ABSTRACT

The development of digital transformation increases the use of electronic documents, especially Portable Document Format (PDF), so that a security mechanism is needed that is able to maintain data confidentiality and integrity. Authenticated Encryption with Associated Data (AEAD) algorithms such as AES-GCM and ChaCha20-Poly1305 offer encryption and authentication processes in one mechanism, but their performance is affected by hardware acceleration support. This study aims to analyze the performance of AES-GCM and ChaCha20-Poly1305 in the encryption and decryption process of PDF files measuring 10 MB to 100 MB in AES-NI active and disabled conditions. The study used a controlled experiment method with testing parameters in the form of encryption time, decryption time, throughput, CPU Usage, and Memory Usage. The results showed that AES-GCM provided the best performance when AES-NI was active with faster execution time and higher throughput. Conversely, when AES-NI was disabled, both algorithms experienced a decrease in performance, but ChaCha20-Poly1305 still showed lower execution time and higher throughput than AES-GCM. CPU usage for both algorithms fluctuates, while memory usage is relatively similar and is more influenced by file size. Based on these results, AES-GCM is more suitable for use on systems that support AES-NI, while ChaCha20-Poly1305 is a more efficient alternative in test environments without AES hardware acceleration.

Keywords: AEAD, AES-GCM, ChaCha20-Poly1305, AES-NI, PDF.

ABSTRAK

Perkembangan transformasi digital meningkatkan penggunaan dokumen elektronik, khususnya *Portable Document Format* (PDF), sehingga diperlukan mekanisme keamanan yang mampu menjaga kerahasiaan dan integritas data. Algoritma *Authenticated Encryption with Associated Data* (AEAD) seperti AES-GCM dan ChaCha20-Poly1305 menawarkan proses enkripsi dan autentikasi dalam satu mekanisme, namun performanya dipengaruhi oleh dukungan akselerasi perangkat keras. Penelitian ini bertujuan menganalisis performa AES-GCM dan ChaCha20-Poly1305 pada proses enkripsi dan dekripsi *file* PDF berukuran 10 MB hingga 100 MB pada kondisi AES-NI aktif dan nonaktif. Penelitian menggunakan metode eksperimen terkontrol dengan parameter pengujian berupa waktu enkripsi, waktu dekripsi, *throughput*, *CPU Usage*, dan *Memory Usage*. Hasil penelitian menunjukkan bahwa AES-GCM memberikan performa terbaik ketika AES-NI aktif dengan waktu eksekusi lebih cepat dan *throughput* lebih tinggi. Sebaliknya, pada kondisi AES-NI nonaktif, kedua algoritma mengalami penurunan performa, namun ChaCha20-Poly1305 tetap menunjukkan waktu eksekusi yang lebih rendah dan *throughput* yang lebih tinggi dibandingkan AES-GCM. *CPU Usage* pada kedua algoritma bersifat fluktuatif, sedangkan *Memory Usage* relatif serupa dan lebih dipengaruhi oleh ukuran *file*. Berdasarkan hasil tersebut, AES-GCM lebih sesuai digunakan pada sistem yang mendukung AES-NI, sedangkan ChaCha20-Poly1305 menjadi alternatif yang lebih efisien pada lingkungan pengujian tanpa dukungan akselerasi perangkat keras AES.

Kata Kunci: *AEAD*, AES-GCM, ChaCha20-Poly1305, AES-NI, *PDF*.