ABSTRACT

The exchange of text messages and media files in modern digital communication demands an end-to-end encryption (E2EE) scheme that guarantees confidentiality, integrity, authenticity, and forward secrecy, while remaining resilient to nonce management errors. The widely used AES-GCM has been shown to be fragile under nonce reuse, enabling plaintext reconstruction and authentication tag forgery, while prior research has yet to integrate AES-GCM-SIV, ECDH Curve25519, and HKDF-SHA256 into a single scheme that handles both text messages and media files with quantitative measurement. This research aims to design, implement, and evaluate an E2EE scheme based on an ECDH Curve25519, HKDF-SHA256, and AES-256-GCM-SIV pipeline across both security and performance dimensions. The approach used is a comparative quantitative experiment on a distributed three-entity architecture (Alice, Bob, and Server) running as separate processes on VPS instances connected via the public internet, with 30 iterations per algorithm-data combination across twelve test categories (text of 100–2,000 bytes; image, audio, and video files up to 33.69 MB), accompanied by five security scenarios under the Dolev-Yao threat model (eavesdropping, tampering, replay attack, nonce reuse, and Man-in-the-Middle) and a cumulative ablation study across four tiered configurations (AES-GCM, AES-GCM-SIV, AES-GCM-SIV+ECDH, AES-GCM-SIV+ECDH+HKDF). The results demonstrate that the proposed scheme satisfies every claimed security property within the defined threat model and tested scenarios, whereas the AES-GCM baseline fails both the nonce-reuse and Man-in-the-Middle scenarios. On text data, AES-GCM-SIV incurs a 29.5%–53.6% encryption-time overhead compared to AES-GCM, which narrows and reverses into an advantage on several large data categories, while memory consumption and size overhead remain identical between both algorithms. The ablation study confirms that each component (AES-GCM-SIV, ECDH, HKDF) delivers a specific and irreplaceable security contribution, with performance cost decreasing marginally in the order components are added. This research contributes empirical evidence that the combination of ECDH Curve25519, HKDF-SHA256, and AES-256-GCM-SIV is a viable foundation for E2EE systems resilient to implementation errors.

Keywords: AES-GCM-SIV, ECDH Curve25519, end-to-end encryption, nonce-misuse resistance, text and media messaging

ABSTRAK

Pertukaran pesan teks dan file media dalam komunikasi digital modern menuntut skema *end-to-end encryption* (E2EE) yang menjamin kerahasiaan, integritas, autentisitas, *forward secrecy*, sekaligus tahan terhadap kesalahan pengelolaan nonce. AES-GCM yang umum digunakan terbukti rapuh terhadap *nonce reuse* yang memungkinkan rekonstruksi plaintext dan pemalsuan authentication tag, sementara penelitian terdahulu belum mengintegrasikan AES-GCM-SIV, ECDH Curve25519, dan HKDF-SHA256 dalam satu skema yang menangani pesan teks dan file media sekaligus dengan pengukuran kuantitatif. Penelitian ini bertujuan merancang, mengimplementasikan, dan mengevaluasi skema E2EE berbasis pipeline ECDH Curve25519, HKDF-SHA256, dan AES-256-GCM-SIV pada dimensi keamanan dan performa. Pendekatan yang digunakan adalah eksperimen kuantitatif komparatif pada arsitektur terdistribusi tiga entitas (Alice, Bob, dan Server) yang berjalan sebagai proses terpisah pada VPS yang saling terhubung melalui jaringan internet publik, dengan 30 iterasi per kombinasi untuk dua belas kategori data uji (teks 100–2.000 byte; gambar, audio, dan video hingga 33,69 MB), disertai lima skenario uji keamanan berdasarkan *threat model* Dolev-Yao (*eavesdropping*, *tampering*, *replay attack*, *nonce reuse*, *Man-in-the-Middle*) dan *ablation study* kumulatif terhadap empat konfigurasi bertingkat (AES-GCM, AES-GCM-SIV, AES-GCM-SIV+ECDH, AES-GCM-SIV+ECDH+HKDF). Hasil menunjukkan skema yang diusulkan memenuhi seluruh properti keamanan dalam lingkup *threat model* dan skenario yang diuji, sementara *baseline* AES-GCM gagal pada skenario *nonce reuse* dan *Man-in-the-Middle*. Pada data teks, AES-GCM-SIV mengalami *overhead* waktu enkripsi 29,5%–53,6% dibanding AES-GCM, yang menyempit dan berbalik menjadi keunggulan pada sebagian kategori data besar, sedangkan konsumsi memori dan *overhead* ukuran data identik pada kedua algoritma. *Ablation study* membuktikan setiap komponen (AES-GCM-SIV, ECDH, HKDF) memberikan kontribusi keamanan yang spesifik dan tidak tergantikan, dengan biaya performa yang menurun secara marjinal seiring urutan penambahannya. Penelitian ini menyediakan bukti empiris bahwa kombinasi ECDH Curve25519, HKDF-SHA256, dan AES-256-GCM-SIV layak diadopsi sebagai pondasi sistem E2EE yang tahan terhadap kesalahan implementasi.

Kata kunci: AES-GCM-SIV, ECDH Curve25519, *end-to-end encryption*, *nonce-misuse resistance*, pesan teks dan file media