

ABSTRAK

Ancaman terhadap integritas dan otentikasi dokumen digital, seperti pemalsuan dan manipulasi data, semakin meningkat di era digital saat ini. Meskipun standar industri seperti PAdES dan XAdES telah tersedia, penerapannya pada skala internal menimbulkan kendala teknis, yaitu keharusan menanamkan tanda tangan langsung ke struktur fisik dokumen sehingga mengubah nilai hash asli dan menyulitkan validasi berbasis konten (*content-based hashing*). Penelitian ini mengusulkan pendekatan alternatif berupa metode *hybrid-signature* yang menggabungkan RSA dan EdDSA pada lapisan metadata dokumen, dilengkapi indikator visual tanda tangan pada struktur fisik dokumen, tanpa memodifikasi konten utama yang menjadi basis perhitungan *content-based hash*. *Private key* pengguna disimpan terenkripsi melalui skema *envelope encryption* menggunakan Argon2id dan AES-256-GCM sehingga tidak perlu diunduh secara manual. Sistem dirancang menggunakan kerangka *Design Science Research Methodology* (DSRM) dan diimplementasikan pada dokumen PDF, DOCX, dan XLSX dalam skenario distribusi internal (*closed-loop*). Untuk mencegah *replay attack*, sistem membentuk *payload* unik melalui konkatenasi *document_id* dan *document_hash* sebelum proses penandatanganan dilakukan. Pengujian fungsionalitas menggunakan metode *black-box testing* menunjukkan bahwa sistem berhasil mendeteksi manipulasi konten, penghapusan metadata, *replay attack*, serta penandatanganan dengan kunci yang dicabut. Hasil pengujian kinerja menunjukkan bahwa algoritma RSA memiliki durasi *signing* pada rentang 0,76-1,99 milisekon, sedangkan EdDSA berada pada rentang 0,02-0,30 milisekon; verifikasi kedua algoritma berada pada rentang 0,05-0,20 milisekon. Evaluasi *storage overhead* menunjukkan penambahan ukuran *file* relatif kecil dan konstan, terutama pada dokumen berukuran besar. Hasil penelitian ini menunjukkan bahwa pendekatan *metadata embedding* dengan *hybrid-signature* merupakan solusi efektif dan efisien untuk menjamin otentikasi serta integritas dokumen digital dalam lingkungan internal tanpa merusak struktur fisik *file* aslinya.

Kata kunci: *content-based hashing*, *digital signature*, EdDSA, *hybrid-signature*, keamanan dokumen digital, metadata dokumen, RSA

ABSTRACT

Threats to the integrity and authenticity of digital documents, such as forgery and manipulation, are increasingly common in the digital era. Although industry standards like PAdES and XAdES are widely used, applying them in internal environments poses technical challenges, since signature data is embedded directly into the document's physical structure, altering the original hash and complicating content-based validation. This research proposes an alternative approach: a hybrid-signature method combining RSA and EdDSA on the document's metadata layer, complemented by a visual signature indicator on the physical structure, without modifying the core content used to compute the content-based hash. The user's private key is stored encrypted through envelope encryption using Argon2id and AES-256-GCM, eliminating manual key download and management. The system was designed using the Design Science Research Methodology (DSRM) and implemented for PDF, DOCX, and XLSX documents within a closed-loop internal distribution scenario. To prevent replay attacks, the system builds a unique payload by concatenating document_id and document_hash before signing. Black-box testing showed the system successfully detected content manipulation, metadata removal, replay attacks, and signing with revoked keys. Performance testing showed RSA signing durations of 0.76-1.99 ms, while EdDSA ranged from 0.02 to 0.30 ms; verification for both algorithms ranged from 0.05 to 0.20 ms. Storage overhead evaluation showed a relatively small, constant increase in file size, particularly negligible for larger documents. These findings indicate that the metadata embedding approach combined with hybrid-signature effectively and efficiently ensures the authentication and integrity of digital documents in internal environments without compromising the original file structure.

Keywords: content-based hashing, digital document security, digital signature, document metadata, EdDSA, hybrid-signature, RSA