

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era digital saat ini, keamanan informasi menjadi salah satu aspek penting di berbagai bidang, termasuk pemerintahan, pendidikan, bisnis, dan kesehatan. Dokumen digital, seperti kontrak elektronik, sertifikat, atau dokumen legal lainnya, sering digunakan untuk memfasilitasi berbagai proses administrasi dan transaksi. Tetapi ancaman terhadap integritas dan otentikasi dokumen digital, seperti pemalsuan, manipulasi data, hingga penyalahgunaan informasi semakin hari semakin meningkat dan perlu ditangani dengan serius [1]. Karena itu, diperlukan teknologi yang dapat memastikan keaslian dan integritas dokumen-dokumen penting tersebut [2].

Salah satu solusi yang banyak digunakan untuk menjamin keamanan dokumen digital adalah *digital signature*, yaitu mekanisme kriptografi berbasis algoritma asimetris yang memvalidasi keaslian pengirim dan memastikan dokumen tidak berubah sejak ditandatangani [3]. Hal ini menjamin bahwa dokumen yang diterima berasal dari pengirim yang sah dan belum mengalami perubahan sejak ditandatangani. Urgensi penerapannya semakin meningkat seiring dengan kebutuhan dokumen digital yang otentik dan diakui secara hukum, sekaligus mendukung kepatuhan terhadap regulasi perlindungan data dan keamanan informasi [4].

Berbagai algoritma kriptografi digunakan dalam implementasi *digital signature*, seperti RSA, DSA, ECDSA, hingga algoritma modern seperti EdDSA, yang masing-masing algoritma memiliki karakteristik berbeda dalam hal keamanan, efisiensi, dan ukuran tanda tangan. Contohnya algoritma RSA yang menawarkan kompatibilitas luas dan keandalannya yang sudah teruji [5], namun ukuran kuncinya yang besar memengaruhi efisiensi dalam proses penandatanganan dan verifikasi dokumen digital [6]. Sebaliknya, algoritma EdDSA memiliki keunggulan dalam kinerja serta ukuran kunci dan tanda tangan yang kecil, meski belum tahan terhadap

komputer kuantum dan memiliki keterbatasan adopsi pada sistem lama [7]. Karena tidak ada algoritma *digital signature* yang ideal secara penuh untuk seluruh skenario, kombinasi beberapa algoritma diperlukan untuk mencapai keseimbangan antara keamanan, efisiensi, dan kompatibilitas, sekaligus mengoptimalkan distribusi kunci pada lingkungan dengan keterbatasan sumber daya [8][9].

Selain pemilihan algoritma, mekanisme penyisipan tanda tangan digital ke dalam dokumen turut menjadi aspek teknis yang krusial. Dalam ekosistem keamanan dokumen digital, industri telah mengenal standar global seperti *PDF Advanced Electronic Signatures* (PAdES) [10] untuk dokumen berformat PDF dan *XML Advanced Electronic Signatures* (XAdES) [11] untuk dokumen berbasis XML seperti Microsoft Office (.docx dan .xlsx). Standar-standar tersebut dirancang untuk menjamin interoperabilitas lintas aplikasi melalui infrastruktur *Public Key Infrastructure* (PKI) yang kompleks dan sangat bergantung pada layanan otoritas sertifikasi (*Certification Authority*) eksternal.

Namun, kedua standar tersebut memiliki karakteristik utama dengan menanamkan data tanda tangan digital langsung ke dalam struktur fisik dokumen, seperti pada blok *ByteRange* untuk PDF atau penambahan *node* XML pada format Office [12]. Modifikasi struktur *byte* ini mengubah wujud asli dokumen tersebut sebelum dan sesudah ditandatangani, sehingga berisiko merusak integritas struktur fisik *file* tersebut. Literatur terbaru bahkan membuktikan bahwa pendekatan ini rentan terhadap eksploitasi *man-in-the-middle* dan serangan *shadow attacks*, dimana peretas dapat menyisipkan konten berbahaya tanpa merusak validitas tanda tangan [13]. Kondisi ini menyulitkan sistem yang mengandalkan metode *content-based hashing* untuk validasi, karena perubahan struktur fisik dokumen turut mengubah nilai *hash* yang dihitung [14], padahal keaslian dokumen seharusnya dinilai dari informasi dan pesan nyata di dalamnya, bukan sekadar struktur fisik penyusun *file* [15][16]. Ketergantungan pada infrastruktur PKI sering kali berlebihan dan tidak efisien untuk alur kerja distribusi dokumen yang bersifat tertutup di lingkungan internal [17].

Merespons kesenjangan tersebut, penelitian ini mengusulkan sebuah pendekatan alternatif dengan memanfaatkan lapisan metadata sebagai media penyimpanan tanda tangan digital hibrida (kombinasi algoritma RSA dan EdDSA), sehingga konten utama dokumen tetap utuh dan nilai *content-based hashing* tetap konsisten meskipun metadata dokumen mengalami perubahan [18]. Untuk mencegah *replay attack*, sistem membentuk *payload* unik melalui konkatenasi *document_id* dan *document_hash*, serta menerapkan pengecekan *hash_current* terhadap *document_hash* dari *database* secara berlapis, sehingga sebuah *digital signature* tidak dapat digandakan atau diputar ulang pada entri data maupun sesi verifikasi yang berbeda [19].

Selain permasalahan pada lapisan penyisipan tanda tangan, aspek pengelolaan kunci privat turut menjadi perhatian penting dalam penelitian ini. Pendekatan konvensional yang mengharuskan pengguna mengunduh dan menyimpan *private key* secara mandiri berisiko menimbulkan permasalahan kegunaan (*usability*), seperti kehilangan berkas kunci atau penyimpanan yang tidak aman di perangkat lokal [20]. Di sisi lain, penyimpanan *private key* secara langsung di sisi *server* tanpa perlindungan tambahan juga membuka risiko kebocoran masif apabila *database* di *server* dikompromikan [21]. Untuk menjembatani kedua risiko tersebut, penelitian ini mengadopsi pendekatan *envelope encryption*, dimana *private key* pengguna dienkripsi menggunakan kunci turunan dari *passphrase* yang hanya diketahui oleh pengguna itu sendiri, sehingga *private key* tidak pernah tersimpan maupun ditransmisikan dalam bentuk teks murni pada sisi mana pun [20], [21].

Selain aspek keamanan kriptografis, penelitian ini turut mempertimbangkan aspek kegunaan bagi pengguna akhir yang tidak selalu memiliki akses atau kemampuan teknis untuk melakukan verifikasi kriptografis secara langsung [22], [23]. Meskipun validasi keaslian dokumen pada penelitian ini sepenuhnya bergantung pada pemeriksaan *content-based hashing* di sisi *backend*, ketiadaan penanda visual pada dokumen dapat menyulitkan pengguna awam untuk mengenali status tanda tangan suatu dokumen tanpa melalui proses verifikasi eksplisit ke sistem [23], [24]. Oleh karena itu, penelitian ini turut menyisipkan indikator visual tanda tangan

digital pada struktur dokumen sebagai penanda kasat mata, tanpa memengaruhi proses validasi kriptografis yang tetap menjadi sumber kebenaran (*source of truth*) utama dalam menentukan keabsahan dokumen [23], [24], [25].

Berdasarkan serangkaian permasalahan yang telah diuraikan diatas, mulai dari tingginya ancaman manipulasi terhadap dokumen digital, adanya batasan performa dan keamanan pada penggunaan algoritma kriptografi tunggal, hingga kompleksitas standar PAdES dan XAdES yang memodifikasi struktur *byte* dokumen sebagai bagian dari proses penyisipan tanda tangan digital digital serta menyulitkan validasi *content-based hashing*, maka diperlukan sebuah solusi pengamanan yang efisien dan presisi untuk skala internal. Salah satu solusi yang digunakan yaitu mengembangkan sistem untuk menggabungkan dua algoritma, yaitu algoritma RSA dan EdDSA yang digunakan sebagai *digital signature* melalui metode *hybrid-signature*. Untuk mengatasi masalah perubahan struktur *file*, sistem ini juga dirancang dengan memanfaatkan lapisan atribut metadata dokumen sebagai media penyisipan *digital signature*. Melalui pendekatan komprehensif tersebut, penelitian ini mengangkat judul yaitu “PENERAPAN ALGORITMA RSA DAN EDDSA DENGAN METODE HYBRID-SIGNATURE UNTUK KEAMANAN DOKUMEN DIGITAL”.

1.2 Rumusan Masalah

Berdasarkan latar belakang permasalahan yang dipaparkan sebelumnya, terdapat berbagai masalah yang dirumuskan sebagai berikut:

1. Bagaimana menerapkan kombinasi algoritma *digital signature* (RSA dan EdDSA) pada metadata dokumen digital?
2. Bagaimana kinerja kombinasi algoritma *digital signature* (RSA dan EdDSA) dalam proses tanda tangan dan verifikasi pada metadata dokumen digital?

1.3 Tujuan Penelitian

Berdasarkan penjabaran rumusan masalah yang telah dipaparkan sebelumnya, dibentuklah tujuan penelitian sebagai berikut:

1. Menerapkan kombinasi algoritma *digital signature* (RSA dan EdDSA) pada metadata dokumen digital.
2. Mengetahui kinerja kombinasi algoritma *digital signature* (RSA dan EdDSA) dalam proses tanda tangan dan verifikasi pada metadata dokumen digital.

1.4 Batasan Masalah

Untuk memusatkan fokus masalah penelitian sehingga dapat dipahami dalam perspektif yang sama dan membatasi cakupan penelitian, terdapat batasan masalah yang bisa dirumuskan sebagai berikut:

1. Penelitian ini hanya diimplementasikan pada dokumen digital dengan ekstensi .pdf, .xlsx, atau .docx, tanpa mencakup jenis data lainnya seperti gambar, suara, atau video.
2. Implementasi metode *hybrid-signature* pada penelitian ini hanya diterapkan pada proses penandatanganan dan verifikasi satu dokumen dalam satu waktu, serta tidak mencakup skenario *multi-signature* maupun penandatanganan kolektif oleh banyak pengguna.
3. Penelitian berfokus pada penyisipan tanda tangan digital pada metadata dokumen dengan validasi integritas menggunakan metode *content-based hashing*.
4. Penelitian ini dirancang untuk lingkungan distribusi dokumen internal (*closed-loop environment*) dan tidak mencakup analisis terhadap skalabilitas sistem, integrasi lintas organisasi, maupun distribusi yang berskala besar.
5. Proses verifikasi dokumen pada penelitian ini bergantung pada ketersediaan basis data dan layanan *backend* sistem.
6. Lingkup fitur keamanan pada penelitian ini berfokus pada pencegahan modifikasi konten dan *replay attack*, serta tidak mencakup mekanisme pencegahan penghapusan metadata tanda tangan secara manual.

7. Sistem tidak menyediakan mekanisme pemulihan (*recovery*) jika *passphrase* hilang. Jika hilang, maka kunci tidak dapat digunakan hingga *passphrase* diinput ulang.
8. Penelitian ini tidak mencakup implementasi maupun evaluasi algoritma ketahanan pasca-kuantum (*post-quantum cryptography*) dan hanya berfokus pada penggunaan algoritma RSA dan EdDSA.
9. Pengujian sistem pada penelitian ini dilakukan pada lingkungan simulasi lokal (*local development environment*) menggunakan dokumen simulasi, tidak mencakup pengujian pada dokumen asli dalam skenario bisnis tertentu maupun pengujian beban bersamaan (*multi-user concurrency*). Proses pengujian kinerja hanya terbatas pada durasi penandatanganan, durasi verifikasi, serta ukuran *file* sebelum dan sesudah penandatanganan.

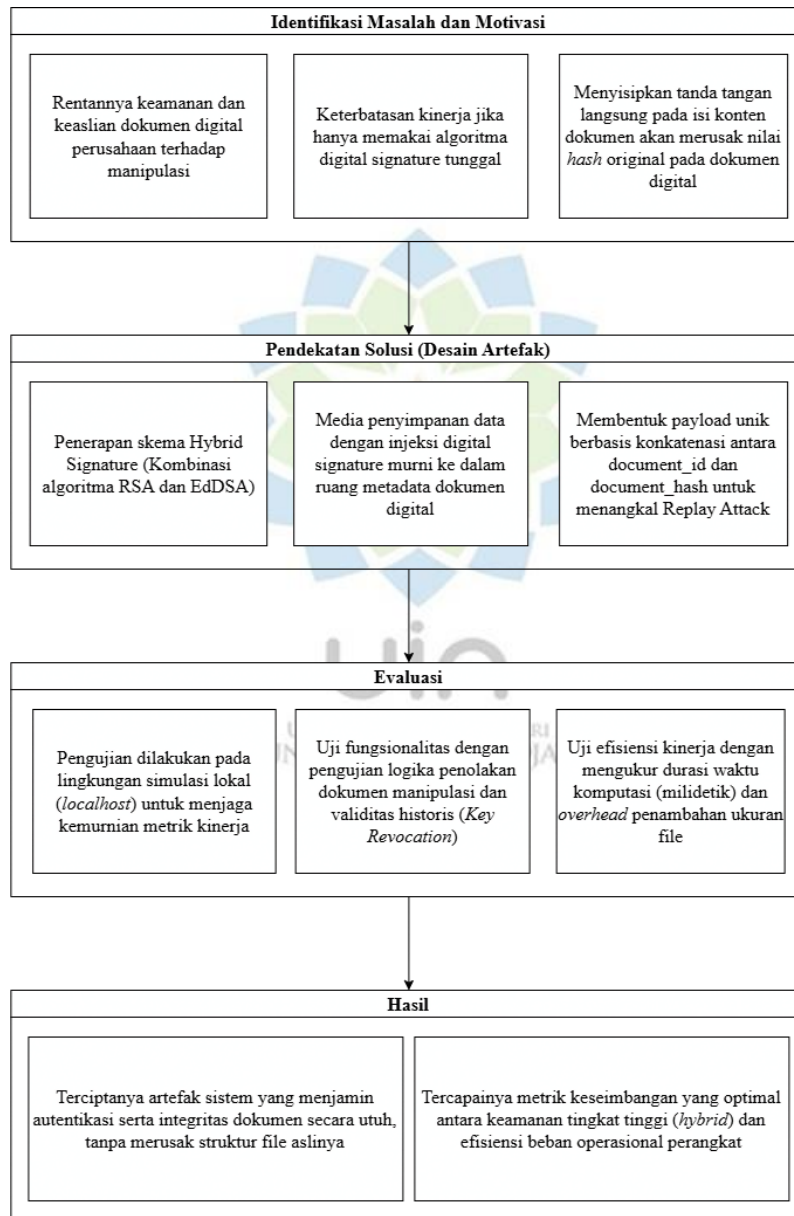
1.5 Manfaat Penelitian

Selain digunakan sebagai tugas akhir perkuliahan peneliti di Program Studi S-1 Teknik Informatika UIN Sunan Gunung Djati Bandung, penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Memberikan kontribusi pada pengembangan pengetahuan di bidang kriptografi, khususnya dalam penerapan *digital signature* pada metadata dokumen.
2. Memberikan solusi untuk meningkatkan keamanan dokumen digital, terutama dalam hal otentikasi dan integritas dokumen.
3. Mengurangi risiko penyalahgunaan atau pemalsuan dokumen digital yang membantu kesadaran tentang pentingnya keamanan dokumen digital, sehingga meningkatkan kepercayaan terhadap dokumen elektronik dalam berbagai transaksi.
4. Mengurangi potensi kerugian akibat manipulasi dokumen digital, baik di tingkat individu maupun organisasi.

1.6 Kerangka Pemikiran

Kerangka pemikiran dalam penelitian ini merupakan struktur logis yang menggambarkan alur penyelesaian masalah, mulai dari tahap identifikasi rintangan teknis hingga pencapaian hasil akhir yang diharapkan. Secara visual, kerangka pemikiran ini dipetakan ke dalam empat fase utama sebagaimana digambarkan pada gambar 1.1.



Gambar 1.1 Diagram kerangka pemikiran

Fase pertama dimulai dengan identifikasi masalah dan motivasi yang menyoroti isu mengenai kerentanan dokumen digital terhadap manipulasi dan

pemalsuan. Tahap ini juga mengidentifikasi bahwa penggunaan algoritma *digital signature* tunggal sering kali menghadapi kendala dalam hal keseimbangan antara tingkat keamanan dan performa kecepatan komputasi. Selain itu, terdapat motivasi teknis untuk menghindari kerusakan nilai *hash* asli dokumen, yang biasanya terjadi apabila tanda tangan digital disisipkan secara langsung ke dalam isi fisik *file* tersebut.

Sebagai langkah penyelesaian, penelitian ini mengusulkan pendekatan perancangan artefak melalui penerapan skema *hybrid-signature* yang mengombinasikan keunggulan algoritma RSA dan EdDSA. Untuk menjaga integritas dokumen, tanda tangan digital tersebut akan disisipkan ke dalam ruang metadata, bukan pada bagian isi utama, sehingga format fisik *file* tetap terjaga secara orisinal. Guna menangani ancaman *replay attack*, pencegahan dilakukan secara berlapis, yaitu sistem pertama-tama akan memeriksa kesesuaian antara *hash_current* yang dibentuk dari dokumen yang diunggah dengan *document_hash* yang diambil dari *database* berdasarkan parameter *document_id* pada metadata. Selanjutnya, sistem membentuk *payload* unik yang dihasilkan melalui konkatenasi (penggabungan) antara parameter *document_id* dan *document_hash*, yang memastikan bahwa setiap tanda tangan digital terikat secara eksklusif pada dokumen tertentu.

Setelah artefak dibangun, proses berlanjut ke fase evaluasi yang dilakukan di dalam lingkungan simulasi lokal (*localhost*) untuk menjamin objektivitas metrik pengujian kinerja tanpa adanya gangguan dari faktor eksternal seperti latensi jaringan, limitasi *bandwidth*, ataupun fluktuasi beban lalu lintas server. Evaluasi ini mencakup dua pengujian utama: pertama, pengujian fungsionalitas untuk memastikan sistem mampu menolak dokumen yang telah dimanipulasi serta memvalidasi status pencabutan kunci (*key revocation*); kedua, pengujian kinerja yang mengukur metrik durasi waktu komputasi dalam satuan milidetik serta dampak penambahan ukuran *file*.

Hasil akhir yang ingin dicapai melalui kerangka pemikiran ini adalah terciptanya sebuah artefak sistem yang tidak hanya menjamin otentikasi serta integritas dokumen secara utuh, tetapi juga tidak merusak struktur *file* aslinya.

Melalui pendekatan ini, diharapkan tujuan penelitian untuk mencapai titik keseimbangan antara tingkat keamanan tinggi dari penerapan *hybrid-signature* dan efisiensi beban operasional perangkat dapat terealisasi sepenuhnya.

1.7 Metode Penelitian

Penelitian ini menggunakan metode pendekatan *Design Science Research Methodology*. Metode ini dipilih karena penelitian ini berfokus pada penciptaan artefak teknologi informasi yang ditujukan untuk menyelesaikan salah satu masalah keamanan dokumen digital. Pendekatan metode penelitian DSRM digunakan untuk merancang sebuah mekanisme pengamanan dokumen yang konkret, di mana metode *hybrid-signature* diterapkan sebagai solusi teknis untuk menjamin integritas dan autentisitas dokumen tanpa mengorbankan kompatibilitas sistem. Proses penelitian ini mengikuti enam tahapan sistematis, dimulai dari identifikasi masalah hingga komunikasi hasil.[26]

Pada tahap pertama yaitu identifikasi masalah dan motivasi, didasarkan pada fenomena meningkatnya ancaman terhadap integritas dokumen digital seperti kontrak elektronik dan sertifikat, yang rentan terhadap pemalsuan dan manipulasi data. Meskipun algoritma *digital signature* RSA menawarkan kompatibilitas luas dan EdDSA menawarkan efisiensi ukuran kunci, penggunaan algoritma tunggal memiliki keterbatasan dalam menyeimbangkan keamanan dan kinerja pada lingkungan internal yang beragam. Masalah spesifik yang diangkat adalah bagaimana menerapkan mekanisme keamanan yang menggabungkan keunggulan kedua algoritma tersebut pada lapisan metadata dokumen digital tanpa memodifikasi konten dokumen itu sendiri. Motivasi penelitian ini adalah menghasilkan solusi yang tidak hanya aman dari sisi kriptografi tetapi juga efisien dalam implementasinya ke dalam dokumen digital.

Dari permasalahan yang sudah dirumuskan di atas, penelitian berlanjut ke tahap definisi solusi. Tujuan solusi diturunkan secara rasional dari rumusan masalah, yaitu merancang sistem yang mampu menerapkan kombinasi

algoritma *digital signature* RSA dan EdDSA secara terintegrasi. Solusi yang dirancang harus mampu berfungsi pada metadata dokumen digital, dengan tujuan kualitatif untuk menjamin keaslian pengirim dan integritas data dan tujuan kuantitatif untuk mengetahui kinerja waktu proses dan efisiensi penyimpanan yang dihasilkan dengan menggunakan pendekatan skema *hybrid-signature*.

Pada tahap desain dan pengembangan, artefak berupa perangkat lunak dikembangkan untuk mengimplementasikan skema *hybrid-signature*. Pengembangan ini berfokus pada pengkodean logika kriptografi yang menggabungkan algoritma *digital signature* RSA dan EdDSA, serta mekanisme penyisipan tanda tangan ke dalam metadata dokumen digital. Lalu artefak yang dihasilkan kemudian masuk ke tahap demonstrasi, di mana sistem diuji menggunakan dokumen digital simulasi untuk membuktikan bahwa konsep *hybrid-signature* dapat berjalan sukses dalam memvalidasi dokumen digital tanpa mengubah konten aslinya.

Rangkaian metodologi penelitian ini diakhiri dengan tahap evaluasi dan komunikasi. Evaluasi dilakukan secara ketat untuk menjawab tujuan penelitian mengenai kinerja sistem. Pengukuran kinerja dibatasi pada indikator durasi proses penandatanganan (*signing*), durasi verifikasi kunci, serta perbandingan ukuran *file* sebelum dan sesudah penandatanganan. Hasil analisis kinerja ini kemudian didokumentasikan dan dikomunikasikan dalam skripsi ini sebagai kontribusi ilmiah untuk memberikan wawasan mengenai efektivitas pendekatan skema *hybrid-signature* dalam mengamankan dokumen digital.

1.8 Sistematika Penulisan

Informasi dan hasil yang didapat dari penelitian ini disusun dalam bentuk tugas akhir. Adapun sistematika penulisannya dapat diuraikan sebagai berikut:

BAB I PENDAHULUAN

Bab I terdiri dari beberapa subbab, yakni Latar Belakang, Rumusan Masalah, Tujuan Penelitian, Batasan Masalah, Kerangka Pemikiran, dan Sistematika Penulisan.

BAB II KAJIAN LITERATUR

Bab II berisikan studi literatur sebagai dasar acuan untuk penelitian ini. Studi literatur pada penelitian terdahulu dimaksudkan untuk membentuk penelitian ini agar sesuai dengan objek dan arah penelitian yang sudah ditentukan.

BAB III METODOLOGI PENELITIAN

Bab III menjelaskan langkah-langkah dan metode penelitian. Selain itu, metodologi yang digunakan disesuaikan untuk memenuhi kebutuhan penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini akan menjelaskan seluruh proses pembuatan sistem. Proses ini dimulai dengan tahap perencanaan kebutuhan sistem, tahap perancangan desain sistem yang digambarkan dalam diagram UML, tahap pengodean sistem, dan tahap pengujian serta kinerja sistem.

BAB V PENUTUP

Pada bab akhir, terdapat simpulan yang membahas jawaban dari pertanyaan pada rumusan masalah. Selain kesimpulan, bab ini pun memuat saran yang ditujukan untuk menunjang dan meningkatkan kualitas pada penelitian selanjutnya.

Daftar Pustaka

Bagian ini berisi daftar dari sumber referensi yang digunakan untuk penelitian.

Lampiran

Dokumen-dokumen tambahan yang digunakan dalam proses penyusunan dan perancangan penelitian dimuat pada bagian lampiran.

