Jurnal Algoritma, Logika dan Komputasi *Vol.IX (No. 02) : 46 - 53. Th. 2026*
Versi Online: https://journal.ubm.ac.id/index.php/alu *p-ISSN: 2620-620X*
DOI: http://dx.doi.org/10.30813/j-alu.v2i2.10143 *e-ISSN: 2621-9840*

PENERAPAN APLIKASI DOMPET DIGITAL BERBASIS *NFC* DENGAN DETEKSI *FRAUD Z-SCORE*

Implementation of NFC-Based Digital Wallet Application with Z-Score Fraud Detection

Alief Ryanto Rahman, 105841104222@student.unismuh.ac.id[1)*], Desi Anggreani, desianggreani@unismuh.ac.id[2)], Muhyiddin A.M. Hayat, muhyiddin@unismuh.ac.id[3)], Chyquitha Danuputri, chyquithadanuputri@unismuh.ac.id[4)], Hijrah, alsyahira.irha@gmail.com[5)]

[1)2)3)4)5)]Program Studi Informatika /Fakultas Teknik, Universitas Muhammadiyah Makassar

Diterima 18 Juni 2026 / Disetujui 24 Juni 2026

ABSTRACT

Near Field Communication (NFC) supports fast and practical contactless payment, yet its implementation in a digital wallet still requires a security mechanism that can recognize unusual transactions during the payment process. This study implements an NFC-based digital wallet application integrated with Z-Score Based Anomaly Detection as a real-time fraud detection mechanism. The system was developed using React Native and Expo Dev Client for the mobile application, Node.js and Express.js for the backend service, SQLite with Prisma ORM for data storage, and a web-based admin dashboard for monitoring. The fraud detection process compares a new transaction with the last twenty historical transactions of each user. The mean and sample standard deviation are calculated from the historical baseline, while the Z-Score determines whether the transaction is classified as ALLOW, REVIEW, or BLOCK. The evaluation was conducted through manual simulation, functional testing, security testing, and Android compatibility testing. The simulation results show that the system correctly classified normal, suspicious, and anomalous transactions. Andri obtained ALLOW with Z = 1.4142, Ibnu obtained REVIEW with Z = 2.6333, and Adit obtained BLOCK with Z = 5.0332. The system also handled the special case of σ = 0 by allowing identical transactions and blocking different transactions. These results indicate that the proposed method is lightweight, explainable, and suitable for prototype-level NFC payment security.
***Keywords**: NFC, Digital Wallet, Fraud Detection, Z-Score, Anomaly Detection*

ABSTRAK

Near Field Communication (*NFC*) memungkinkan pembayaran nirkontak dilakukan secara cepat dan praktis, tet*api* penerapannya pada dompet digital tetap membutuhkan mekanisme keamanan yang mampu mengenali transaksi tidak wajar selama proses pembayaran berlangsung. Penelitian ini mengimplementasikan aplikasi dompet digital berbasis *NFC* yang terintegrasi dengan *Z-Score Based Anomaly Detection* sebag*ai* mekanisme deteksi *fraud* secara *real-time*. Sistem dikembangkan menggunakan *React Native* dan *Expo Dev Client* pada aplikasi *mobile*, *Node.js* dan *Express.js* pada *backend*, *SQLite* melalui *Prisma ORM* sebag*ai* penyimpanan data, serta *dashboard* admin berbasis *web* untuk pemantauan. Proses deteksi *fraud* dilakukan dengan membandingkan transaksi baru terhadap dua puluh transaksi historis terakhir setiap pengguna. Nil*ai mean* dan standar deviasi sampel dihitung dari *baseline* historis, kemudian nil*ai Z-Score* digunakan untuk menentukan keputusan *ALLOW*, *REVIEW*, atau *BLOCK*. Pengujian dilakukan melalui simulasi manual, pengujian fungsional, pengujian keamanan, dan pengujian

*Korespondensi Penulis:
E-mail: **105841104222@student.unismuh.ac.id**

kompatibilitas perangkat *Android*. Hasil simulasi menunjukkan bahwa sistem mampu membedakan transaksi *normal*, mencurigakan, dan anomali. Andri memperoleh keputusan *ALLOW* dengan Z = 1,4142, Ibnu memperoleh *REVIEW* dengan Z = 2,6333, dan Adit memperoleh *BLOCK* dengan Z = 5,0332. Sistem juga mampu menangani kondisi khusus $\sigma = 0$ dengan mengizinkan transaksi identik dan memblokir transaksi yang berbeda dari pola historis. Hasil ini menunjukkan bahwa metode yang diterapkan ringan, transparan, dan relevan untuk keamanan pembayaran *NFC* pada tingkat prototipe.
Kata Kunci: *NFC*, Dompet Digital, Deteksi *Fraud*, *Z-Score*, Deteksi Anomali

PENDAHULUAN

a. Latar Belakang

Perkembangan pembayaran digital mendorong masyarakat menggunakan sistem transaksi yang lebih cepat, praktis, dan minim kontak fisik. Salah satu teknologi yang banyak digunakan untuk mendukung kebutuhan tersebut adalah *Near Field Communication* (*NFC*). Melalui mekanisme *tap-to-pay*, pengguna dapat melakukan pembayaran hanya dengan mendekatkan kartu atau perangkat ke pembaca *NFC*. Namun, kemudahan ini perlu diikuti mekanisme keamanan yang mampu menjaga validitas transaksi dan mencegah penyalahgunaan kartu maupun akun pengguna [1]

Keamanan pembayaran elektronik tidak cukup dinil*ai* dari berhasil atau tidaknya transaksi diproses. Sistem juga harus menjaga kerahasiaan data, integritas saldo, ketersediaan layanan, autentikasi pengguna, dan akuntabilitas aktivitas transaksi. Pada pembayaran berbasis *NFC*, risiko seperti penyadapan, relay attack, cloning, dan manipulasi transaksi tetap perlu diperhatikan karena komunikasi berlangsung cepat dan nirkontak. Oleh karena itu, sistem pembayaran digital membutuhkan pengamanan berl*api*s yang tidak hanya memvalidasi kartu, tet*api* juga memantau kewajaran transaksi pengguna [2]

Penelitian ini menerapkan *Z-Score Based Anomaly Detection* sebag*ai* mekanisme *AI Fraud Detection* pada aplikasi dompet digital berbasis *NFC*. Pendekatan ini dipilih karena tidak memerlukan data *fraud* berlabel, mudah dijelaskan secara matematis, dan dapat dijalankan pada alur transaksi *real-time*. Dengan membandingkan nominal transaksi baru terhadap histori masing-masing pengguna, sistem menghasilkan keputusan *ALLOW*, *REVIEW*, atau *BLOCK* secara transparan dan dapat diaudit. Kajian *fraud detection* juga menekankan pentingnya pola historis transaksi untuk membedakan aktivitas *normal* dan aktivitas mencurigakan [3], [4], [5], [6], [7], [8], [9].

Pemilihan *Z-Score* dalam penelitian ini juga didasarkan pada kebutuhan pembayaran NFC berbasis prototipe yang menuntut proses deteksi ringan dan keputusan cepat saat transaksi berlangsung. Dibandingkan metode pembelajaran mesin tersupervisi yang umumnya memerlukan dataset *fraud* berlabel, proses pelatihan model, serta komputasi yang lebih kompleks, *Z-Score* cukup menggunakan histori transaksi pengguna, memiliki perhitungan sederhana, dan menghasilkan dasar keputusan yang mudah ditelusuri melalui mean, standar deviasi, serta nilai *Z-Score.*

b. Identifikasi Masalah

Berdasarkan ur*ai*an tersebut, permasalahan utama dalam penelitian ini adalah bag*ai*mana membangun aplikasi dompet digital berbasis *NFC* yang mampu menjalankan transaksi *tap-to-pay* secara aman, serta bag*ai*mana menerapkan deteksi *fraud* berbasis *Z-Score* agar sistem dapat menghasilkan keputusan *ALLOW*, *REVIEW*, dan *BLOCK* secara *real-time*.

c. Tujuan dan Manfaat Penelitian

Penelitian ini bertujuan mengimplementasikan aplikasi dompet digital berbasis *NFC* dan mengintegrasikan *Z-Score Based Anomaly Detection* sebag*ai* mekanisme deteksi *fraud*. Manfaat penelitian ini adalah memberikan contoh implementasi sistem pembayaran digital yang dapat diaudit, menjelaskan dasar keputusan risiko secara matematis, serta menjadi referensi pengembangan keamanan aplikasi pembayaran nirkontak.

METODE PENELITIAN

Tahapan Penelitian

Penelitian ini menggunakan pendekatan rekayasa aplikasi yang berfokus pada pembangunan dan pengujian sistem. Tahapan penelitian dimul*ai* dari identifikasi masalah, analisis kebutuhan, perancangan arsitektur, implementasi aplikasi *mobile* dan *backend*, integrasi modul deteksi *fraud*, pengujian fungsional, pengujian keamanan, hingga evaluasi hasil simulasi *Z-Score*. Alur tersebut dipilih agar sistem tidak hanya dijelaskan secara konseptual, tet*api* juga dibuktikan melalui implementasi dan pengujian. Pendekatan rekayasa serta evaluasi artefak sistem ini sejalan dengan prinsip design science research [10]

Arsitektur Sistem

Aplikasi *mobile* dikembangkan menggunakan *React Native*, *Expo Dev Client*, *TypeScript*, *React Navigation*, *AsyncStorage*, dan *React Native NFC Manager*. *Backend* dibangun dengan *Node.js* dan *Express.js*, sedangkan penyimpanan data menggunakan *SQLite* melalui *Prisma ORM*. Sistem juga menyediakan *dashboard* admin berbasis *web* untuk memantau pengguna, transaksi, perangkat, dan *fraud* alert. Komponen tersebut membentuk arsitektur *client-server* yang memisahkan antarmuka pengguna, logika bisnis, dan penyimpanan data [11], [12], [13], [14].

Formula dan Aturan Keputusan *Z-Score*

Deteksi *fraud* dijalankan sebelum transaksi baru disimpan sebag*ai* histori. Sistem mengambil 20 transaksi historis terakhir pengguna sebag*ai baseline* perilaku. Jika histori belum mencap*ai* 20 transaksi, transaksi diizinkan sementara agar *baseline* dapat terbentuk secara bertahap. *Mean* historis dihitung menggunakan rumus (1).

$$\mu = \frac{\sum X_i}{n} \quad (1)$$

Varians sampel dihitung menggunakan koreksi Bessel seperti pada rumus (2), kemudian standar deviasi dihitung melalui rumus (3). Koreksi Bessel digunakan karena data historis diperlakukan sebag*ai* sampel perilaku pengguna, sehingga pembagi n−1 memberikan estimasi varians yang lebih tepat untuk jumlah data terbatas [15], [16].

$$\sigma^2 = \frac{\sum(X_i-\mu)^2}{n-1} \quad (2)$$

$$\sigma = \sqrt{\sigma^2} \quad (3)$$

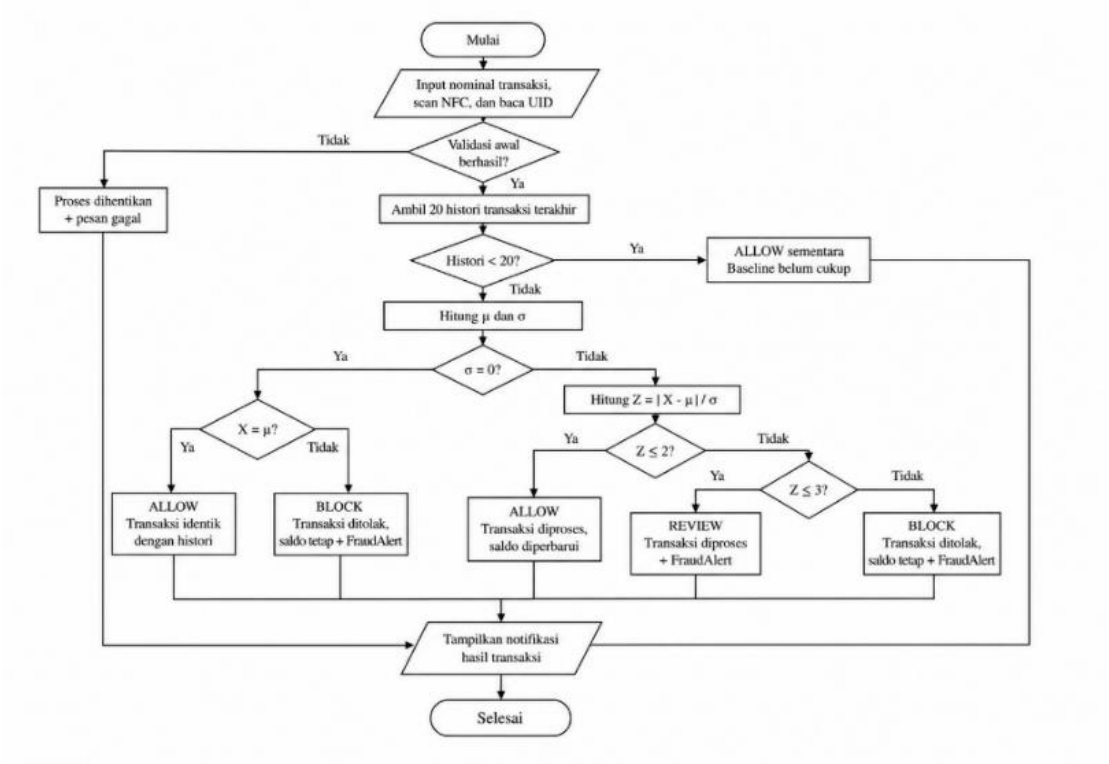
Z-Score dihitung dengan membandingkan transaksi baru X terhadap *mean* historis μ dan standar deviasi σ sebag*ai*mana ditunjukkan pada rumus (4). Nil*ai* absolut digunakan agar penyimpangan nominal, b*ai*k lebih besar maupun lebih kecil dari kebiasaan pengguna, tetap dapat dikenali sebag*ai* anomali.

$$Z = \frac{|X-\mu|}{\sigma} \quad (4)$$

Keputusan sistem ditentukan berdasarkan *threshold* statistik. Transaksi dengan $Z \leq 2$ diklasifikasikan sebag*ai ALLOW*, transaksi dengan $2 < Z \leq 3$ diklasifikasikan sebag*ai REVIEW*, sedangkan transaksi dengan $Z > 3$ diklasifikasikan sebag*ai BLOCK*. *Threshold* tersebut mengacu pada prinsip distribusi *normal* dan aturan tiga sigma yang umum digunakan dalam pengendalian statistik [15], [17]. Kondisi khusus $\sigma = 0$ ditangani tanpa pembagian: jika $X = \mu$ maka transaksi *ALLOW*, sedangkan jika $X \neq \mu$ maka transaksi *BLOCK*.

Flowchart Ringkas Proses Transaksi dan Deteksi *Fraud*

Gambar 1 menyajikan alur transaksi *NFC* dan deteksi *fraud*, mul*ai* dari input dan validasi awal, proses *Z-Score*, keputusan *ALLOW*, *REVIEW*, atau *BLOCK*, hingga notifikasi hasil transaksi.



Gambar 1. Flowchart transaksi *NFC* dan deteksi *fraud*.

Tabel 1 menyajikan parameter utama yang digunakan dalam implementasi algoritma *Z-Score Based Anomaly Detection* pada aplikasi dompet digital *NFC*.

Tabel 1. Parameter Implementasi Algoritma *Z-Score*

Parameter	Nil*ai* / Kondisi	Keputusan / Fungsi
Baseline	20 transaksi historis terakhir	Membentuk pola *normal* pengguna
$Z \leq 2$	Penyimpangan rendah	*ALLOW* / *NORMAL*
$2 < Z \leq 3$	Penyimpangan sedang	*REVIEW* / *SUSPICIOUS*
$Z > 3$	Penyimpangan ekstrem	*BLOCK* / *ANOMALY*
$\sigma = 0$ dan $X = \mu$	Transaksi identik	*ALLOW*
$\sigma = 0$ dan $X \neq \mu$	Menyimpang dari pola identik	*BLOCK*
Histori < 20	*Baseline* belum cukup	*ALLOW* sementara

HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil implementasi aplikasi, simulasi perhitungan *Z-Score*, pengujian sistem, serta pembahasan yang meng*ai*tkan temuan penelitian dengan konsep deteksi anomali dan penelitian terdahulu.

Implementasi Sistem

Aplikasi dompet digital berbasis *NFC* berhasil dibangun dengan fitur *login*, registrasi pengguna, registrasi kartu *NFC*, pembayaran *NFC*, *top up* saldo, riwayat transaksi, *dashboard* pengguna, *dashboard* admin, dan pembuatan *fraud* alert. Implementasi ini menunjukkan bahwa proses pembayaran dan deteksi risiko berada dalam satu alur sistem yang saling terhubung.

Secara antarmuka, sistem diimplementasikan melalui aplikasi *mobile* dan *dashboard* admin. Pada sisi *mobile,* antarmuka digunakan untuk mendukung proses login, registrasi pengguna, registrasi kartu *NFC,* top up saldo, pembayaran *NFC,* dan riwayat transaksi. Pada sisi admin*, dashboard* digunakan untuk memantau data pengguna, transaksi, perangkat, kartu *NFC,* serta *fraud alert* yang muncul dari keputusan *REVIEW* atau *BLOCK*. Dengan demikian, antarmuka sistem berfungsi sebagai media operasional dan monitoring, sedangkan pembuktian

ilmiah pada artikel ini difokuskan pada alur logika sistem dan hasil evaluasi algoritma melalui flowchart proses transaksi serta grafik hasil *Z-Score*.

Backend berperan sebagai pusat validasi dan pengambilan keputusan. Pada endpoint pembayaran *NFC,* sistem memeriksa JWT, format input, status kartu, kecukupan saldo, histori transaksi, dan hasil perhitungan *Z-Score*. Jika keputusan yang dihasilkan adalah ALLOW atau *REVIEW*, transaksi tetap diproses dan saldo diperbarui. Jika keputusan *BLOCK,* transaksi ditolak dan *fraud alert* dibuat untuk ditinjau admin.

Model *database* meliputi *User, Transaction, FraudAlert, Device, UserSession, AdminLog, SystemSettings, NFCCard,* dan *NFCTransactio*n. Struktur tersebut mendukung pencatatan transaksi, pemantauan perangkat, pengelolaan kartu, audit aktivitas, serta penyimpanan dasar keputusan fraud detection secara terstruktur.

Simulasi dan Analisis *Z-Score*

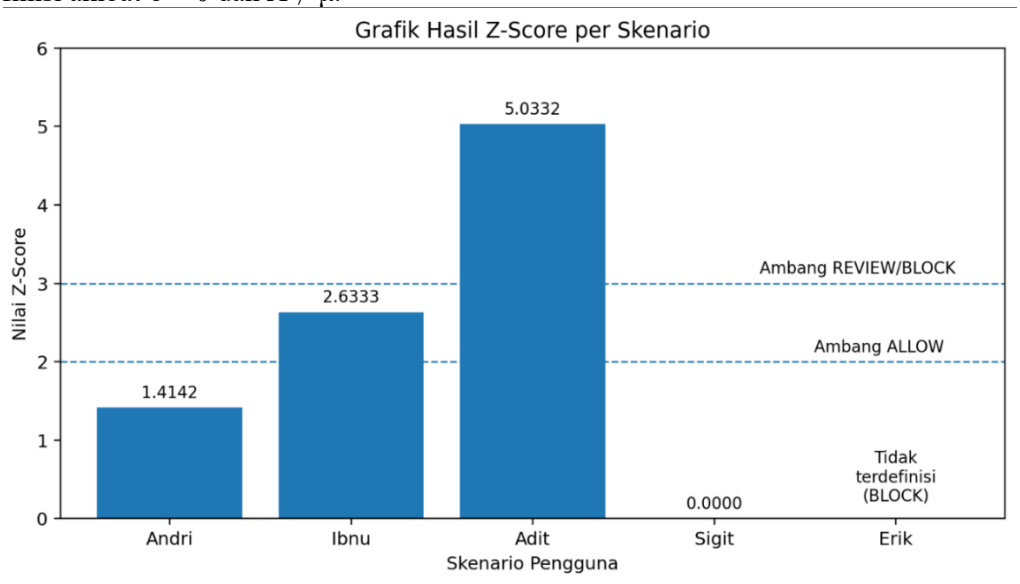
Pengujian deteksi *fraud* dilakukan melalui lima skenario simulasi. Tiga skenario utama mewakili keputusan *ALLOW*, *REVIEW*, dan *BLOCK*, sedangkan dua skenario tambahan digunakan untuk menguji kondisi khusus $\sigma = 0$. Setiap simulasi menggunakan 20 transaksi historis sebag*ai baseline* dan satu transaksi baru sebag*ai* data yang dievaluasi.

Tabel 2 menunjukkan bahwa sistem mampu membedakan transaksi *normal*, mencurigakan, dan anomali ekstrem berdasarkan standar deviasi historis masing-masing pengguna. Hasil ini menegaskan bahwa keputusan tidak hanya dipengaruhi oleh nominal transaksi baru, tet*api* juga oleh konsistensi pola transaksi pengguna.

Tabel 2. Ringkasan Hasil Simulasi *Z-Score*

Pengguna	μ	σ	X Baru	*Z-Score*	Keputusan
Andri	Rp50.000	Rp1.414,21	Rp52.000	1,4142	*ALLOW*
Ibnu	Rp50.000	Rp3.797,51	Rp60.000	2,6333	*REVIEW*
Adit	Rp50.000	Rp794,72	Rp54.000	5,0332	*BLOCK*
Sigit	Rp50.000	0	Rp50.000	0 / khusus	*ALLOW*
Erik	Rp50.000	0	Rp51.000	Tidak terdefinisi	*BLOCK*

Untuk melengk*api* hasil simulasi, Gambar 2 menampilkan visualisasi nil*ai Z-Score* pada setiap skenario. Andri memperoleh $Z = 1{,}4142$ dan berada di bawah ambang 2 sehingga diklasifikasikan sebag*ai ALLOW*. Ibnu memperoleh $Z = 2{,}6333$ dan berada pada rentang $2 < Z \leq 3$ sehingga masuk kategori *REVIEW*. Adit memperoleh $Z = 5{,}0332$ yang melebihi ambang 3 sehingga diklasifikasikan sebag*ai BLOCK*. Sigit ditampilkan bernil*ai* 0 karena transaksi identik dengan rata-rata historis, sedangkan Erik tidak divisualisasikan pada grafik karena nil*ai* Z tidak terdefinisi akibat $\sigma = 0$ dan $X \neq \mu$.



Gambar 2. Grafik hasil *Z-Score* per skenario.

Interpretasi Hasil Simulasi

Pada skenario Andri, transaksi Rp52.000 menghasilkan Z = 1,4142 sehingga sistem menetapkan *ALLOW* dan tidak membuat *fraud* alert. Pada skenario Ibnu, transaksi Rp60.000 menghasilkan Z = 2,6333 sehingga sistem menetapkan *REVIEW*, memproses transaksi, dan membuat *fraud* alert. Pada skenario Adit, transaksi Rp54.000 menghasilkan Z = 5,0332 sehingga sistem menetapkan *BLOCK*, menolak transaksi, dan menjaga saldo tetap tidak berubah.

Dua skenario tambahan menunjukkan bahwa sistem menangani $\sigma = 0$ secara eksplisit. Pada Sigit, seluruh histori bernil*ai* Rp50.000 dan transaksi baru juga Rp50.000, sehingga sistem menetapkan *ALLOW*. Pada Erik, histori bernil*ai* Rp50.000 tet*api* transaksi baru Rp55.000, sehingga sistem menetapkan *BLOCK* karena transaksi menyimpang dari pola historis yang sepenuhnya identik.

Pengujian Fungsionalitas, Keamanan, dan Kompatibilitas

Sel*ai*n simulasi *Z-Score*, sistem diuji menggunakan *black box testing*, pengujian keamanan, dan pengujian kompatibilitas *Android*. Pengujian ini memverifikasi alur autentikasi, registrasi kartu, pembayaran *NFC*, validasi saldo, pembuatan *fraud* alert, pembatasan status kartu, serta kestabilan aplikasi pada beberapa perangkat *Android* [18]

Tabel 3. Rekap Hasil Pengujian Sistem

Jenis Pengujian	Jumlah / Objek Uji	Hasil Utama
Black Box Testing	60 kasus uji	Fitur utama berjalan sesu*ai* skenario.
Pengujian Keamanan	10 skenario	Token, input, saldo, dan *FraudAlert* tervalidasi.
Kompatibilitas *Android*	3 perangkat	Aplikasi berjalan pada perangkat uji.
Keputusan *Fraud*	5 skenario	*ALLOW*, *REVIEW*, dan *BLOCK* sesu*ai* aturan *Z-Score*.

Untuk memperlihatkan konsistensi keputusan sistem pada setiap skenario pengujian, hasil keputusan *ALLOW*, *REVIEW*, dan *BLOCK* diringkas pada Tabel 4.

Tabel 4. Performa Keputusan Sistem per Skenario

Skenario	Keputusan	Status Transaksi	*FraudAlert*
Andri	*ALLOW*	Diproses; saldo diperbarui	Tidak dibuat
Ibnu	*REVIEW*	Diproses; saldo diperbarui	Dibuat
Adit	*BLOCK*	Ditolak; saldo tetap	Dibuat
Sigit	*ALLOW* khusus $\sigma = 0$	Diproses; histori identik	Tidak dibuat
Erik	*BLOCK* khusus $\sigma = 0$	Ditolak; $X \neq \mu$	Dibuat

Berdasarkan Tabel 4, seluruh skenario menunjukkan hubungan yang konsisten antara nil*ai* *Z-Score*, status transaksi, dan pembentukan *FraudAlert*. Keputusan *ALLOW* tidak menghasilkan alert, keputusan *REVIEW* tetap memproses transaksi tet*api* membuat alert, sedangkan keputusan *BLOCK* menolak transaksi dan mencatat alert untuk ditinjau admin.

Pembahasan Umum

Hasil penelitian menunjukkan bahwa *Z-Score Based Anomaly Detection* dapat digunakan sebag*ai* mekanisme deteksi *fraud* yang ringan, transparan, dan mudah diaudit. Keputusan sistem dapat dijelaskan melalui *mean*, standar deviasi, dan *Z-Score*, sehingga admin memiliki dasar yang jelas ketika suatu transaksi diklasifikasikan sebag*ai normal*, mencurigakan, atau anomali.

Sebag*ai* acuan tambahan pada aspek pengembangan dan evaluasi sistem berbasis kecerdasan buatan, [18] menunjukkan bahwa sistem *AI* yang disesu*ai*kan dengan data spesifik institusi dapat dievaluasi melalui metrik kinerja dan penerimaan pengguna. Meskipun dom*ai*n penelitian tersebut berbeda, prinsip evaluasi sistem berbasis data spesifik dom*ai*n relevan dengan penelitian ini karena modul deteksi *fraud* juga diuji melalui simulasi, pengujian fungsional, dan interpretasi keputusan sistem.

Sistem juga bersifat personal karena batas kewajaran transaksi dibentuk dari histori masing-masing pengguna. Transaksi Rp54.000 pada Adit diblokir karena pola historisnya sangat konsisten, sedangkan transaksi Rp52.000 pada Andri tetap diizinkan karena masih berada dalam

batas variasi normal. Temuan ini menunjukkan bahwa pendekatan berbasis histori lebih adaptif dibandingkan batas nominal tetap.

Keterbatasan penelitian ini terletak pada penggunaan nominal transaksi sebag*ai* satu-satunya variabel analisis. Variabel l*ai*n seperti waktu transaksi, frekuensi, lokasi, penerima, perangkat, dan pola *login* belum dimasukkan ke dalam model. Sel*ai*n itu, implementasi masih berada pada tingkat prototipe sehingga penguatan produksi, seperti HTTPS/TLS, *secure storage*, *certificate pinning*, *challenge-response NFC*, dan *root detection*, masih perlu diterapkan pada pengembangan berikutnya [11], [6], [19], [7], [12].

Perbandingan dengan Penelitian Sebelumnya

Untuk mendukung pembahasan, penelitian ini dibandingkan dengan lima penelitian terdahulu yang paling relevan. Perbandingan tersebut digunakan untuk menegaskan perbedaan fokus dan kontribusi penelitian, sebag*ai*mana ditunjukkan pada Tabel 5.

Tabel 5. Penelitian Terdahulu

Penelitian	Fokus Utama	Kontribusi / Perbedaan Penelitian Ini
Onumadu dan Abroshan [1]	Ancaman siber dan mitigasi transaksi *NFC*.	Dasar keamanan *NFC*; diterapkan sebag*ai* validasi transaksi dan deteksi *fraud*.
Dewi dkk. [9]	Keamanan pembayaran elektronik.	Acuan keamanan e-payment: token, kartu, saldo, dan alert.
Bolton dan Hand [3]	*Statistical fraud detection*.	Dasar statistik *fraud detection* berbasis pola historis.
Chandola dkk. [4]	*Anomaly detection*.	Dasar *anomaly detection* pada nominal transaksi.
Vanini dkk. [8]	*Risk management* pembayaran.	Acuan perubahan anomali menjadi *ALLOW*, *REVIEW*, dan *BLOCK*.

Berdasarkan Tabel 5, penelitian sebelumnya membahas keamanan *NFC*, keamanan pembayaran elektronik, *statistical fraud detection*, *anomaly detection*, dan *risk management* pembayaran. Penelitian ini berbeda karena menerapkan deteksi anomali berbasis *Z-Score* secara langsung pada aplikasi dompet digital *NFC*, mul*ai* dari aplikasi *mobile*, *backend REST API*, *database*, *dashboard* admin, hingga keputusan operasional *ALLOW*, *REVIEW*, dan *BLOCK*.

SIMPULAN

Penelitian ini berhasil mengimplementasikan aplikasi dompet digital berbasis *NFC* yang terintegrasi dengan *AI Fraud Detection* menggunakan *Z-Score Based Anomaly Detection*. Sistem dibangun dengan aplikasi *mobile*, *backend REST API*, *database SQLite-Prisma*, dan *dashboard* admin, sehingga alur transaksi dapat diproses, divalidasi, dianalisis, dan dipantau secara terstruktur.

Hasil simulasi menunjukkan bahwa sistem mampu mengklasifikasikan transaksi sesu*ai* *threshold* yang ditetapkan. Andri memperoleh keputusan *ALLOW* dengan Z = 1,4142, Ibnu memperoleh *REVIEW* dengan Z = 2,6333, dan Adit memperoleh *BLOCK* dengan Z = 5,0332. Sistem juga mampu menangani $\sigma = 0$ dengan mengizinkan transaksi yang identik dengan histori dan memblokir transaksi yang berbeda dari histori identik.

Pengembangan berikutnya disarankan menambahkan variabel waktu, frekuensi transaksi, lokasi, penerima, *device fingerprint*, *challenge-response NFC*, serta penguatan keamanan produksi. Penambahan variabel tersebut diharapkan dapat meningkatkan ketepatan deteksi sekaligus menjaga keseimbangan antara keamanan transaksi dan kenyamanan pengguna, khususnya pada implementasi *NFC* dan aplikasi pembayaran yang mengikuti praktik keamanan berlapis.

DAFTAR PUSTAKA

[1] P. Onumadu and H. Abroshan, "Near-field communication (NFC) cyber threats and mitigation solutions in payment transactions: A review," *Sensors*, vol. 24, no. 23, p.

7423, 2024, doi: 10.3390/s24237423.

[2] A. C. Dewi, E. I. H. Ujianto, and R. Rianto, "Electronic payment threats and security: A systematic literature review," *J. Nas. Pendidik. Tek. Inform.*, vol. 13, no. 2, 2024.

[3] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Stat. Sci.*, vol. 17, no. 3, pp. 235–255, 2002, doi: 10.1214/ss/1042727940.

[4] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, 2009, doi: 10.1145/1541880.1541882.

[5] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decis. Support Syst.*, vol. 50, no. 3, pp. 559–569, 2011.

[6] P. Vanini, S. Rossi, E. Zvizdic, and T. Domenig, "Online payment fraud: From anomaly detection to risk management," *Financ. Innov.*, vol. 9, no. 1, p. 66, 2023, doi: 10.1186/s40854-023-00470-w.

[7] Y. Kou, C. T. Lu, S. Sirwongwattana, and Y. P. Huang, "Survey of fraud detection techniques BT - IEEE International Conference on Networking, Sensing and Control," 2004, pp. 749–754.

[8] P. Vanini, S. Rossi, E. Zvizdic, and T. Domenig, "Online payment fraud: from anomaly detection to risk management," *Financ. Innov.*, vol. 9, no. 1, 2023, doi: 10.1186/s40854-023-00470-w.

[9] Amelia Citra Dewi, Erik Iman Heri Ujianto, and R. Rianto, "Electronic Payment Threats and Security: A Systematic Literature Review," *J. Nas. Pendidik. Tek. Inform.*, vol. 13, no. 2, pp. 301–315, 2024, doi: 10.23887/janapati.v13i2.76635.

[10] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.

[11] EMVCo, "EMV Contactless Specifications for Payment Systems, Book C-8: Kernel 8 Specification, Version 1.1," EMVCo, LLC, 2021.

[12] N. X. P. Semiconductors, "NTAG213/215/216: NFC Forum Type 2 Tag IC with 144/504/888 bytes EEPROM: Data Sheet," NXP Semiconductors, 2021. [Online]. Available: https://www.nxp.com/docs/en/data-sheet/NTAG213_215_216.pdf

[13] I. Meta Platforms, "React Native Documentation: Learn Once, Write Anywhere," 2023. [Online]. Available: https://reactnative.dev/docs/getting-started

[14] I. Prisma Data, "Prisma ORM Documentation: Database Toolkit for Node.js and TypeScript," 2023. [Online]. Available: https://www.prisma.io/docs

[15] OpenStax, *Introductory Statistics 2e: The Standard Normal Distribution*. Rice University, 2023. [Online]. Available: https://openstax.org/books/introductory-statistics-2e

[16] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes: The Art of Scientific Computing*, 3rd ed. Cambridge University Press, 2007.

[17] D. C. Montgomery, *Introduction to Statistical Quality Control*, 7th ed. John Wiley & Sons, 2012.

[18] O. Foundation, "OWASP Application Security Verification Standard," OWASP Foundation, 2024. [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/

[19] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decis. Support Syst.*, vol. 50, no. 3, pp. 602–613, 2011, doi: 10.1016/j.dss.2010.08.006.