



**IMPLEMENTASI ZERO TRUST ACCESS CONTROL
DAN ENKRIPSI AES-GCM PADA PLATFORM
MONITORING BERBASIS *PROGRESSIVE WEB APP*
(PWA)**

SKRIPSI

**SALSABILLA AULIA
2207421049**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
TAHUN 2026**



**IMPLEMENTASI ZERO TRUST ACCESS CONTROL
DAN ENKRIPSI AES-GCM PADA PLATFORM
MONITORING BERBASIS *PROGRESSIVE WEB APP*
(PWA)**

SKRIPSI

**Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk
Memperoleh Diploma Empat Politeknik**

**SALSABILLA AULIA
2207421049**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
TAHUN 2026**



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Salsabilla Aulia

NIM : 2207421049

Jurusan/Program Studi : T. Informatika dan Komputer / T. Multimedia dan Jaringan

Judul skripsi : IMPLEMENTASI ZERO TRUST ACCESS CONTROL
DAN ENKRIPSI AES-GCM PADA PLATFORM MONITORING BERBASIS
PROGRESSIVE WEB APP (PWA)

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 9 Juni 2026
Yang membuat pernyataan



(Salsabilla Aulia)
NIM. 2207421049



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : Salsabilla Aulia
NIM : 2207421049
Program Studi : TMJ
Judul Skripsi : IMPLEMENTASI ZERO TRUST ACCESS CONTROL
DAN ENKRIPSI AES-GCM PADA PLATFORM MONITORING BERBASIS
PROGRESSIVE WEB APP (PWA)

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Selasa Tanggal 23
Bulan Juni Tahun 2026 dan dinyatakan **LULUS**.

Disahkan oleh:

Pembimbing I : Susana Dwi Yulianti, M.Kom.

Penguji I : Maria Agustin, S.Kom., M.Kom.

Penguji II : Dr. Defiana Arnaldy, S.Tp., M.Si.

Penguji III : Chandra Wirawan, S.Kom., M.Kom.

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.

NIP. 197908032003122003



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala limpahan rahmat, hidayah, dan karunia-Nya, sehingga skripsi yang berjudul "Implementasi Zero Trust Access Control dan Enkripsi AES-GCM pada Platform Monitoring Berbasis Progressive Web App (PWA)" ini dapat diselesaikan dengan baik. Penulis menyadari bahwa tanpa pertolongan-Nya, proses penyusunan skripsi ini tidak akan dapat dilalui hingga tahap akhir.

Skripsi ini tidak lepas dari dukungan, bantuan, dan doa dari berbagai pihak yang telah memberikan kontribusi selama proses penelitian dan penyusunannya. Oleh karena itu, penulis ingin menyampaikan terima kasih kepada:

1. Ibu Susana Dwi Yulianti, S.Kom, M.Kom, selaku dosen pembimbing, yang telah dengan sabar meluangkan waktu, tenaga, dan pikiran untuk memberikan arahan, bimbingan, serta masukan yang sangat berharga selama proses penelitian dan penyusunan skripsi ini.
2. Kedua orang tua penulis, yang selalu menjadi rumah, tempat pulang, sekaligus sumber kekuatan terbesar bagi penulis. Terima kasih atas kasih sayang yang tidak pernah berkurang, doa yang tidak pernah putus, pengorbanan yang tidak pernah dihitung, serta dukungan moral maupun material yang selalu diberikan. Semoga segala pengorbanan dan doa yang telah diberikan menjadi amal kebaikan yang senantiasa dibalas oleh Allah SWT.
3. Mas dan adik, yang selalu menjadi panutan sekaligus penyemangat bagi penulis untuk terus belajar, bertumbuh, dan menjadi pribadi yang lebih baik. Terima kasih karena kehadiran kalian selalu menjadi penguat bagi penulis selama menempuh pendidikan hingga menyelesaikan skripsi ini.
4. Izzaturrachmi, rekan satu tim skripsi, atas kerja sama, diskusi, saling membantu, dan perjuangan bersama dalam merancang, mengembangkan, serta menyelesaikan penelitian ini. Terima kasih telah menjadi partner yang selalu berusaha memberikan yang terbaik hingga penelitian ini dapat diselesaikan.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

5. Rekan-rekan PBL, yaitu Abian, Azzuri, Ayu, Christian, Pratama, dan Rei, atas kebersamaan, dukungan, semangat, serta pengalaman berharga yang telah dibagikan selama proses perkuliahan dan pengerjaan proyek.
6. Sahabat-sahabat penulis sejak SMP, yaitu Nanda, Vindka, dan Dian, yang selalu hadir memberikan semangat, doa, tawa, serta menjadi tempat berbagi cerita. Terima kasih telah menjadi sahabat yang tetap kebersamai hingga hari ini.
7. Seluruh teman-teman Teknik Multimedia dan Jaringan angkatan 2022 (TMJ 22), atas kebersamaan, bantuan, dan kenangan yang telah menjadi bagian penting dalam perjalanan akademik penulis di Politeknik Negeri Jakarta.
8. Seluruh dosen, tenaga kependidikan, serta semua pihak yang tidak dapat penulis sebutkan satu per satu, yang telah memberikan ilmu, bantuan, dan dukungan selama penulis menempuh pendidikan hingga penyelesaian skripsi ini.

Penulis menyadari bahwa skripsi ini masih memiliki berbagai keterbatasan dan jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi penyempurnaan penelitian di masa mendatang. Semoga skripsi ini dapat memberikan manfaat bagi pembaca serta berkontribusi terhadap pengembangan ilmu pengetahuan, khususnya di bidang keamanan siber dan pengembangan aplikasi berbasis web.

Depok, 9 Juni 2026

Salsabilla Aulia



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI
SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama : Salsabilla Aulia

NIM : 2207421049

Jurusan/Program Studi : T. Informatika dan Komputer / T. Multimedia dan Jaringan
Demi pengembangan ilmu pengetahuan , menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul :

IMPLEMENTASI ZERO TRUST ACCESS CONTROL DAN ENKRIPSI AES-GCM PADA PLATFORM MONITORING BERBASIS *PROGRESSIVE WEB APP* (PWA)

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 09 Juni 2026

Yang menyatakan



Salsabilla Aulia



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Implementasi Zero Trust Access Control dan Enkripsi AES-GCM Pada Platform Monitoring Berbasis *Progressive Web App* (PWA)

ABSTRAK

Posyandu memiliki peran penting dalam memantau pertumbuhan balita dan mencegah stunting. Namun, digitalisasi pencatatan kesehatan masih menghadapi masalah keamanan data dan keterbatasan koneksi internet. Penelitian ini bertujuan mengembangkan platform pemantauan gizi untuk Posyandu Orchid yang aman dan tetap dapat digunakan saat jaringan tidak stabil. Sistem dikembangkan menggunakan *Progressive Web App* (PWA) dengan pendekatan *Offline-First*. Keamanan data diterapkan melalui Zero Trust Access Control, Role-Based Access Control (RBAC), JSON Web Token (JWT), dan enkripsi AES-256-GCM menggunakan Web Crypto API. Kemampuan bekerja secara luring didukung oleh IndexedDB, Service Worker, dan Background Sync. Hasil pengujian menunjukkan bahwa seluruh skenario fungsional dan keamanan berhasil dijalankan dengan tingkat keberhasilan 100%. Sistem mampu mendeteksi perubahan data yang tidak sah, memiliki latensi enkripsi di bawah 1 milidetik, serta mencapai tingkat keberhasilan sinkronisasi data 100% tanpa kehilangan data. Pengujian beban dengan 30 pengguna virtual juga menunjukkan sistem tetap stabil tanpa kegagalan layanan. Berdasarkan hasil tersebut, sistem yang dikembangkan berhasil meningkatkan keamanan data kesehatan dan menjaga ketersediaan layanan pada kondisi jaringan yang tidak stabil.

Kata Kunci: AES-256-GCM, Posyandu, *Progressive Web App*, Web Crypto API, Zero Trust.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME.....	III
LEMBAR PENGESAHAN.....	IV
KATA PENGANTAR.....	V
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI UNTUK KEPENTINGAN AKADEMIS.....	VII
ABSTRAK.....	VIII
DAFTAR ISI.....	IX
DAFTAR GAMBAR.....	XI
DAFTAR TABEL.....	XII
BAB I	
PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Perumusan Masalah.....	3
1.3 Batasan Masalah.....	4
1.4 Tujuan dan Manfaat.....	4
1.4.1 Tujuan.....	4
1.4.2 Manfaat.....	4
1.5 Sistematika Penulisan.....	5
BAB II	
TINJAUAN PUSTAKA.....	7
2.1 Digitalisasi Posyandu dan Tantangan Keamanan Data.....	7
2.2 Internet of Things (IoT) dalam Kesehatan Masyarakat.....	7
2.3 Arsitektur Zero Trust Network Access (ZTNA).....	7
2.4 Enkripsi AES-GCM.....	9
2.5 Analisis Kinerja Web Crypto API dan Latensi Enkripsi.....	10
2.6 Progressive Web Apps (PWA) dan Resiliensi Jaringan.....	11
2.7 JSON Web Token (JWT) dan Manajemen Sesi Stateless.....	12
2.8 Black Box Testing.....	13
2.9 Negative Testing.....	13
2.10 OWASP Web Security Testing Guide (WSTG).....	13
2.11 Standar Usabilitas Latensi Nielsen.....	14
2.12 Penelitian Terdahulu.....	14
BAB III	
METODE PENELITIAN.....	18
3.1 Rancangan Penelitian.....	18
3.2 Objek Penelitian.....	20
3.3 Sumber Data.....	21
3.4 Teknik Pengumpulan Data.....	22



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB IV	
HASIL DAN PEMBAHASAN.....	24
4.1 Analisis Kebutuhan.....	24
4.1.1 Kebutuhan Fungsional.....	24
4.1.2 Kebutuhan Non-Fungsional.....	25
4.1.3 Kebutuhan Perangkat Keras (Hardware/Infrastructure).....	26
4.1.4 Kebutuhan Perangkat Lunak (Software).....	27
4.2 Perancangan Sistem.....	27
4.2.1 Arsitektur Jaringan.....	27
4.2.2 Topologi Jaringan.....	28
4.2.3 Diagram Alur Sistem (Flowchart).....	30
4.3 Implementasi Sistem.....	33
4.3.1 Implementasi Lingkungan Sistem.....	33
4.3.2 Implementasi Kriptografi Sisi Klien (Web Crypto API).....	34
4.3.3 Implementasi Dekripsi dan Autentikasi Sisi Server (Zero Trust Middleware).....	38
4.3.4 Implementasi Resiliensi PWA dan Penyimpanan Luring (IndexedDB & Service Worker).....	41
4.4 Pengujian.....	44
4.4.1 Deskripsi Pengujian.....	44
4.4.2 Prosedur Pengujian.....	45
4.4.3 Data Hasil Pengujian.....	49
A. Hasil Pengujian Fitur dan Kontrol Akses.....	49
B. Hasil Pengujian Keamanan dan Integritas Data.....	50
C. Hasil Pengujian Latensi Komputasi Kriptografi.....	51
D. Hasil Pengujian Resiliensi PWA pada Kondisi Jaringan Fluktuatif.....	52
E. Hasil Pengujian Beban dan Skalabilitas Server Backend.....	53
4.4.4 Analisis Data dan Evaluasi Pengujian.....	54
A. Analisis Pengujian Fitur dan Kontrol Akses.....	54
B. Analisis Pengujian Keamanan dan Integritas Data.....	55
C. Analisis Pengujian Latensi Komputasi Kriptografi.....	56
D. Analisis Resiliensi PWA pada Kondisi Jaringan Fluktuatif.....	57
E. Analisis Pengujian Beban dan Skalabilitas Server Backend.....	58
BAB V	
PENUTUP.....	59
5.1 Kesimpulan.....	59
5.2 Saran.....	60
DAFTAR PUSTAKA.....	61
DAFTAR RIWAYAT HIDUP.....	65
LAMPIRAN.....	66



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR GAMBAR

Gambar 3.1 Flowchart Tahapan Penelitian.....	19
Gambar 4.1 Arsitektur Jaringan.....	28
Gambar 4.2 Topologi Jaringan.....	29
Gambar 4.3 Alur Enkripsi dan Pengiriman Data - Mode Online (Client-Side).....	30
Gambar 4.4 Alur Sinkronisasi Delay-Tolerant - Mode Offline (PWA Side).....	31
Gambar 4.5 Alur Dekripsi dan Validasi Sesi (Server-Side).....	32
Gambar 4.6 Fungsi Enkripsi Sisi Klien Menggunakan Web Crypto API.....	35
Gambar 4.7 Pemanggilan Fungsi Enkripsi dan Pengukuran Latensi pada Event Handler Tombol Simpan.....	36
Gambar 4.8 Antarmuka Form Sebelum Enkripsi (Plaintext).....	37
Gambar 4.9 Hasil Enkripsi AES-GCM Aliran Paket Jaringan Wireshark.....	38
Gambar 4.10 Fungsi Enkripsi dan Dekripsi AES-256-GCM Sisi Server.....	39
Gambar 4.11 Respons Penolakan Server akibat Manipulasi Integritas Data.....	40
Gambar 4.12 Respons Kesuksesan Penerimaan dan Dekripsi Data yang Valid....	41
Gambar 4.13 Notifikasi Pengalihan Penyimpanan ke Mode Luring.....	42
Gambar 4.14 Antrean Data Terenkripsi pada Penyimpanan IndexedDB Klien.....	43
Gambar 4.15 Status Aktif Komponen Service Worker pada browser Klien.....	43

POLITEKNIK
NEGERI
JAKARTA



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu.....	14
Tabel 4.1 Spesifikasi Perangkat Keras dan Infrastruktur.....	26
Tabel 4.2 Skenario Pengujian Fitur dan Kontrol Akses (RBAC).....	45
Tabel 4.3 Skenario Pengujian Keamanan dan Integritas Data.....	47
Tabel 4.4 Skenario Pengujian Resiliensi Offline-First PWA.....	48
Tabel 4.5 Hasil Pengujian Fitur dan Keamanan Sistem.....	49
Tabel 4.6 Hasil Pengujian Keamanan dan Integritas Data.....	51
Tabel 4.7 Hasil Pengujian Latensi Komputasi AES-256-GCM Sisi Klien.....	52
Tabel 4.8 Hasil Pengujian Resiliensi Offline-First PWA pada Kondisi Jaringan Fluktuatif.....	53
Tabel 4.9 Hasil Pengujian Beban dan Kestabilan Server Backend (Simulasi 30 VUs).....	54





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Penanganan *stunting* merupakan prioritas nasional di Indonesia yang menuntut ketersediaan ekosistem data kesehatan yang akurat, konsisten, dan memiliki integritas tinggi. Sebagai unit layanan kesehatan primer, Posyandu memegang peran strategis dalam akuisisi data antropometri balita. Namun, metode konvensional yang mengandalkan pencatatan manual sering kali menghadapi kendala validitas data, redundansi pencatatan, serta latensi waktu antara pengambilan data di lapangan dan pelaporan ke tingkat pusat. Ketidakefisienan ini menghambat intervensi gizi yang tepat sasaran, sehingga mendorong urgensi transformasi digital pada manajemen data Posyandu.

Upaya digitalisasi di tingkat dasar telah dirintis melalui berbagai penelitian terapan. Yulianti et al. (2025) mengembangkan sistem presensi berbasis QR Code di Posyandu Orchid, Depok, yang terbukti efektif meningkatkan efisiensi operasional dan literasi digital kader. Senada dengan itu, Mulyana et al. (2022) melakukan digitalisasi pelayanan administratif Posyandu berbasis *website* yang berhasil merapikan database balita. Namun, evaluasi terhadap sistem-sistem tersebut menunjukkan pola yang sama: fokus pengembangan masih terpaku pada fungsionalitas pencatatan dasar (*functional-centric*). Tim Penulis JEKIN (2025) juga mencatat bahwa meskipun sistem informasi Posyandu digital mampu berjalan secara fungsional, aspek keamanan data medis sering kali terabaikan dan belum memenuhi standar perlindungan privasi.

Kelemahan mendasar pada implementasi sistem digital Posyandu lokal terletak pada penggunaan arsitektur keamanan perimeter tradisional. Baik pada sistem yang dikembangkan oleh Yulianti et al. (2025) maupun Mulyana et al. (2022), mekanisme autentikasi masih bersifat statis dan transmisi data belum menerapkan enkripsi *end-to-end*. Akibatnya, data medis sensitif seperti Nomor Induk Kependudukan (NIK) dan status gizi balita berpotensi tersimpan dan ditransmisikan dalam bentuk *plaintext*. Risiko tersebut menjadi semakin besar



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

karena operasional Posyandu sering memanfaatkan jaringan publik atau koneksi internet yang tingkat keamanannya tidak selalu terjamin. Kondisi ini dapat membuka peluang terjadinya serangan *Man-in-the-Middle* (MitM) maupun akses tidak sah oleh pengguna internal (*insider threat*) akibat pengelolaan hak akses yang kurang ketat.

Di sisi lain, lanskap keamanan siber kesehatan global telah mengalami pergeseran paradigma dari model "percaya namun verifikasi" (*trust but verify*) menjadi *Zero Trust Network Access* (ZTNA). Literatur internasional terkini, seperti studi oleh Son et al. (2024), menegaskan bahwa model keamanan tradisional tidak lagi memadai untuk melindungi ekosistem *Internet of Things* (IoT) medis. Hal ini diperkuat oleh Wan et al. (2025) yang menyatakan bahwa dalam lingkungan IoT, otentikasi tidak boleh berhenti di halaman login, melainkan harus dilakukan secara berkelanjutan (*continuous verification*) pada setiap pertukaran data perangkat. Lebih lanjut, Khan et al. (2025) melalui kajian literatur yang dilakukannya menjelaskan bahwa standar global saat ini merekomendasikan penggunaan *lightweight cryptography* seperti Advanced Encryption Standard - Galois/Counter Mode (AES-GCM) untuk menjaga kerahasiaan (*confidentiality*) dan integritas (*integrity*) data pada perangkat dengan sumber daya terbatas. Perbedaan antara penerapan standar keamanan global tersebut dengan kondisi implementasi lokal menunjukkan adanya risiko terhadap keamanan data antropometri balita, baik berupa kebocoran maupun manipulasi data.

Selain aspek keamanan, tantangan operasional di lapangan menuntut sistem yang memiliki resiliensi terhadap ketidakstabilan infrastruktur. Fenomena *network jitter* dan konektivitas *intermittent* (putus-nyambung) sering kali menghambat proses input data massal. Meskipun studi seperti Sachdeva et al. (2025) telah mengembangkan aplikasi mobile *native* untuk memastikan ketersediaan data secara *offline*, pendekatan instalasi aplikasi *native* membebani memori perangkat kader. Di sisi lain, prinsip *Delay-Tolerant Network* (DTN) yang menjamin ketiadaan data yang hilang (*zero data loss*) pada sistem sensor terdistribusi sangat esensial untuk diadaptasi (Mohseni-Ejiyeh et al., 2023). Oleh karena itu, penelitian ini mengadopsi prinsip *delay-tolerant* melalui teknologi *Progressive*



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Web Apps (PWA) yang lebih ringan, tidak memerlukan instalasi aplikasi secara khusus, serta mampu mendukung operasional lintas platform pada kondisi jaringan yang tidak stabil.

Guna menjembatani kesenjangan antara implementasi digital Posyandu lokal dengan tuntutan standar keamanan dan resiliensi global, penelitian ini mengusulkan pengembangan arsitektur sistem pemantauan gizi yang memiliki pertahanan mendalam (*defense-in-depth*). Penelitian ini dirancang untuk mengisi celah teknologi tersebut dengan mengembangkan sebuah *Platform Monitoring Status Gizi Balita Berbasis IoT* yang mengintegrasikan aspek keamanan siber dan ketahanan operasional dalam satu ekosistem terpadu di Posyandu Orchid, Kota Depok. Sistem yang diusulkan dirancang dengan menerapkan mekanisme *fail-safe* melalui pendekatan *hybrid input* dan diperkuat dengan kapabilitas PWA, arsitektur *Zero Trust*, serta enkripsi sisi klien (*client-side encryption*) berbasis AES-GCM sebagai perlindungan privasi standar medis global.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka perumusan masalah dalam penelitian ini didefinisikan sebagai berikut:

1. Bagaimana merancang mekanisme *Zero Trust Access Control* dengan verifikasi kontinyu pada platform monitoring Posyandu untuk memitigasi risiko eskalasi hak akses dan manipulasi data oleh pihak internal?
2. Bagaimana mengimplementasikan standar enkripsi *AES-GCM* pada alur data *hybrid* (input manual dan IoT) untuk menjamin kerahasiaan dan integritas data medis di database tanpa membebani kinerja perangkat kader?
3. Seberapa besar efektivitas penerapan *Progressive Web App* (PWA) dengan mekanisme sinkronisasi *delay-tolerant* dalam mempertahankan ketersediaan layanan (*availability*) dan pengalaman pengguna nirlatensi saat terjadi fluktuasi jaringan?



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.3 Batasan Masalah

Adapun batasan masalah pada penelitian ini:

1. Sistem keamanan yang dibangun dibatasi pada pengembangan *middleware* otentikasi dan otorisasi berbasis *Zero Trust* pada sisi aplikasi web dan API, dengan asumsi bahwa infrastruktur fisik jaringan telah tersedia.
2. Implementasi kriptografi pada penelitian ini difokuskan pada penggunaan algoritma AES-256-GCM di tingkat aplikasi (*Application Layer*) untuk mengamankan data antropometri balita berupa berat badan (BB) dan tinggi badan (TB) yang dikirimkan ke server, bukan untuk mengamankan seluruh komunikasi perangkat keras IoT.
3. Pengujian efektivitas sistem (resiliensi PWA) difokuskan pada pengukuran latensi interaksi pengguna (*Zero Latency UX*) dan integritas data saat kondisi jaringan *intermittent*, dengan simulasi data input yang berasal dari antarmuka manual maupun data tiruan (*dummy data*).

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

1. Merancang mekanisme *Zero Trust Access Control* yang menerapkan verifikasi kontinyu pada setiap permintaan akses data di platform monitoring, sehingga dapat mencegah akses ilegal secara efektif.
2. Mengimplementasikan standar enkripsi AES-GCM pada sisi klien dan *backend* untuk menjamin kerahasiaan serta integritas data medis yang tersimpan di *database*, sekaligus menjaga performa aplikasi tetap ringan.
3. Mengukur efektivitas penerapan *Progressive Web App* (PWA) dalam menjaga ketersediaan layanan dan meminimalkan waktu tunggu (*latency*) kadeer saat melakukan input data di kondisi jaringan yang tidak stabil.

1.4.2 Manfaat

Adapun manfaat yang akan dicapai dari penelitian ini adalah:



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1. Meminimalkan risiko manipulasi data dan penyalahgunaan hak akses oleh pihak internal maupun eksternal melalui penerapan verifikasi ketat yang tidak mempercayai sesi pengguna secara implisit.
2. Menjamin privasi data antropometri balita dari risiko kebocoran (*data breach*) atau manipulasi, karena data tersimpan dalam format terenkripsi yang hanya dapat dibuka oleh pihak berwenang.
3. Menghilangkan hambatan teknis berupa *loading* lama atau kegagalan simpan data akibat gangguan sinyal, sehingga kader dapat bekerja secara efisien dan responsif dalam melayani antrean balita yang padat.

1.5 Sistematika Penulisan

Berikut adalah sistematika penulisan yang diterapkan dalam proses penyusunan laporan dari penelitian ini:

1. BAB I PENDAHULUAN

Membahas latar belakang masalah urgensi keamanan data dan resiliensi sistem Posyandu, perumusan dan batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan laporan.

2. BAB II TINJAUAN PUSTAKA

Menguraikan landasan teori mengenai Digitalisasi Posyandu, konsep *Zero Trust Network Access* (ZTNA), standar kriptografi ringan *Advanced Encryption Standard - Galois/Counter Mode* (AES-GCM), teknologi *Progressive Web Apps* (PWA), serta analisis celah penelitian terdahulu.

3. BAB III METODE PENELITIAN

Menjelaskan metode pengembangan sistem, mencakup perancangan arsitektur keamanan *Zero Trust*, desain alur enkripsi *Client-Side* dan skema sinkronisasi IndexedDB, serta skenario pengujian untuk validasi keamanan dan pengukuran resiliensi jaringan.

4. BAB IV HASIL DAN PEMBAHASAN



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Menyajikan hasil implementasi *middleware Zero Trust*, modul enkripsi AES-GCM, dan antarmuka PWA, diikuti analisis pengujian kerahasiaan data, integritas, serta pengukuran latensi input pada kondisi jaringan stabil maupun intermiten.

5. BAB V PENUTUP

Berisi kesimpulan dari hasil penelitian berdasarkan tujuan yang telah ditetapkan dan saran untuk pengembangan sistem di masa mendatang.





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB V PENUTUP

5.1 Kesimpulan

Rancang bangun *Platform Monitoring* Status Gizi Balita Berbasis IoT yang mengintegrasikan arsitektur *Zero Trust*, enkripsi sisi klien AES 256 GCM, dan *Progressive Web App* berbasis PWA berhasil menjawab tiga rumusan masalah penelitian. Mekanisme *Zero Trust Access Control* yang dirancang menggabungkan validasi *token JWT* berbasis *risk based authentication* dengan batas masa berlaku atau TTL selama lima jam serta *Role Based Access Control* atau RBAC. Hasil pengujian menunjukkan bahwa sistem mampu menahan seluruh upaya eskalasi hak akses lintas peran dan menolak seratus persen permintaan yang menggunakan *token* tidak valid atau sudah kedaluwarsa. Hal ini menegaskan bahwa prinsip tidak adanya kepercayaan implisit berhasil diterapkan pada setiap permintaan akses data.

Pada aspek kriptografi, implementasi AES 256 GCM melalui *Web Crypto API* berhasil menjaga kerahasiaan dan integritas data antropometri balita pada jalur input manual oleh kader. Latensi komputasi enkripsi tergolong sangat rendah, dengan rata rata sebesar 0,097 milidetik untuk payload 1 KB hingga 35,717 milidetik untuk payload 1 MB. Seluruh nilai tersebut berada jauh di bawah ambang batas nirlatensi sebesar 100 milidetik. Hasil pengujian *negative testing* juga membuktikan bahwa setiap bentuk manipulasi sekecil apa pun pada data terenkripsi dapat terdeteksi melalui ketidaksesuaian *authentication tag*, sehingga sistem menolak seluruh permintaan yang terindikasi mengalami perubahan tidak sah. Validasi keamanan pada penelitian ini difokuskan pada jalur input manual sesuai batasan masalah yang telah ditetapkan, sedangkan pengujian *end to end* pada jalur transmisi data telemetri perangkat IoT belum dilakukan dan menjadi ruang pengembangan lanjutan.

Untuk menjawab kebutuhan resiliensi jaringan, arsitektur *offline first* berbasis PWA yang dikembangkan memanfaatkan *service worker*, IndexedDB, dan *Background Sync API* untuk menjalankan mekanisme sinkronisasi *delay tolerant*. Pengujian pada tiga skenario konektivitas, yaitu kondisi daring stabil, luring



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

penuh, dan transisi dari luring ke daring, menghasilkan tingkat keberhasilan sebesar seratus persen dari lima puluh percobaan pada setiap kondisi. Hasil ini membuktikan bahwa tidak terdapat data yang hilang akibat gangguan jaringan. Pada pengujian beban menggunakan simulasi 30 *virtual users* secara bersamaan, *server backend* berhasil memproses 273 transaksi dalam 40 detik dengan *throughput* 6,12 *request* per detik dan tingkat kegagalan nol persen. Meskipun demikian, waktu respons rata-rata meningkat menjadi 3,64 detik pada kondisi beban puncak tersebut, yang merepresentasikan skenario ekstrem berupa sinkronisasi massal setelah pemulihan jaringan, bukan pola akses harian Posyandu yang umumnya terjadi secara bertahap.

5.2 Saran

Meskipun sistem telah berhasil diimplementasikan sesuai dengan tujuan penelitian, masih terdapat ruang untuk penyempurnaan di masa mendatang. Beberapa saran yang dapat dipertimbangkan untuk penelitian dan pengembangan selanjutnya adalah sebagai berikut:

1. Menambahkan fitur *Web Push Notification* untuk memberikan notifikasi secara real-time kepada kader mengenai status sinkronisasi data, pengingat jadwal kegiatan Posyandu, maupun informasi penting lainnya yang berkaitan dengan pelayanan kesehatan.
2. Melakukan pengujian pada skala implementasi yang lebih luas dengan melibatkan beberapa Posyandu atau fasilitas kesehatan lainnya untuk mengevaluasi performa sistem pada jumlah pengguna dan volume data yang lebih besar.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR PUSTAKA

- Al-Hammuri, K., Gebali, F., Kanan, A., Mamun, M. and Hazratifard, S.M. (2024). Zero Trust Context-Aware Access Control Framework for IoT Devices in Healthcare Cloud AI Ecosystem. *arXiv preprint*.
- Baig, M.H.M., Ul Haq, H.B. and Habib, W. (2024). A Comparative Analysis of AES, RSA, and 3DES Encryption Standards based on Speed and Performance. *Management Science Advances*, 1(1), pp.20–30. doi:<https://doi.org/10.31181/msa1120244>.
- Buljić, I., Kadušić, E., Živić, N. and Marevac, E. (2025). Evaluating Legacy and Modern Cryptography on the Web: RSA, Hybrid AES and Ed25519 in Wasm and JavaScript. *Journal of Communications*, 20(6), pp.681–693. doi:<https://doi.org/10.12720/jcm.20.6.681-693>.
- Chrome for Developers (2025). Richer Offline Experiences with the Background Sync API. [online] Google. Available at: <https://developer.chrome.com/docs/capabilities> [Accessed 23 Jun. 2026].
- Dalimunthe, S., Putra, E.H. and Muhammad (2023). Restful API Security Using JSON Web Token (JWT) With HMAC-Sha512 Algorithm in Session Management. *IT Journal Research and Development*, 8(1), pp.81–94. doi:<https://doi.org/10.25299/itjrd.2023.12029>.
- Edo, O.C., Ang, D., Billakota, P. and Ho, J.C. (2024). A Zero Trust Architecture for Health Information Systems. *Health and Technology*, 14(1), pp.189–199. doi:<https://doi.org/10.1007/s12553-023-00809-4>.
- ElSayed, Z., Elsayed, N. and Bay, S. (2024). A Novel Zero-Trust Machine Learning Green Architecture for Healthcare IoT Cybersecurity: Review, Analysis, and Implementation. [online] *arXiv.org*. Available at: <https://arxiv.org/html/2401.07368v1> [Accessed 23 Jun. 2026].
- Khan, S., Ferreira Lopes Martins, P.A., Sousa, B. and Pereira, V. (2025). A Comprehensive Review on Lightweight Cryptographic Mechanisms for Industrial Internet of Things Systems. *ACM Computing Surveys*, 58(1), pp.1–37. doi:<https://doi.org/10.1145/3757734>.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Kim, K., Choi, S., Kwon, H., Kim, H., Liu, Z. and Seo, H. (2020). PAGE — Practical AES-GCM Encryption for Low-End Microcontrollers. *Applied Sciences*, 10(9), 3131.

Kokila, M. and Reddy, K.S. (2025). Authentication, Access Control and Scalability Models in Internet of Things Security – A Review. *Cyber Security and Applications*, 3, 100057. doi:<https://doi.org/10.1016/j.csa.2025.100057>.

Mario, B., Wiradinata, T. and Christian, C. (2025). Enhancing Web Security and Performance with Hybrid Stateless Authentication. *Journal of Applied Informatics and Computing*, 9(3), pp.611–616. doi:<https://doi.org/10.30871/jaic.v9i3.9251>.

National Institute of Standards and Technology (2007). *NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*.

MDN Web Docs (2025). Offline and Background Operation - Progressive Web Apps. [online] Mozilla. Available at: https://developer.mozilla.org/en-US/docs/Web/Progressive_web_apps/Guides/Offline_and_background_operation [Accessed 23 Jun. 2026].

Mulyana, T., Nopendri, N., Putra, S.A., Kusumasari, T.I.F., Fakhurroja, H., Setyorini, S., Adytia, D., Soekarnen, W. and Destian, D. (2022). Digitalisasi Pelayanan Posyandu Melalui Sistem Informasi Posyandu Berbasis Website di Posyandu Anyelir RW 09 Kelurahan Burangrang Kecamatan Lengkong Kota Bandung. *Charity*, 5(1), p.37. doi:<https://doi.org/10.25124/charity.v5i1.3632>.

Myers, G.J., Sandler, C. and Badgett, T. (2011). *The Art of Software Testing*. 3rd ed. Hoboken, NJ: John Wiley & Sons.

Nielsen, J. (1993). *Usability Engineering*. San Francisco: Morgan Kaufmann.

Nouma, S.E., Mumcu, G. and Yavuz, A.A. (2025). *Diamond: Design and Implementation of Breach-Resilient Authenticated Encryption Framework For Internet of Things*. University of South Florida.

OWASP (2021). OWASP Web Security Testing Guide v4.2. [online] Available at: <https://owasp.org/www-project-web-security-testing-guide/> [Accessed 23 Jun. 2026].



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pressman, R.S. (2010). *Software Engineering: A Practitioner's Approach*. 7th ed. New York: McGraw-Hill.

Rana, M., Pandey, A., Mishra, A. and Kandu, V. (2023). Enhancing Data Security: A Comprehensive Study on the Efficacy of JSON Web Token (JWT) and HMAC SHA-256 Algorithm for Web Application Security. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(9), pp.4409–4416. doi:<https://doi.org/10.17762/ijritcc.v11i9.9930>.

Sachdeva, S., Bhalla, S., Juyal, N. and Kumar, A. (2025). MedEForm: Medical Data Mobile App. *Frontiers in Artificial Intelligence and Applications*, 411. doi:<https://doi.org/10.3233/faia250551>.

Son, S., Kwon, D., Lee, S., Kwon, H. and Park, Y. (2024). A Zero-Trust Authentication Scheme With Access Control for 6G-Enabled IoT Environments. *IEEE Access*, 12, pp.154066–154079. doi:<https://doi.org/10.1109/access.2024.3484522>.

Tripathi, A. (2025). Evaluating the Role of Confidentiality, Integrity, and Availability in Cyber Defence. *IJIRMPs - International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences*, 13(4). Available at: <https://www.ijirmps.org/research-paper.php?id=232662> [Accessed 23 Jun. 2026].

Triwiyanto, T., Luthfiyah, S., Hamzah, T., Utomo, B., Lamidi, L., Setyobudi, S.I., Julianto, J. and Rosari, A.E.S. (2023). Implementation of Digital Anthropometry for Real Time Toddlers Nutrition Status at Balongdowo Village Posyandu. *Indonesian Journal of Electronics, Electromedical Engineering and Medical Informatics*, 5(4), pp.193–200. doi:<https://doi.org/10.35882/ijeeemi.v5i4.185>.

Vidaković, A., Petrović, T., Kresoja, P. and Veinović, M. (2024). Impact of Database Encryption on Web Application Performance. *International Scientific Conference on Information Technology, Computer Science, and Data Science*, pp.82–87. doi:<https://doi.org/10.15308/sinteza-2024-82-87>.

Wan, T., Shi, B. and Wang, H. (2025). A Continuous Authentication Scheme for Zero-Trust Architecture in Industrial Internet of Things. *Alexandria Engineering Journal*, 122, pp.555–563. doi:<https://doi.org/10.1016/j.aej.2025.03.012>.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Yulianti, S.D., Hermawan, I., Iswara, R.W., Miharja, M.E. and Rauf, F. (2025). Penerapan Teknologi QR Code dan Aplikasi Mobile Sederhana untuk Digitalisasi Kehadiran serta Deteksi Dini Status Gizi Balita di Posyandu. Jurnal Pepadu, 6(3), pp.361–371. doi:<https://doi.org/10.29303/wb1n4s44>.





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR RIWAYAT HIDUP



Salsabilla Aulia merupakan anak kedua dari tiga bersaudara yang lahir di Jakarta pada tahun 2004. Penulis menempuh pendidikan di SMA Negeri 105 Jakarta jurusan IPA dan berhasil menyelesaikan pendidikan pada tahun 2022. Saat ini, berkesempatan untuk menempuh pendidikan pada Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta (PNJ).





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LAMPIRAN

Lampiran 1: Hasil Pengujian Fitur dan Kontrol Akses

a. Tangkapan Layar Pemrosesan Data Formulir (FT01)

The screenshot shows a web form for data processing. At the top, there are two tabs: 'IoT (Otomatis)' and 'Manual'. Below the tabs, there is a message 'Pilih IoT untuk menggunakan alat pengukur otomatis'. The form contains several input fields: 'Tanggal Pencatatan' (07 Jul), 'Berat Badan (kg)' (20), 'Tinggi Badan (cm)' (56), 'Lingkar Kepala', 'Cara Ukur' (Telentang), and 'Jenis Imunisasi'. At the bottom, there are two buttons: 'Simpan' (Save) and 'Batal' (Cancel). A modal dialog box is displayed in the center, showing a green checkmark and the text 'insert success' with an 'OK' button.

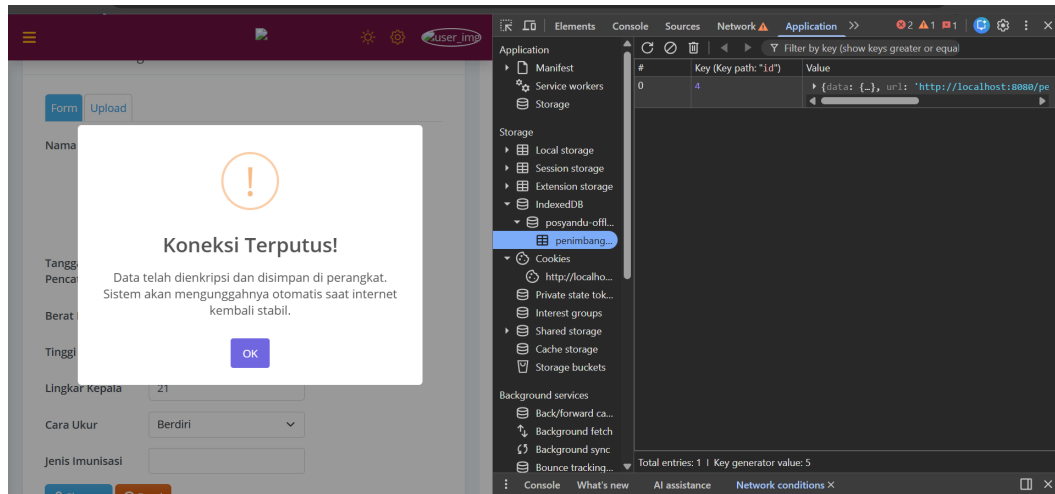
a. Tangkapan Layar Pembatasan Akses Tanpa Autentikasi (FT03)

The screenshot shows the login page for 'Posyandu Orchid'. The page has a dark blue background with a pink orchid logo. The login form is centered and contains fields for 'Username' and 'Password', a red 'Submit' button, and links for 'Panduan kader', 'Panduan Orang Tua', and 'Aplikasi Android'. The footer text reads '© 2026 Posyandu Orchid Green Park'.

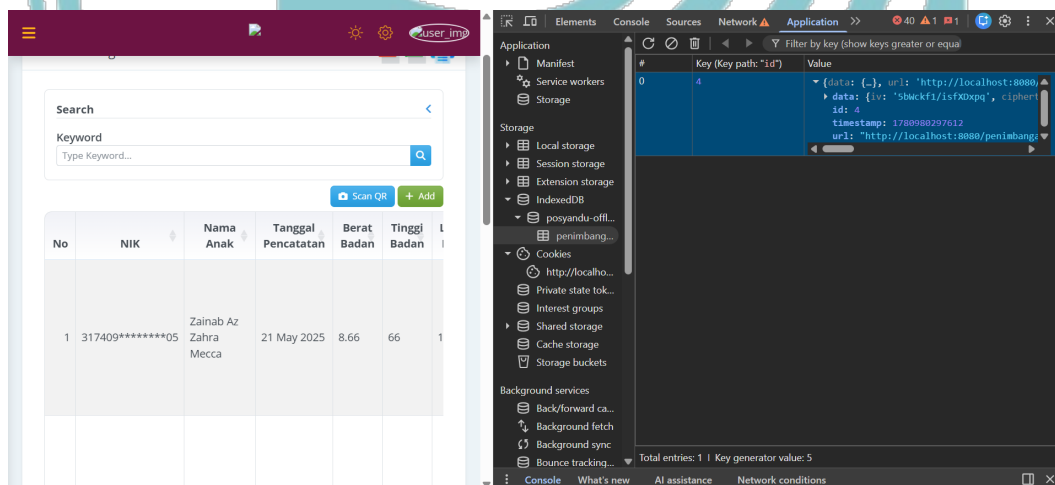


b. Tangkapan Layar Penyimpanan Data Saat Offline

Notifikasi Pengalihan Penyimpanan ke Mode Luring



Hasil Penyimpanan di IndexedDB





Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 2: Hasil Pengujian Keamanan dan Integritas Data

a. Tangkapan Layar Kerahasiaan Data dalam Transmisi (ST01)

```

Wireshark · Follow TCP Stream (tcp.stream eq 156) · Adapter for loopback traffic capture

Cookie: jwd_adm_token=app_token; jwd_adm_mobile=0; app_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlbnV4MTc0MTA5NDZMcWiaWRRfdXN1ciI6IjM3MyJ9.1DVCVqLHglz-mG7y_JW_sxBjZhdTlD0CbK-1kyaBw-A; jwd_access_token_expire=1781094130; app_token_refresh=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlbnV4MTc0MTA5NDZMcWiaWRRfdXN1ciI6IjM3MyJ9.1DVCVqLHglz-mG7y_JW_sxBjZhdTlD0CbK-1kyaBw-A; jwd_refresh_token_expire=1789024930; ci_session=240q19tm15toe7ltm1bq2mprupcopdoj; csrf_app_token=7ab05363f87d847d644b5840d78e92a92d0fa4759bcadb4d796f3718a9caa6ec

iv=JGkf5YkA4Yo%2Bjlm5&ciphertext=nk7iWYreZM2eNwHpwCsQnm1ZmQ%2BbTYXcaRwtKiKeXPVK6j%2FKQTwrB%2BXR%2Bp89k2jKQn3bwua3KKtaCbnZUq%2FAQpBo7qpgp8%2F4L8yPbwJeIE3y10DsurHF5CHHqxxhPD1QrLTeHak%2B5snIMGY2t%2B8ndogpatfkSLFxj5zuBtIU1%2Bsv94H8tag=zY9q1%2BgW06Vx76akcRXQ%3D%3D&csrf_app_token=9e62e1fd3713e0d3196d29182ad0529e82d8c0509c3ab0e6e30cbf4c6371eecf

HTTP/1.1 200 OK
Host: localhost:8080
Date: Wed, 10 Jun 2026 09:00:47 GMT
Connection: close
X-Powered-By: PHP/8.2.12
Set-Cookie: csrf_app_token=deleted; expires=Thu, 01 Jan 1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: csrf_app_token=d595b100394e7044ad081ecc4817779bb36bc0e5943070145f1bb924a0464787; expires=Wed, 10 Jun 2026 11:00:46 GMT; Max-Age=7200; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type: application/json; charset=utf-8

{"message": "insert success", "id": 428, "status": "ok", "token": "d595b100394e7044ad081ecc4817779bb36bc0e5943070145f1bb924a0464787"}

2 client pkts, 2 server pkts, 1 turn.
Entire conversation (2388 bytes) Show as ASCII No delta times Stream 156
Find: Case sensitive Find Next
Filter Out This Stream Print Save as... Back Close Help
  
```

b. Tangkapan Layar Integritas Data (ST02)

```

Params Headers Body
none form-data x-www-form-urlencoded raw binary GraphQL JSON Beautify

1 {
2   "iv": "PWa6YbDn9Zhs/4ZI",
3   "ciphertext": "L6B881eSI93Sr6AGf34z0krvbkIB4eDkdEkdQiM4DeN3inSbR15FmE1sE0zcpuNu8privXR/Tm4Lb/DWkRcV7FP+D/BVmsgQfjq0TFavhWNYRIz1qctLmTotB0uYzJ1s=",
4   "tag": "e8TFdB9/7BHrCy1myjactx==" //ubah beberapa huruf
5 }

Body Headers 10 Status Code 401 Unauthorized
Raw Preview
1 {
2   "status": 401,
3   "error": 401,
4   "messages": {
5     "error": "Integritas data rusak! Pengiriman ditolak."
6   }
7 }
  
```



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

c. Tangkapan Layar Perlindungan Data Sensitif atau Data Masking (ST04)

No	NIK	Nama Anak	Tanggal Pencatatan	Berat Badan	Tinggi Badan	Lingkar Kepala	Cara Ukur	Jenis Imunisasi
1	317305*****01	ijaa	10 Jun 2026	10	88	16	Berdiri	
2	317305*****01	ijaa	10 Jun 2026	15	98	17	Berdiri	
3	317305*****01	ijaa	10 Jun 2026	20	112	18	Berdiri	

d. Tangkapan Layar Validasi Autentikasi dan Validasi Masa Berlaku Token (ST05 & ST06)

☐ none
 ☐ form-data
 ☐ x-www-form-urlencoded
 ☒ raw
 ☐ binary
 ☐ GraphQL
 JSON
 ☐ Schema
 Beautify

```

1 {
2   "iv": "PWa6YbDn9Zhs/4ZI",
3   "ciphertext": "L6B881eSI93Si6AGf34z0kivbkIB4eDkdEkdQiM4DeN3inSbR15FmE1sE0zcpuNu8pivXR/Tm4Lb/
4   "tag": "e8TFdB9/7BHrCy1myjactx==" //ubah beberapa huruf
5 }
  
```

Body **401 Unauthorized** • 325 ms • 686 B • Save Response ...

☒ JSON
 ☐ Preview
 ☐ Pass the correct auth credentials

```

1 {
2   "status": "error",
3   "message": "Akses ditolak (token tidak ditemukan)",
4   "error_type": "need_login",
5   "status_code": 401
6 }
  
```



Lampiran 3: Hasil Pengujian Resiliensi Offline-First PWA

Rincian Data Mentah Hasil Pengukuran Latensi Kriptografi AES-256-GCM Sisi Klien (30 Iterasi)

Iterasi	Latensi 1 KB (ms)	Latensi 10 KB (ms)	Latensi 100 KB (ms)	Latensi 1 MB (ms)
1	4,000	2,000	67,000	496,000
2	6,000	4,000	20,000	328,000
3	2,000	1,000	11,000	469,000
4	3,000	3,000	23,000	133,000
5	3,000	3,000	26,000	222,000
6	3,000	1,000	8,000	157,000
7	5,000	1,000	15,000	219,000
8	3,000	1,000	9,000	158,000
9	2,000	2,000	11,000	195,000
10	3,000	1,000	8,000	141,000
11	3,000	3,000	25,000	233,000
12	2,000	0	11,000	168,000
13	2,000	2,000	10,000	255,000
14	3,000	1,000	20,000	179,000
15	4,000	1,000	14,000	229,000
16	3,000	1,000	10,000	157,000
17	3,000	3,000	11,000	267,000
18	13,000	4,000	13,000	170,000
19	3,000	1,000	26,000	215,000
20	3,000	1,000	7,000	160,000

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Iterasi	Latensi 1 KB (ms)	Latensi 10 KB (ms)	Latensi 100 KB (ms)	Latensi 1 MB (ms)
21	2,000	2,000	10,000	203,000
22	3,000	1,000	13,000	202,000
23	3,000	1,000	9,000	304,000
24	2,000	1,000	9,000	133,000
25	2,000	1,000	13,000	240,000
26	4,000	0	10,000	148,000
27	2,000	1,000	10,000	220,000
28	3,000	1,000	10,000	159,000
29	2,000	1,000	10,000	245,000
30	3,000	2,000	13,000	130,000

POLITEKNIK
NEGERI
JAKARTA



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 4: Hasil Pengujian K6 Beban dan Skalabilitas Server Backend

```
D:\Semester 8>k6 run load_test.js

Grafana
K6

execution: local
script: load_test.js
output: -

scenarios: (100.00%) 1 scenario, 30 max VUs, 1m10s max duration (incl. graceful stop):
  * default: 30 looping VUs for 40s (gracefulStop: 30s)

THRESHOLDS

http_req_duration
X 'p(95)<500' p(95)=3.93s

http_req_failed
✓ 'rate==0' rate=0.00%

TOTAL RESULTS

checks_total.....: 273      6.122133/s
checks_succeeded...: 100.00% 273 out of 273
checks_failed.....: 0.00%   0 out of 273

✓ Transaksi Sukses

HTTP
http_req_duration.....: avg=3.64s min=214.6ms med=3.76s max=5.03s p(90)=3.89s p(95)=3.93s
{ expected_response:true }...: avg=3.64s min=214.6ms med=3.76s max=5.03s p(90)=3.89s p(95)=3.93s
http_req_failed.....: 0.00% 0 out of 273
http_reqs.....: 273      6.122133/s

EXECUTION
iteration_duration.....: avg=4.64s min=1.21s med=4.76s max=6.03s p(90)=4.89s p(95)=4.93s
iterations.....: 273      6.122133/s
vus.....: 4      min=4      max=30
vus_max.....: 30      min=30      max=30

NETWORK
data_received.....: 172 kB 3.9 kB/s
data_sent.....: 159 kB 3.6 kB/s

running (0m44.6s), 00/30 VUs, 273 complete and 0 interrupted iterations
default ✓ [=====] 30 VUs 40s
ERRO[0044] thresholds on metrics 'http_req_duration' have been crossed
```