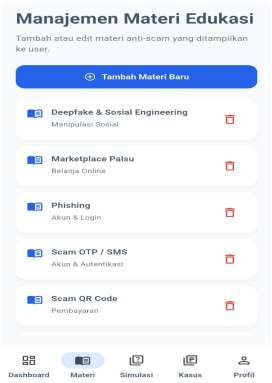
Halaman *Dashboard* Admin



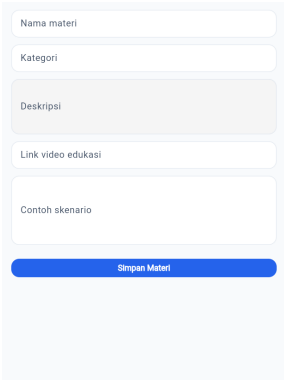
Gambar 7 Halaman *Dashboard* Admin

Gambar 7 menunjukkan *Dashboard* Admin yang tampil ketika akun dengan peran admin berhasil *login*. Halaman ini menyajikan ringkasan jumlah konten dalam empat kartu, yaitu Materi (8), Simulasi (10), Kasus (6), dan Aktivitas (6). Di bawahnya terdapat daftar Aktivitas Terbaru yang mencatat perubahan konten, misalnya Materi ditambahkan beserta kategorinya. Admin berpindah antarhalaman melalui menu navigasi bawah yang terdiri dari *Dashboard*, Materi, Simulasi, Kasus, dan Profil.

Halaman Manajemen Materi



Gambar 8 a Daftar Manajemen Materi

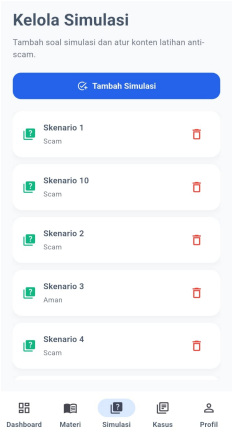


Gambar 8 b Formulir Tambah Materi

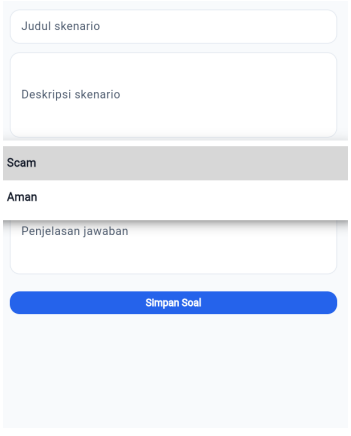
Gambar 8 a menunjukkan halaman Manajemen Materi Edukasi yang digunakan admin untuk menambah atau menghapus materi anti-scam yang ditampilkan kepada pengguna. Tombol Tambah Materi Baru berada di bagian atas, diikuti daftar materi beserta kategorinya, seperti *Deepfake* & Sosial Engineering (Manipulasi Sosial), *Phishing* (Akun & *Login*), dan *Scam* QR Code (Pembayaran). Ikon tong sampah pada setiap materi digunakan untuk menghapus materi tersebut.

Gambar 8 b menunjukkan formulir penambahan materi yang memuat kolom Nama materi, Kategori, Deskripsi, *Link* video edukasi, dan Contoh skenario. Setelah tombol Simpan Materi ditekan, data disimpan ke Cloud Firestore dan langsung tampil pada halaman Edukasi pengguna.

Halaman Manajemen Simulasi



Gambar 9 a Daftar Manajemen Simulasi



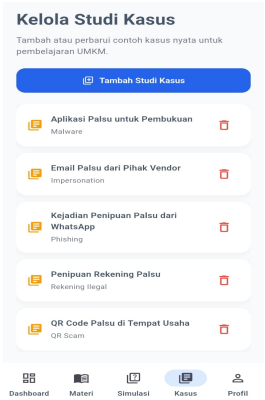
Gambar 9 b Formulir Tambah Simulasi

Gambar 9 a menunjukkan halaman Kelola Simulasi untuk menambah soal simulasi dan mengatur konten latihan anti-scam. Daftar skenario ditampilkan beserta kunci jawabannya, yaitu *Scam* atau Aman, dan setiap skenario dapat dihapus melalui ikon tong sampah. Tombol

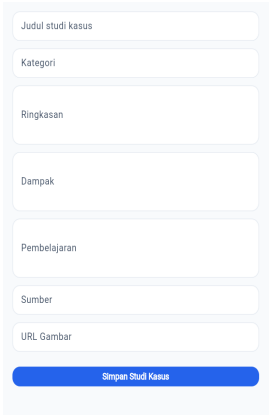
Tambah Simulasi digunakan untuk membuat skenario baru.

Gambar 9 b menunjukkan formulir penambahan soal simulasi yang memuat Judul skenario, Deskripsi skenario, pilihan kunci jawaban (*Scam* atau Aman), dan Penjelasan jawaban yang akan ditampilkan sebagai umpan balik kepada pengguna.

Halaman Manajemen Studi Kasus



Gambar 10 a Daftar Manajemen Studi Kasus



Gambar 10 b Formulir Tambah Studi Kasus

Gambar 10 a menunjukkan halaman Kelola Studi Kasus untuk menambah atau menghapus contoh kasus nyata bagi pembelajaran UMKM. Daftar kasus memuat judul dan kategorinya, seperti Aplikasi Palsu untuk Pembukuan (*Malware*), *Email* Palsu dari Pihak Vendor (*Impersonation*), dan QR Code Palsu di Tempat Usaha (QR *Scam*). Ikon tong sampah pada setiap kasus digunakan untuk menghapus studi kasus tersebut.

Hasil Penelitian

Hasil Pemenuhan Kebutuhan Sistem

Tabel 1 Pemenuhan Kebutuhan Fungsional Sistem

ID	Kebutuhan Fungsional	Realisasi pada Aplikasi	Gambar
F-01	Materi Edukasi	Menu Edukasi menampilkan daftar modus penipuan beserta tingkat risiko, tanda bahaya, tips aman, contoh penipuan, dan video edukasi.	6 A–6 C
F-02	Simulasi Kasus	Menu Simulasi menampilkan skenario kasus penipuan yang dijawab pengguna dengan pilihan *Scam* atau Aman, disertai Studi Kasus berupa kejadian nyata.	3 A, 4

ID	Kebutuhan Fungsional	Realisasi pada Aplikasi	Gambar
F-03	*Pre-test* dan *Post-test*	Sesi 10 soal acak dari bank soal digunakan sebagai *pre-test* dan *post-test*, dengan hasil berupa persentase skor serta jumlah jawaban benar dan salah.	3 A, 3 B
F-04	Riwayat Skor	Bagian Riwayat sesi menyimpan dan menampilkan skor, jumlah jawaban benar, dan tanggal pengerjaan setiap sesi.	3 C
F-05	*Input* URL	Menu Deteksi menyediakan kolom *input* URL dan tombol Cek *Link*.	5 A
F-06	Perbandingan URL	URL dibandingkan dengan domain resmi/tepercaya menggunakan algoritma *Levenshtein Distance*, dan hasilnya dinyatakan sebagai jarak edit.	5 C
F-07	Hasil dan Peringatan	Hasil ditampilkan dalam kartu berisi status, skor risiko, poin yang terdeteksi, dan saran tindakan.	5 B–5 D
F-08	Pengelolaan Konten oleh Admin	Admin dapat menambah dan mengubah materi edukasi, simulasi, dan studi kasus melalui panel admin.	7–10

Adapun kebutuhan non-fungsional terpenuhi melalui penggunaan aplikasi pada platform Android (NF-01), antarmuka dengan navigasi bawah yang sederhana serta pemakaian kartu dan warna status yang mudah dipahami (NF-02), serta konten yang dapat diperbarui admin tanpa mengubah kode program (NF-06).

Hasil Pengujian Black Box

Tabel 2 Hasil Pengujian *Black Box*

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Aktual	Status
1	Membuka aplikasi	Halaman *login* dengan kolom *email*, *password*, tombol Masuk dan Daftar tampil	Halaman *login* tampil (Gambar 1)	Sesuai
2	*Login* berhasil sebagai pengguna	*Dashboard* pengguna tampil beserta menu navigasi bawah	*Dashboard* tampil (Gambar 2 A dan 2 B)	Sesuai

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Aktual	Status
3	Membuka menu Edukasi	Daftar materi beserta tingkat risiko tampil	Daftar materi tampil (Gambar 6 A)	Sesuai
4	Menekan Lihat Detail / Detail *Scam*	Detail materi (tanda bahaya, tips aman, contoh) tampil	Detail materi tampil (Gambar 6 B dan 6 C)	Sesuai
5	Membuka menu Simulasi	Skenario dengan pilihan *Scam* dan Aman serta indikator soal 1 sampai 10 tampil	Skenario tampil (Gambar 3 A)	Sesuai
6	Menyelesaikan 10 soal	Hasil berupa persentase skor serta jumlah benar dan salah tampil	Hasil tampil (Gambar 3 B)	Sesuai
7	Melihat riwayat skor	Skor, jumlah benar, dan tanggal sesi tampil pada Riwayat sesi	Riwayat sesi tampil (Gambar 3 C)	Sesuai
8	Membuka Studi Kasus	Kasus nyata beserta dampak dan pembelajaran tampil	Studi kasus tampil (Gambar 4)	Sesuai
9	Membuka Deteksi *Link* tanpa *input*	Status Belum Diperiksa dengan skor 0/100 tampil	Status Belum Diperiksa tampil (Gambar 5 A)	Sesuai
10	Memeriksa URL yang aman	Status Aman tampil	Status Aman, skor 0/100 (Gambar 5 B)	Sesuai
11	Memeriksa URL yang menyerupai domain resmi	Peringatan domain mirip dan jarak edit tampil	Status Tidak Aman, skor 18/100, jarak edit 2 (Gambar 5 C)	Sesuai
12	Memeriksa URL yang mencurigakan	Status Berbahaya beserta poin terdeteksi dan saran tindakan tampil	Status Berbahaya, skor 72/100 (Gambar 5 D)	Sesuai
13	*Login* sebagai admin	*Dashboard* Admin berisi jumlah konten dan aktivitas terbaru tampil	*Dashboard* Admin tampil (Gambar 7)	Sesuai
14	Menambah/mengubah materi	Daftar materi dan formulir penyimpanan materi tampil	Daftar dan formulir tampil (Gambar 8 A dan 8 B)	Sesuai
15	Menambah/mengubah simulasi	Daftar skenario dan formulir penyimpanan soal tampil	Daftar dan formulir tampil (Gambar 9 A dan 9 B)	Sesuai

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Aktual	Status
16	Menambah/mengubah studi kasus	Daftar kasus dan formulir penyimpanan studi kasus tampil	Daftar dan formulir tampil (Gambar 10 A dan 10 B)	Sesuai

Hasil Pengujian Pemeriksaan Tautan

Tabel 3 Hasil Pengujian Pemeriksaan Tautan

No	URL Uji	Hasil yang Diharapkan	Hasil Sistem	Status
1	(kosong)	Belum diperiksa	Belum Diperiksa, skor 0/100	Sesuai
2	URL berparameter (braid=…&gclid=…)	Tidak ditemukan kemiripan maupun indikator mencurigakan	Aman, skor 0/100	Sesuai
3	https://whatsappqr.com/	Mirip domain resmi whatsapp.com (jarak 2, berpotensi *typosquatting*)	Tidak Aman, skor 18/100, jarak edit 2 dari whatsapp.com	Sesuai
4	http://bank-verify-account.online/login?token=123	Terdeteksi mencurigakan (HTTP, kata kunci *phishing*, permintaan *login*)	Berbahaya, skor 72/100, empat poin terdeteksi	Sesuai

Hasil User Acceptance Test (UAT)

Tabel 4 Rekapitulasi Hasil UAT

No	Indikator Penilaian	Rata-rata Skor	Kategori
1	Kemudahan penggunaan aplikasi	4,42	Sangat Baik
2	Kejelasan materi	4,55	Sangat Baik
3	Kemudahan mengikuti simulasi	4,25	Sangat Baik
4	Kemudahan menggunakan *link checker*	4,55	Sangat Baik
5	Kesesuaian aplikasi dengan kebutuhan pengguna	4,58	Sangat Baik
	Rata-rata keseluruhan	4,47	Sangat Baik

Hasil Pre-test dan Post-test

Tabel 5 Perbandingan Skor *Pre-test* dan *Post-test*

No	Responden	Skor *Pre-test*	Skor *Post-test*	Peningkatan
1	Responden 1	60	100	40
2	Responden 2	50	100	50
3	Responden 3	70	90	20
4	Responden 4	50	100	50
	Rata-rata	57,5	97,5	40,0

Pembahasan

Pengujian fungsional. Berdasarkan Tabel 2, seluruh 16 skenario *black box testing* menghasilkan keluaran aktual yang sama dengan keluaran yang diharapkan sehingga dinyatakan Sesuai. Hal ini menunjukkan bahwa fitur akses aplikasi, materi edukasi, simulasi, riwayat skor, studi kasus, pemeriksaan tautan, dan pengelolaan konten oleh admin telah berfungsi sesuai kebutuhan fungsional pada Tabel 3.1.

Pengujian pemeriksaan tautan. Berdasarkan Tabel 3, fitur pemeriksaan tautan mampu membedakan URL tanpa indikator mencurigakan, URL yang menyerupai domain resmi, dan URL yang mencurigakan. Pada URL whatsappqr.com, perhitungan *Levenshtein Distance* menurut Persamaan (2.3) pada Subbab 2.15 terhadap whatsapp.com menghasilkan jarak 2, yaitu dua operasi penyisipan karakter (q dan r). Karena jarak tersebut tidak melebihi ambang batas 3, sistem menandainya sebagai berpotensi *typosquatting*. Pada URL bank-verify-account.online, tautan tidak mirip dengan domain resmi tertentu, tetapi tetap ditandai Berbahaya karena sistem juga mengenali indikator lain, yaitu penggunaan HTTP, kata kunci *phishing*, dan permintaan *login*. Dengan demikian, hasil pemeriksaan tidak hanya bergantung pada jarak edit, tetapi juga dilengkapi skor risiko dan saran tindakan agar pengguna memperoleh informasi yang lebih lengkap. Namun, status Aman tidak menjamin tautan bebas dari risiko sehingga sistem tetap mengingatkan pengguna untuk berhati-hati.

Penerimaan pengguna. Berdasarkan Tabel 4, rata-rata skor UAT keseluruhan sebesar 4,47 dengan kategori Sangat Baik. Indikator dengan skor tertinggi adalah kesesuaian aplikasi dengan kebutuhan pengguna (4,58), sedangkan indikator dengan skor terendah adalah kemudahan mengikuti simulasi (4,25). Hasil ini menunjukkan bahwa aplikasi dapat diterima dengan sangat baik oleh pemilik dan karyawan Idola Cafe, mudah digunakan, serta sesuai dengan kebutuhan mereka dalam mengenali penipuan *online*.

Perubahan pemahaman pengguna. Berdasarkan Tabel 5, rata-rata skor *pre-test* sebesar 57,5 dan rata-rata skor *post-test* sebesar 97,5, sehingga terjadi peningkatan sebesar

40,0 poin. Peningkatan skor tersebut menunjukkan bahwa pemahaman pengguna dalam mengenali modus penipuan digital meningkat pada seluruh responden, dengan peningkatan skor antara 20 sampai 50 poin dan seluruh skor *post-test* berada pada rentang 90 sampai 100 setelah pengguna mempelajari materi dan mengikuti simulasi pada aplikasi.

D. KESIMPULAN

Berdasarkan hasil penelitian, implementasi aplikasi edukasi keamanan digital dan simulasi deteksi penipuan online berbasis mobile di Idola Cafe dapat disimpulkan bahwa aplikasi berhasil dirancang dan dibangun menggunakan framework Flutter dengan Firebase sebagai layanan backend, yang dilengkapi fitur login pengguna dan admin, dashboard, materi edukasi, simulasi kasus penipuan online, pre-test dan post-test, riwayat skor, studi kasus, serta pemeriksaan tautan (link checker) untuk membantu pemilik dan karyawan memahami berbagai modus penipuan, seperti pesanan fiktif, phishing, tautan atau QRIS palsu, dan promosi palsu, dengan hasil UAT pada indikator kesesuaian aplikasi terhadap kebutuhan pengguna sebesar 4,58 dalam kategori Sangat Baik. Penerapan algoritma Levenshtein Distance pada fitur pemeriksaan tautan juga berhasil mengukur kemiripan URL terhadap domain resmi atau tepercaya dengan ambang batas jarak 3, di mana URL whatsappqr.com memperoleh jarak edit sebesar 2 terhadap domain whatsapp.com sehingga dikategorikan Tidak Aman karena berpotensi merupakan typosquatting. Pemeriksaan tersebut turut didukung indikator risiko lain, seperti penggunaan protokol HTTP, kata kunci phishing, dan permintaan login. Selanjutnya, hasil pengujian menggunakan metode Black-Box Testing menunjukkan bahwa seluruh 16 skenario pengujian memperoleh status Sesuai dengan tingkat keberhasilan 100%, sedangkan hasil User Acceptance Test (UAT) memperoleh rata-rata 4,47 dari skala 5 dengan kategori Sangat Baik berdasarkan penilaian empat responden. Evaluasi pemahaman melalui pre-test dan post-test juga menunjukkan peningkatan nilai rata-rata dari 57,5 menjadi 97,5 atau sebesar 40 poin. Hasil tersebut menunjukkan bahwa aplikasi dapat diterima dengan baik dan berpotensi meningkatkan pemahaman pemilik serta karyawan Idola Cafe mengenai keamanan digital dan pencegahan penipuan online.

E. DAFTAR PUSTAKA

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060. https://doi.org/10.3389/fcomp.2021.563060

Anan, M., Rahmah, S. A., & Risuhendri, R. (2024). Meningkatkan kesadaran digital dalam pencegahan penipuan online untuk kelompok UMKM Desa Tanjung Haratan. Abdi Dalem: Jurnal Pengabdian Kepada Masyarakat, 1(2), 56–63.

Andrzejewska, M., & Stolińska, A. (2022). Do structured flowcharts outperform pseudocode? Evidence from eye movements. IEEE Access, 10, 132965–132975. https://doi.org/10.1109/ACCESS.2022.3230981

Arockiya Jerson, J., & Preethi, N. (2023). An analysis of Levenshtein distance using dynamic programming method. Lecture Notes in Networks and Systems, 540, 525–532. Springer.

Atika, P. D., Hafshah, A. A., Putri, F. A., Wijaya, R., Wijaya, R. P., Fauzan, Z. N., Nurfauzi, R., Darusman, R., Dzulfiqar, M. A., Ferdiansyah, M. D., Saputro, S., & Ramadhan, T. (2026). Pelatihan peningkatan kesadaran keamanan akun digital bagi pelaku UMKM Desa Sawarna Banten. Journal of Computer Science Contributions (JUCOSCO), 6(1), 11–20. https://doi.org/10.31599/xkyzys72

Aziz, M., Umar, R., & Ibdal. (2026). Literasi keamanan siber UMKM diaspora Indonesia–China melalui pelatihan anti-penipuan berbasis GIS. Jurnal Pengabdian UntukMu NegeRI, 10(2), 254–259. https://doi.org/10.37859/jpumri.v10i2.11560

Bailey, T., & Biessek, A. (2023). Flutter for beginners: Cross-platform mobile development from Hello, World! to app release with Flutter 3.10+ and Dart 3.x (3rd ed.). Packt Publishing.

Butnaru, A., Mylonas, A., & Pitropakis, N. (2021). Towards lightweight URL-based phishing detection. Future Internet, 13(6), 154. https://doi.org/10.3390/fi13060154

Haryanto, H. (2025). Cyber security paradox in MSMEs: Imbalance of awareness and implementation in the digital era. Electronic Journal of Education, Social Economics and Technology, 6(1), 143–149. https://doi.org/10.33122/ejeset.v6i1.470

Holilah, D., Ardi, B., Ar-Rahji, M. F., Anda, D., Gunawan, J. B., & Ayyasy, A. A. (2026). Peningkatan kesadaran keamanan siber mahasiswa melalui edukasi dan simulasi serangan phishing di Politeknik Piksi Input Serang. COMSERVA: Jurnal Penelitian dan Pengabdian Masyarakat, 6(2), 86–95. https://doi.org/10.59141/comserva.v6i2.3571

Kävrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., Roos, R., & Furnell, S. (2022). Evaluation of contextual and game-based training for phishing detection. Future Internet, 14(4), 104.

Lamusu, R., Lasaruddin, A., Ibrahim, I., & Lestari, G. (2023). Repository perpustakaan berbasis Android di Universitas Muhammadiyah Gorontalo. Jurnal Ilmu Komputer (JUIK), 3(1), 21–24. https://doi.org/10.31314/juik.v3i1.2000

Lee, J. S., & Yam, G. P. D. (2021). TypoSwype: An imaging approach to detect typo-squatting. In

Proceedings of the International Conference on New Technologies, Mobility and Security (NTMS). IEEE. https://doi.org/10.1109/NTMS49979.2021.9432673

Lovrić, L., Fischer, M., Röderer, N., & Wünsch, A. (2023). Evaluation of the cross-platform framework Flutter using the example of a cancer counselling app. In Proceedings of ICT4AWE 2023 (pp. 135–142). SciTePress. https://doi.org/10.5220/0011824500003476

Napitupulu, H. Y. P., & Nugraha, I. G. D. (2024). Fog computing-based system for decentralized smart parking system by using Firebase. Jurnal Nasional Teknik Elektro dan Teknologi Informasi, 13(1). https://doi.org/10.22146/jnteti.V13i1.10095

Noprianti, Aripin, D., & Heryanto, D. (2023). Aplikasi media belajar bahasa Ogan di OKU berbasis Android. Jurnal Sistem Informasi Mahakarya (JSIM), 6(2), 44–53.

Nugroho, H., Ihsan, M. N., Haryoko, A., Ma'arif, F., & Alifah, F. (2023). Edukasi keamanan digital untuk meningkatkan kewaspadaan masyarakat terhadap link phising. Alahyan: Jurnal Pengabdian Masyarakat Multidisiplin, 1(2), 104–111.

Panga, R. C. T., Marwa, J., & Ndibwile, J. D. (2022). A game or notes? The use of a customized mobile game to improve teenagers' phishing knowledge, case of Tanzania. Journal of Cybersecurity and Privacy, 2(3), 466–489.

Pasaribu, T. T., Wediawati, B., Ratnawati, R., Dewi, E., Adriani, Z., Darma, B., & Ramadhan, R. F. (2026). Pelatihan dan penerapan keamanan cyber pada pelaku usaha UMKM dalam mendukung transformasi digital. Jurnal Pengabdian Masyarakat dan Riset Pendidikan, 5(1), 4246–4251. https://doi.org/10.31004/jerkin.v5i1.8013

Pika, P. A. T. P., & Putra, A. A. G. A. K. A. (2026). Optimalisasi literasi keuangan digital masyarakat untuk meminimalisir resiko penipuan link phising. Abdimas Galuh, 8(2), 1184–1191. https://doi.org/10.25157/ag.v8i2.23667

Pratama, S. D., Lasimin, L., & Dadaprawira, M. N. (2023). Pengujian black box testing pada aplikasi Edu Digital berbasis website menggunakan metode equivalence dan boundary value. Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD, 6(2), 560–569. https://doi.org/10.53513/jsk.v6i2.8166

Riandi, M. H., Putri, I. L. A., Rahman, H. A., & Kusumadewi, A. W. (2023). Perilaku keamanan siber bagi UMKM. Jurnal Pengabdian kepada Masyarakat Nusantara, 4(5), 278–283.

Sofyan, A., Nurdin, A., & Santoso, D. (2023). Pengujian black box aplikasi presensi karyawan dengan teknik equivalence partitioning. LOGIC: Jurnal Ilmu Komputer dan Pendidikan, 2(1), 59–65. https://journal.mediapublikasi.id/index.php/logic/article/view/2753

Sukmana, Y., & Rosmansyah, Y. (2021). The use of Cloud Firestore for handling real-time data updates: An empirical study of gamified online quiz. In Proceedings of the 2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT) (pp. 1239–1244). IEEE. https://doi.org/10.1109/CECIT53797.2021.00220

Tarsini, I., & Anggraeni, R. (2024). Explore flowchart and pseudocode concepts in algorithms and programming. Indonesian Journal of Multidisciplinary Science, 3(5). https://doi.org/10.55324/ijoms.v3i5.807

Tupsamudre, H., Jain, S., & Lodha, S. (2021). PhishMatch: A layered approach for effective detection of phishing URLs (arXiv:2112.02226). arXiv.

Uiphanit, T., Chutosri, T., Wattanaprapa, N., Bunchongkien, W., Chiewchan, P., & Nachin, N. (2025). Phishing awareness through game-based learning: A mobile-responsive web application for middle school learners. International Journal of Interactive Mobile Technologies (iJIM), 19(12), 55–67. https://doi.org/10.3991/ijim.v19i12.53199

Umbu Pingge, R. M. P., Nalle, S. M., Mali, A. K., Saputra, P. A., & Feoh, G. (2023). Implementasi use case diagram dan activity diagram pada perancangan aplikasi pembelajaran bahasa Inggris berbasis Android di SDN 5 Gulingan. Prosiding SINTESA, 6, 407–418. https://jurnal.undhirabali.ac.id/index.php/sintesa/article/view/2832

Wayahdi, M. R., & Ruziq, F. (2023). Pemodelan sistem penerimaan anggota baru dengan Unified Modeling Language (UML) (Studi kasus: Programmer Association of Battuta). Jurnal Minfo Polgan, 12(1), 1514–1521. https://doi.org/10.33395/jmp.v12i1.12870

Wulandari, Nofiyani, & Hasugian, H. (2023). User acceptance testing (UAT) pada electronic data preprocessing guna mengetahui kualitas sistem. JMIK (Jurnal Mahasiswa Ilmu Komputer), 4(1), 20–27. https://scholar.ummetro.ac.id/index.php/IlmuKomputer/article/view/3383

Yakub, H., Daniawan, B., Wijaya, A., & Damayanti, L. (2024). Sistem informasi e-commerce berbasis website dengan metode pengujian user acceptance testing. JSITIK: Jurnal Sistem Informasi dan Teknologi Informasi Komputer, 2(2), 113-127.https://doi.org/10.53624/jsitik.v2i2.36