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/

INTISARI

ANALISIS KOMPARATIF KEAMANAN PERTUKARAN PAYLOAD REKAM MEDIS ELEKTRONIK BERBASIS HL7 FHIR PADA PENDEKATAN SATUSEHAT, AES-GCM 128-BIT DENGAN ECC, DAN CHACHA20-POLY1305

oleh

FEBRIANO AHDAN NADIF
22/493642/PA/21206

Transformasi digital dalam sektor kesehatan meningkatkan efisiensi pengelolaan Rekam Medis Elektronik (RME), tetapi juga menimbulkan risiko terhadap kerahasiaan, integritas, dan autentisitas data pasien. Penelitian ini bertujuan merancang dan mengevaluasi prototipe pertukaran payload RME berstruktur HL7 FHIR antara Node A dan Node B dengan membandingkan baseline konseptual lokal alur aplikasi SATUSEHAT, AES-GCM 128-bit dengan ECC, dan ChaCha20-Poly1305.

Prototipe mengimplementasikan tiga pipeline aplikasi. Baseline konseptual lokal merepresentasikan pembentukan payload, token dummy, header, serialisasi, dan penerimaan pesan tanpa mekanisme autentikasi payload. Pipeline AES-GCM menggunakan kunci 128 bit, sedangkan ChaCha20-Poly1305 menggunakan kunci 256 bit dengan tag autentikasi 128 bit. Kedua pipeline AEAD menggunakan identitas ECDSA P-256, pertukaran kunci ECDH P-256, HKDF-SHA-256 yang terikat konteks sesi, AES Key Wrap, dan tanda tangan transkrip. Pengujian menggunakan 30 payload sintetis yang terdiri atas kategori kecil, sedang, besar, 1 MB, 5 MB, dan 10 MB dalam microbenchmark pipeline aplikasi lokal.

Hasil pengujian menunjukkan bahwa ketiga pendekatan mempertahankan kesesuaian data pada 30 dari 30 payload. Modifikasi body pada baseline tidak terdeteksi pada lima dari lima pengujian karena baseline tidak memiliki mekanisme autentikasi payload. Sebaliknya, AES-GCM dan ChaCha20-Poly1305 masing-masing menolak 25 dari 25 paket yang dimodifikasi pada komponen yang berlaku. Pengukuran waktu menghasilkan 2.700 observasi mentah, sedangkan memori puncak diukur melalui run terpisah menggunakan tracemalloc. Pada kategori 10 MB, rata-rata waktu proses baseline adalah 16,123 ms, AES-GCM 516,613 ms, dan ChaCha20-Poly1305 516,434 ms. Baseline mempunyai overhead payload sebesar 0%, sedangkan overhead pesan aplikasinya menurun seiring pertambahan ukuran payload. Pada kategori 10 MB, overhead paket AES-GCM dan ChaCha20-Poly1305 masing-masing sekitar 33,3445% dan 33,3444%.

Hasil tersebut menunjukkan bahwa kedua pipeline AEAD memberikan kemampuan autentikasi dan penolakan modifikasi yang tidak dimiliki baseline, dengan konsekuensi peningkatan waktu proses, ukuran pesan, dan penggunaan memori. Perbedaan kinerja mencerminkan keseluruhan pekerjaan pipeline aplikasi

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/

dan tidak digunakan untuk menyimpulkan keunggulan murni salah satu algoritma kriptografi. Pengujian dilakukan secara lokal tanpa jaringan nyata, handshake TLS, OAuth 2.0 produksi, atau endpoint SATUSEHAT sehingga hasilnya tidak merepresentasikan kinerja layanan SATUSEHAT produksi.

Kata Kunci: Rekam Medis Elektronik, HL7 FHIR, SATUSEHAT, AES-GCM, ECC, ChaCha20-Poly1305, Kriptografi Terautentikasi, Keamanan Data.

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/

ABSTRACT

COMPARATIVE SECURITY ANALYSIS OF HL7 FHIR-BASED ELECTRONIC MEDICAL RECORD PAYLOAD EXCHANGE: SATUSEHAT APPROACH, AES-GCM 128-BIT WITH ECC, AND CHACHA20-POLY1305

by

FEBRIANO AHDAN NADIF
22/493642/PA/21206

Digital transformation in the healthcare sector improves the efficiency of Electronic Health Record (EHR) management but also introduces risks to the confidentiality, integrity, and authenticity of patient data. This study aims to design and evaluate an HL7 FHIR-structured EHR payload exchange prototype between Node A and Node B by comparing a conceptual local baseline based on the SATUSEHAT application flow, 128-bit AES-GCM with ECC, and ChaCha20-Poly1305.

The prototype implements three application pipelines. The conceptual local baseline represents payload preparation, dummy-token generation, header construction, serialization, and message reception without a payload-authentication mechanism. The AES-GCM pipeline uses a 128-bit key, whereas ChaCha20-Poly1305 uses a 256-bit key with a 128-bit authentication tag. Both AEAD pipelines employ ECDSA P-256 identities, ECDH P-256 key exchange, context-bound HKDF-SHA-256, AES Key Wrap, and transcript signatures. The evaluation uses 30 synthetic payloads covering small, medium, large, 1 MB, 5 MB, and 10 MB categories in a local application-pipeline microbenchmark.

The results show that all three approaches preserve data consistency for 30 out of 30 payloads. Body modification in the baseline was not detected in any of the five tests because the baseline does not provide payload authentication. In contrast, AES-GCM and ChaCha20-Poly1305 each rejected 25 out of 25 packets modified in applicable components. The timing experiment produced 2,700 raw observations, while peak memory was measured in separate runs using tracemalloc. For the 10 MB category, the mean processing times were 16.123 ms for the baseline, 516.613 ms for AES-GCM, and 516.434 ms for ChaCha20-Poly1305. The baseline produced 0% payload overhead, while its application-message overhead decreased as the payload size increased. For the 10 MB category, the AES-GCM and ChaCha20-Poly1305 packet overheads were approximately 33.3445% and 33.3444%, respectively.

These findings demonstrate that both AEAD pipelines provide authentication and modification-rejection capabilities that are absent from the baseline, at the cost of increased processing time, message size, and memory consumption. The performance differences reflect the complete application-

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/

pipeline workloads and therefore do not establish the inherent superiority of either cryptographic algorithm. The evaluation was conducted locally without an actual network, TLS handshake, production OAuth 2.0 flow, or SATUSEHAT endpoint; consequently, the results do not represent the performance of the production SATUSEHAT service.

Keywords: *Electronic Health Records, HL7 FHIR, SATUSEHAT, AES-GCM, ECC, ChaCha20-Poly1305, Authenticated Encryption, Data Security.*