UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR ISI

HALAMAN JUDUL ii

HALAMAN PENGESAHAN iii

PERNYATAAN BEBAS PLAGIASI iv

KATA PENGANTAR v

DAFTAR ISI vii

DAFTAR GAMBAR xi

DAFTAR TABEL xii

DAFTAR KODE xiii

INTISARI xiv

ABSTRACT xvi

I PENDAHULUAN 1

1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Tujuan Penelitian 4
1.4 Batasan Penelitian 4
1.5 Manfaat Penelitian 5

II TINJAUAN PUSTAKA 7

2.1 HL7 FHIR dalam Interoperabilitas Rekam Medis 9
2.2 Penerapan AES-GCM untuk Keamanan Data Kesehatan 10
2.3 Penerapan ECC dan Skema Hibrida pada Data Kesehatan 11
2.4 Rekam Medis Elektronik 12
2.5 Keamanan Informasi pada Data Kesehatan 14
2.6 Kriptografi 16
2.7 Advanced Encryption Standard (AES) 17
2.8 AES-GCM 18
2.9 ChaCha20-Poly1305 19
2.10 Elliptic Curve Cryptography (ECC) 20
2.11 HL7 FHIR 22
2.12 Rekam Medis Elektronik Berbasis HL7 FHIR 24
2.13 Pendekatan SATUSEHAT sebagai Baseline Konseptual Lokal . . . 24
2.14 Skema Hibrida AEAD dan ECC pada RME 25

UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

III METODOLOGI PENELITIAN **27**
3.1 Rancangan Penelitian 27
3.2 Pendekatan dan Batas Evaluasi 27
3.3 Objek dan Sumber Data 28
3.3.1 Struktur *Payload* 28
3.3.2 Kategori dan Provenans *Dataset* 29
3.4 Teknik Pengumpulan Data 29
3.5 Tahapan Penelitian 30
3.5.1 Perencanaan dan Perancangan 30
3.5.2 Implementasi dan Validasi 30
3.5.3 Pengujian, Penyimpanan Bukti, dan Analisis 31
3.6 Rancangan Arsitektur dan Mekanisme Keamanan 31
3.6.1 *Baseline* Konseptual Lokal SATUSEHAT 31
3.6.2 *Pipeline* AES-GCM dan ChaCha20-Poly1305 32
3.6.3 Autentikasi, Siklus Hidup Kunci, dan Konteks HKDF 32
3.6.4 Struktur Paket dan Jalur Penolakan 33
3.6.5 Model Matematis dan Derivasi Kunci 33
3.7 Rancangan Pengujian 34
3.7.1 Pengujian Fungsional dan Kesesuaian Data 34
3.7.2 Pengujian Integritas 34
3.7.3 Pengujian Kinerja dan Batas Timer 35
3.7.4 Desain Iterasi dan Lingkungan Uji 35
3.8 Metrik Evaluasi 36
3.9 Teknik Analisis Data dan Reproduksibilitas 37

IV IMPLEMENTASI **39**
4.1 Lingkungan dan Struktur Implementasi 39
4.1.1 Lingkungan Acuan Penelitian dan Status Provenans 39
4.1.2 Struktur Modul 40
4.2 Implementasi Data Uji Sintetis 41
4.2.1 Struktur dan Batas Validasi 41
4.2.2 Pembentukan Kategori KB dan MB 42
4.3 Implementasi *Baseline* Konseptual Lokal SATUSEHAT 43
4.3.1 Ruang Lingkup *Baseline* 43
4.3.2 Penyusunan dan Penerimaan Pesan Lokal 44
4.4 Implementasi Identitas, Pertukaran Kunci, dan Paket 45
4.4.1 Model Kepercayaan dan Siklus Kunci 45
4.4.2 Konteks HKDF dan AAD 46

UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

4.4.3 Struktur Paket dan Tanda Tangan Transkrip 46
4.5 Implementasi Dua *Pipeline* AEAD 48
4.5.1 AES-GCM 128-bit dengan ECC Terautentikasi 48
4.5.2 ChaCha20-Poly1305 dengan ECC Terautentikasi 48
4.5.3 Proses Penerimaan dan Klasifikasi Kegagalan 49
4.6 Implementasi Antarmuka Web 50
4.6.1 Pengelolaan *State* dan Pemilihan *Dataset* 50
4.6.2 Halaman *Node* A dan *Node* B 50
4.6.3 Halaman Uji Integritas dan *Benchmark* 51
4.7 Implementasi Modul Pengujian 52
4.7.1 Pengujian Fungsional dan Kesesuaian Data 52
4.7.2 Simulasi Modifikasi dan Kontrol Negatif 52
4.7.3 *Benchmark* Terkontrol dan Ekspor Artefak 54
4.8 Ringkasan Implementasi dan Batas Klaim 55

V HASIL DAN PEMBAHASAN 56
5.1 Sumber Data dan Rancangan Eksperimen 56
5.1.1 Lingkungan Acuan dan Provenans Hasil 56
5.1.2 *Dataset*, Pengulangan, dan Unit Analisis 57
5.2 Hasil Fungsional dan Kesesuaian Data 58
5.2.1 Keberhasilan *Pipeline* pada Seluruh *Dataset* 58
5.2.2 Batas Makna Keberhasilan Fungsional 58
5.3 Hasil Pengujian Integritas 59
5.3.1 Matriks Modifikasi yang Berlaku 59
5.3.2 Interpretasi Tahap Penolakan 59
5.4 Analisis Waktu Proses 60
5.4.1 Statistik Deskriptif Observasi Mentah 60
5.4.2 Rasio Waktu dan Larangan Klaim Kausal 61
5.5 *Overhead*, *Throughput*, dan Memori 62
5.5.1 *Overhead Payload* dan Pesan Aplikasi 62
5.5.2 *Throughput* dan Memori Puncak 64
5.6 Pembahasan dan Batas Interpretasi 64
5.6.1 *Trade-off* yang Didukung Data 64
5.6.2 Perbandingan dengan Penelitian Terdahulu 65
5.6.3 Implikasi bagi Integrasi RME 66
5.6.4 Keterbatasan Hasil 66

VI KESIMPULAN DAN SARAN 68

UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

6.1 Kesimpulan 68
6.2 Keterbatasan Penelitian 70
6.3 Saran 71

DAFTAR PUSTAKA **73**

UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR GAMBAR

3.1 Tahapan penelitian dan pengendalian artefak 30
3.2 Arsitektur pengamanan *Node* A-*Node* B dan *baseline* lokal 31
4.1 Struktur modul prototipe final dan keterhubungan komponen 41
4.2 Halaman *Node* A pada prototipe final 51
4.3 Halaman pemilihan skenario uji integritas pada prototipe final 51
5.1 Perbandingan *mean* waktu *pipeline* aplikasi pada skala logaritmik 61
5.2 Perbandingan *overhead* pesan aplikasi terhadap *payload* asli 63

UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR TABEL

2.1 Ringkasan perbandingan penelitian terdahulu 7
3.1 Ruang lingkup tiga pendekatan yang dievaluasi 27
3.2 Peran *resource* pada data uji sintetis 28
3.3 Kategori, komposisi, dan ukuran aktual data uji 29
3.4 Parameter kriptografi dua *pipeline* AEAD 32
3.5 Desain eksperimen dan lingkungan pengujian utama 35
3.6 Definisi operasional metrik evaluasi 36
4.1 Lingkungan acuan penelitian Apple/macOS 39
4.2 Pemetaan modul prototipe final 40
4.3 Kategori dan *byte dataset* aktual yang digunakan 42
4.4 Siklus hidup material kunci pada prototipe 45
4.5 Komponen paket *transport* AEAD 46
4.6 Prosedur dan kriteria pengujian fungsional 52
4.7 Matriks implementasi skenario modifikasi 53
4.8 Konfigurasi dan keluaran *benchmark* mode penuh penelitian 54
5.1 Lingkungan acuan dan status provenans artefak hasil 56
5.2 *Dataset* dan ukuran byte aktual 57
5.3 Hasil fungsional dan kesesuaian data pada 30 *payload* 58
5.4 Hasil pengujian integritas dan tahap penolakan 59
5.5 Statistik waktu *pipeline* per kategori dan pendekatan 60
5.6 Rasio *mean* waktu *pipeline* 61
5.7 *Overhead* ukuran *payload* dan pesan aplikasi 62
5.8 *Mean throughput* dan memori puncak 64

UNIVERSITAS
GADJAH MADA
Analisis Komparatif Keamanan Pertukaran Payload Rekam Medis Elektronik Berbasis HL7 FHIR pada Pendekatan SATUSEHAT, AES-GCM 128-Bit dengan ECC, dan CHACHA20-POLY1305
Febriano Ahdan Nadif, Dr. Nur Rokhman, S.Si., M.Kom.; Muhammad Oriza Nurfajri, S.Kom., M.IT.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR KODE

4.1 Inti penentuan ukuran dan pembentukan lampiran *binary* deterministik 42
4.2 Inti pembentukan *token dummy* lokal bertanda tangan HMAC-SHA-256 43
4.3 Penyusunan *header* dan *body* pada *baseline* aplikasi lokal 44
4.4 Pembentukan konteks kanonik untuk HKDF-SHA-256 46
4.5 Pembentukan dan penandatanganan paket transport 47
4.6 Enkripsi AES-GCM 128-bit dan pembungkusan *data key* 48
4.7 Enkripsi ChaCha20-Poly1305 dan pembungkusan *data key* 48
4.8 Klasifikasi kegagalan pada proses penerimaan paket 49
4.9 Modifikasi semantik JSON untuk kontrol negatif *baseline* 52
4.10 Pengendalian *warm-up*, identitas *run*, dan urutan pendekatan 54