DAFTAR ISI

LEMBAR PENGESAHAN TUGAS AKHIR i
PENGESAHAN PENGUJI SIDANG TUGAS AKHIR ii
LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR iii
ABSTRACT iv
ABSTRAK v
MOTO DAN PERSEMBAHAN vi
KATA PENGANTAR vii
DAFTAR ISI ix
DAFTAR GAMBAR xii
DAFTAR TABEL xiii
DAFTAR LAMPIRAN xiv
BAB I PENDAHULUAN I-1
1.1 Latar Belakang I-1
1.2 Rumusan Masalah I-7
1.3 Tujuan Penelitian I-8
1.4 Manfaat Penelitian I-9
1.5 Batasan Penelitian I-10
BAB II LANDASAN TEORI II-1
2.1 Advanced Encryption Standard (AES) II-1
2.2 Authenticated Encrypted with Associated Data (AEAD) II-3
2.3 AES-GCM Synthetic Initialization Vector (AES-GCM-SIV) II-6
2.4 Elliptic Curve Diffie Hellman (ECDH) II-11
2.5 HMAC-based Key Derivation Function (HKDF) II-14
2.6 Pesan Teks dan File Media II-17
2.7 Parameter Pengujian Performa II-21
2.8 Penelitian Terkait II-24
BAB III METODOLOGI III-1
3.1 Desain Penelitian III-1
3.1.1 Variabel Penelitian III-2

3.2 Tahapan Penelitian III-3
3.2.1 Studi Literatur III-4
3.2.2 Pengumpulan Data III-5
3.2.3 Arsitektur Sistem III-5
3.2.4 *Threat Model* III-7
3.2.5 Implementasi Algoritma III-8
3.2.6 Perhitungan Metrik III-9
3.2.7 Analisis Data III-10
3.2.8 Skenario Uji III-12
3.2.9 Perbandingan *Baseline* dan *Ablation Study* III-13
3.2.10 Penarikan Kesimpulan III-15
BAB IV HASIL DAN PEMBAHASAN IV-1
4.1 Implementasi Sistem IV-1
4.2 Hasil Pengujian Performa IV-5
4.2.1 Performa pada Pesan Teks IV-5
4.2.2 Performa pada File Gambar IV-8
4.2.3 Performa pada File Audio IV-9
4.2.4 Performa pada File Video IV-11
4.3 Analisis Performa Sistem IV-13
4.3.1 Analisis Waktu Eksekusi dan *Throughput* IV-14
4.3.2 Analisis Konsumsi Memori IV-15
4.3.3 Analisis *Overhead* Ukuran Data IV-16
4.4 Hasil Pengujian Keamanan IV-16
4.4.1 *Eavesdropping* IV-17
4.4.2 *Tampering* IV-18
4.4.3 *Replay Attack* IV-18
4.4.4 *Nonce Reuse* IV-19
4.4.5 *Man-in-the-Middle* IV-21
4.5 Analisis Keamanan Sistem IV-22
4.6 Hasil *Ablation Study* IV-25
4.6.1 AES-GCM IV-26

4.6.2 AES-GCM-SIV IV-27
4.6.3 AES-GCM-SIV + ECDH IV-27
4.6.4 AES-GCM-SIV + ECDH + HKDF IV-28
4.7 Analisis *Ablation Study* IV-28
4.8 Pembahasan IV-30
4.8.1 Perbandingan dengan *Baseline* IV-31
4.8.2 *Trade-off* Keamanan dan Performa IV-32
4.8.3 Implikasi terhadap Sistem E2EE IV-34
4.8.4 Perbandingan dengan Penelitian Terdahulu IV-37
4.9 Keterbatasan Penelitian IV-39
BAB V KESIMPULAN DAN SARAN V-1
5.1 Kesimpulan V-1
5.2 Saran V-3
DAFTAR PUSTAKA 1
LAMPIRAN 9