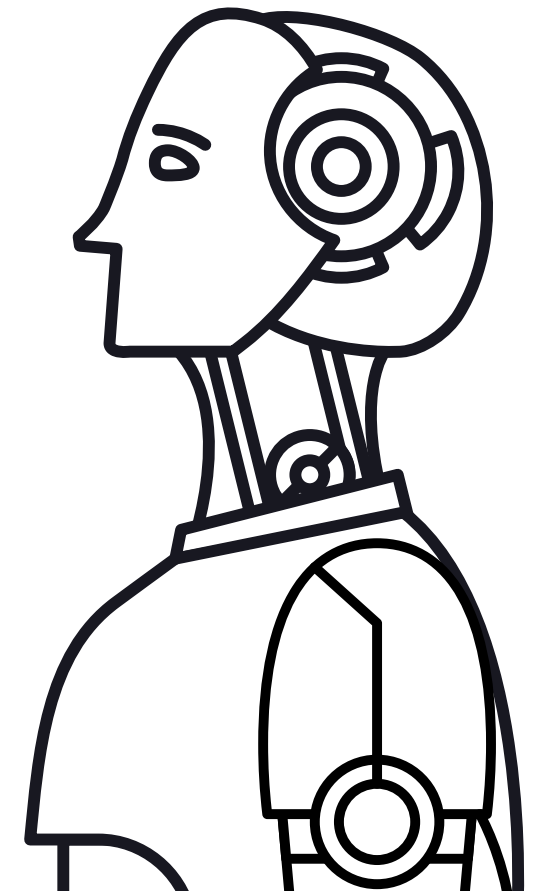
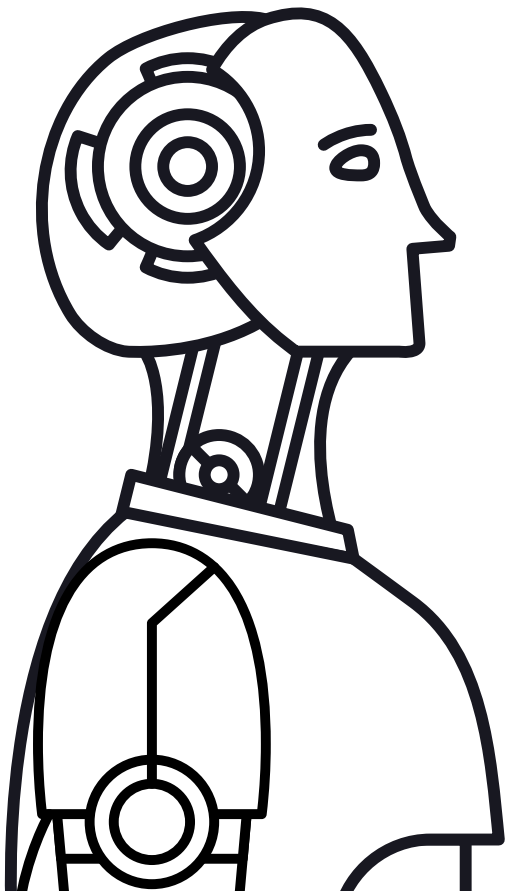


SYSTEMATIC LITERATURE REVIEW

PERBANDINGAN KEAMANAN
ALGORITMA RSA DAN ADVANCED
ENCRYPTION STANDARD (AES) UNTUK
IMPLEMENTASI TANDA TANGAN
DIGITAL

AZKIYA ZHRUL UMAM - 20230801187



Latar Belakang Dan Metologi

01

LATAR BELAKANG

- Perkembangan teknologi digital memerlukan sistem keamanan data yang kuat
- RSA dan AES merupakan dua algoritma kriptografi paling populer
- Perlunya pemahaman komparatif tentang keunggulan dan kelemahan masing-masing

02

METODOLOGI

- Penelusuran sistematis melalui 5 database ilmiah
- 10 artikel diidentifikasi, 5 artikel memenuhi kriteria inklusi
- Periode publikasi: 2020-2025
- Fokus: analisis keamanan, performa, dan implementasi

DASAR TEORI

01

MENURUT SOOD & KAUR (2023)

Keamanan adalah mekanisme yang melindungi informasi dan layanan dari akses tidak sah

02

KLASIFIKASI ALGORITMA

- Simetris (AES): Satu kunci untuk enkripsi & dekripsi
- Asimetris (RSA): Pasangan kunci publik dan privat

03

PAREKH & MARU (2025)

Di era digital, melindungi kerahasiaan, integritas, dan keamanan data adalah kekhawatiran utama



RSA DAN AES

01

RSA

- Menggunakan dua kunci (publik dan privat).
- Cocok untuk tanda tangan digital dan autentikasi identitas.
- Sood & Kaur (2023): "RSA adalah salah satu sistem kriptografi kunci publik paling terkenal untuk tanda tangan digital."

02

AES

- Algoritma simetris, digunakan untuk enkripsi dokumen sebelum tanda tangan.
- Baig et al. (2024):
- "AES menyediakan keamanan kuat untuk transmisi data dan penyimpanan."

HASIL STUDI LITELATUR

No	Peneliti	Fokus	Temuan Utama	
1	Parekh & Maru (2025)	Review keamanan	AES unggul untuk enkripsi, RSA untuk tanda tangan	
2	Sood & Kaur (2023)	Survei komparatif	AES cepat & aman, RSA kurang efisien	
3	Mahesh et al. (2023)	Hybrid RSA–AES	Kombinasi optimal untuk performa & keamanan	
4	Baig et al. (2024)	Studi komparatif	AES efisien, RSA unggul untuk asimetri	
5	Laurentinus et al. (2020)	Eksperimen performa	AES 5.8x lebih cepat dari RSA	



THE STATE OF TECHNOLOGY TODAY

01

ANALISIS UTAMA

- RSA unggul untuk digital signature karena sifat asimetris.
- AES unggul dalam kecepatan enkripsi dokumen.
- Hybrid RSA–AES menjadi kombinasi terbaik (Mahesh et al., 2023).

02

ARAH PENELITIAN SELANJUTN

- 1.Membuat website untuk digital signature
- 2.Standardized Benchmarking untuk Tanda Tangan Digital
- 3.Energy-Efficient Cryptography untuk Perangkat Mobile
- 4.Integration with laravel untuk Sertifikasi Dokumen
- 5.Key Management System untuk Sertifikat Digital

KESIMPULAN

1. RSA cocok untuk tanda tangan digital karena mendukung autentikasi dan non-repudiasi.
2. AES unggul dalam enkripsi cepat dan menjaga kerahasiaan dokumen.
3. Hybrid RSA–AES direkomendasikan untuk sistem tanda tangan digital yang aman dan efisien.
4. Perlu pengembangan kriptografi pasca-kuantum untuk keamanan jangka panjang.



Sumber:

Sood & Kaur (2023); Parekh & Maru (2025); Mahesh et al. (2023); Baig et al. (2024); Laurentinus et al. (2020)



..

..

TERIMA KASIH

