Implementasi Algoritma Kriptografi Tanda Tangan Digital Qrcode Pada Dokumen Dengan Menggunakan Metode Riverst Shamir Adleman (RSA)

Yusmaniar Lubis [1], Ibnu Rusydi[2], Ananda Hadi Elyas[3]

[1,2,3] Rekayasa Perangkat Lunak, Universitas Dharmawangsa
Email: 1 yusminarulubis@gmail.com, 2 ibnurusydi@dharmawangsa.ac.id, 3,* Nanda@dharmawangsa.ac.id
Email Penulis Korespondensi: yusminarulubis@gmail.com

ABSTRAK: Dokumen merupakan aset penting yang menjadi sumber informasi bagi instansi, organisasi, atau individu. Keamanan dan keaslian dokumen sangat krusial, terutama dalam era digital, karena dokumen yang tidak dijaga dengan baik dapat dimanipulasi atau dipalsukan. Permasalahan utama yang dihadapi adalah meningkatnya pemalsuan dokumen, yang seringkali dilakukan dengan memodifikasi isi dokumen atau membuat duplikat dengan tampilan yang mirip. Verifikasi manual tidak lagi efektif karena memerlukan waktu dan upaya lebih. Solusi yang ditawarkan dalam penelitian ini adalah penggunaan tanda tangan digital dengan algoritma RSA yang diubah menjadi Quick Response (QR) Code, yang kemudian dicantumkan pada dokumen fisik untuk menjaga integritas dan keasliannya. Hasil dari penelitian ini adalah terciptanya sistem otentikasi dokumen yang mampu menjaga keaslian dokumen digital dan fisik, dengan mempermudah proses verifikasi dan mengurangi risiko pemalsuan.

Kata Kunci: Digital Signature, RSA Algorithm, QR Code

ABSTRACT: Documents are vital assets that serve as sources of information for institutions, organizations, or individuals. The security and authenticity of documents are crucial, especially in the digital era, where poorly protected documents can be manipulated or forged. The primary issue faced is the increasing occurrence of document forgery, often done by modifying the document's content or creating duplicates with a similar appearance. Manual verification is no longer effective, as it requires more time and effort. The solution proposed in this research is the use of digital signatures with the RSA algorithm, converted into Quick Response (QR) Codes, which are then affixed to physical documents to maintain their integrity and authenticity. The result of this research is the development of a document authentication system capable of preserving the authenticity of both digital and physical documents, simplifying the verification process, and reducing the risk of forgery.

Keywords: Digital Signature, RSA Algorithm, QR Code

PENDAHULUAN

Dokumen merupakan aset vital dan sumber informasi yang dibutuhkan oleh instansi, organisasi, negara, maupun individu. Apabila dokumen tidak dikelola dengan baik, risiko kehilangan data di masa mendatang menjadi sangat mungkin terjadi. Tanda tangan digital dapat menjamin data atau dokumen tidak berubah, sehingga dapat memenuhi sifat keaslian dan membuat pihak yang membuat dokumen tersebut tidak bisa menyangkal.

Penggunaan tanda tangan digital dapat membantu dalam memastikan integritas dari dokumen digital dikarenakan terjadi perhitungan matematika yang dibuat berdasarkan identitas pengirim dan isi dari dokumen tersebut. Dengan berkembangnya teknologi informasi, pemalsuan dokumen semakin mudah dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Pemalsuan biasanya terjadi dengan memanipulasi konten dokumen, menciptakan dokumen baru yang menyerupai desain dan tampilan aslinya. Selain itu, biaya untuk memalsukan dokumen semakin terjangkau, sehingga risiko pemalsuan pun meningkat. Akibatnya, kebutuhan akan keamanan informasi dan perlindungan keaslian dokumen menjadi semakin penting.

Di era teknologi saat ini, verifikasi secara manual menjadi kurang efisien karena memerlukan waktu dan tenaga lebih serta prosedur yang cenderung kompleks. Namun ada beberapa teknik keamanan data selain RSA dan Advanced Encryption Standard (AES) adalah dua algoritma kriptografi yang populer digunakan untuk melindungi data dalam dunia digital. RSA adalah algoritma enkripsi asimetris yang mengandalkan kunci publik dan kunci privat, sedangkan AES adalah algoritma enkripsi simetris yang terkenal akan kekuatannya dalam melindungi informasi dengan kunci yang sama untuk enkripsi dan dekripsi.

Advanced Encryption Standard (AES) telah menggantikan Data Encryption Standard (DES) yang lebih lama sebagai algoritma enkripsi utama dalam berbagai aplikasi, termasuk di bidang militer, keuangan, dan komunikasi online. Keandalan AES dalam memberikan keamanan tinggi dan kecepatan enkripsi menjadikannya pilihan unggul untuk melindungi informasi sensitif di era digital yang semakin terhubung.

Kelebihan Algoritma RSA memiliki tingkat keamanan yang tinggi, memudahkan pertukaran kunci secara aman tanpa harus mengubah kunci privat. Dapat digunakan dalam penanda tanganan digital, dan digunakan secara luas dalam melindungi komunikasi internet, serta dalam pembuatan kunci rahasia.

Kekurangan Algoritma RSA untuk data yang besar dapat memperlambat proses pengerjaan, memiliki ukuran kunci yang lebih besar, dan rentan terhadap suatu serangan dari luar. Maka dari itu Dalam penelitian ini mengambil suatu teknik untuk pengamanan dokumen menggunakan digital signature dengan mengubah signature tersebut ke dalam bentuk dua dimensi.

Metode yang dikembangkan akan mengonversi tanda tangan digital menjadi bentuk Quick Response (QR) code, yang kemudian dapat disertakan pada dokumen fisik sebagai bukti bahwa dokumen tersebut telah ditandatangani secara digital. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem autentikasi dokumen yang memadukan teknik tanda tangan digital dan QR code guna menjaga keaslian dokumen.

METODE PENELITIAN

2.1 Tahapan Pengumpulan Data

Mengumpulkan data dari sumber yang relevan dengan perancangan sistem. Pengumpulan data dilakukan melalui survei di lokasi penelitian, dengan dokumen berformat (docx dan pdf) sebagai data yang dikumpulkan.Data yang telah dikumpulkan kemudian dianalisis sesuai kebutuhan dalam melakukan perancangan serta pembentukan tanda tangan digital. Waktu penelitian yang digunakan untuk melakukan penelitian, mulai dari perencanaan, pengumpulan data, perancangan, penerapan serta pengujian. Rincian keterangan kegiatan selama waktu pembuatan skripsi berlangsung sebagaiberikut:

1. Perencanaan

   Tahap perencanaan adalah fase awal dalam penyusunan skripsi dan perancangan sistem ini melibatkan identifikasi masalah, tujuan, dan kebutuhan.

2. Pengumpulan Data

Pengumpulan data adalah tahap di mana informasi yang diperlukan untuk sistem pembuatan tanda tangan digital dengan menggunakan qr code, data yang diperoleh dapat di terapkan dengan proses identifikasi data, teknik pengumpulan, dan validasi data.

3. Perancangan

   Perancangan adalah tahap yang dilakukan untuk merancang sistem yang akan dibangun berdasarkan data yang telah dikumpulkan dan dianalisis. Tahap ini melibatkan perancangan arsitektur sistem, struktur basis data, dan antar muka pengguna.

4. Penerapan

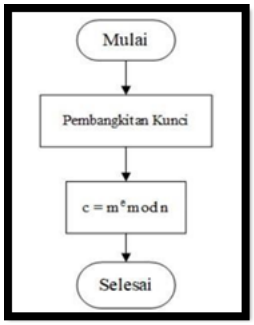
   Penerapan adalah tahap yang dilakukan untuk merealisasikan sistem yang telah dirancang menjadi program yang dapat dijalankan. Selain itu, tahap ini juga melibatkan dokumentasi sistem, yang berisi penjelasan tentang fungsi, fitur, dan cara penggunaan sistem.

5. Pengujian

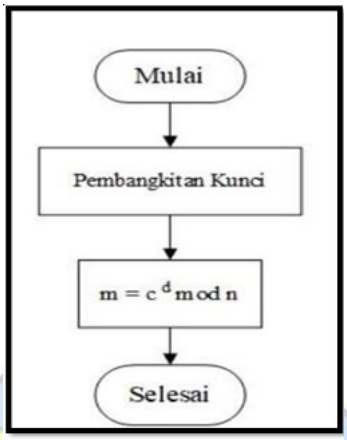
   Pengujian adalah tahap yang dilakukan untuk mengevaluasi kinerja, fungsionalitas, dan kualitas sistem yang telah diimplementasikan. Tahapini melibatkan pengujian sistem, dan integrasi system.

2.2 Penerapan Metode Riverst Shamir Adleman (RSA)

Melakukan perancangan kebutuhan perangkat Merancang kebutuhan perangkat lunak dan tahapan implementasi algoritma kriptografi RSA untuk tanda tangan digital. Proses enkripsi menggunakan kunci publik yang telah ditetapkan sebelumnya, yaitu pasangan (n, e). Sedangkan pada proses dekripsi, digunakan kunci privat (n, d) yang telah ditentukan sejak awal perhitungan.



Gambar 1 Flowchart enkripsi Algoritma Kriptografi RSA



Gambar 2 Flowchart dekripsiAlgoritma Kriptgrafi RSA

HASIL DAN PEMBAHASAN

Algoritma RSA terdiri dari tiga tahapan utama: pembangkitan kunci, enkripsi, dan dekripsi. Tantangan utama dari algoritma ini adalah menemukan dua bilangan prima besar yang akan digunakan sebagai kunci publik dan kunci privat, yaitu p dan q dengan syarat $p \neq q$. RSA mendasarkan proses enkripsi dan dekripsi pada prinsip matematika, khususnya pada konsep bilangan prima dan aritmatika modulo.

Proses matematika ini dilakukan untuk menghasilkan kunci privat yang hanya dapat digunakan dalam proses dekripsi. Algoritma RSA bergantung pada pemfaktoran bilangan besar menjadi faktor-faktor prima. Semakin besar bilangan yang difaktorkan, semakin lama waktu yang dibutuhkan, sehingga meningkatkan kesulitan pemfaktoran. Dengan demikian, semakin besar bilangan yang digunakan, semakin kuat keamanan algoritma RSA.Besaran yang digunakan dalam algoritma kriptografi RSA:

1. p dan q bilangan prima (rahasia)
2. r= p.q (tidak rahasia)
3. $\Phi(n) = (p - 1)(q - 1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)
6. m (plainteks) (rahasia)
7. c (chiperteks) (tidak rahasia)

Permasalahan utama dalam RSA adalah mencari akar dari bilangan komposit dalam modulo nnn yang merupakan pangkat eee dari ciphertext, dengan tujuan menemukan nilai mmm yang memenuhi persamaan me=cmod nm^e = c \mod nme=cmodn, di mana (e,n)(e, n)(e,n) adalah kunci publik RSA dan ccc adalah ciphertext. Pendekatan yang dianggap efektif dalam memecahkan masalah ini adalah dengan memfaktorkan modulus nnn. Jika faktor-faktor prima dari nnn berhasil ditemukan, serangan tersebut dapat menghitung eksponen privat ddd berdasarkan kunci publik (e,n)(e, n)(e,n), kemudian mendekripsi ccc menggunakan prosedur dekripsi standar.

Untuk menyelesaikannya, Memfaktor nilai n menjadi p dan q, lalu menghitung (p-1) (q-1) yang dapat menghasilkan nilai d dan e.

1. Menentukan p dan q.
2. Menghitung nilai modulus (n): n=p.q.
3. Menentukan ⏀(n), prima terhadap n.

Berikut ini adalah hasil dan pembahasan yang ada pada Implementasi Algoritma Kriptografi Tanda Tangan Digital Qrcode Pada Dokumen Dengan Menggunakan Metode Riverst Shamir Adleman (RSA). dalam Sistem Implementasi Algoritma Kriptografi Tanda Tangan Digital Qrcode Pada Dokumen Dengan Menggunakan Metode Riverst Shamir Adleman (Rsa). Pada form login, user harus memasukkan username dan password yang telah terdaftar oleh admin agar dapat masuk ke dalam sistem.

1. Form Login User

Pada form login, user harus memasukkan username dan password yang telah terdaftar oleh admin agar dapat masuk ke dalam system ketika username dan pasword tidak diinputkan terlebih dahulu maka sistem tidak akan bisa digunakan.

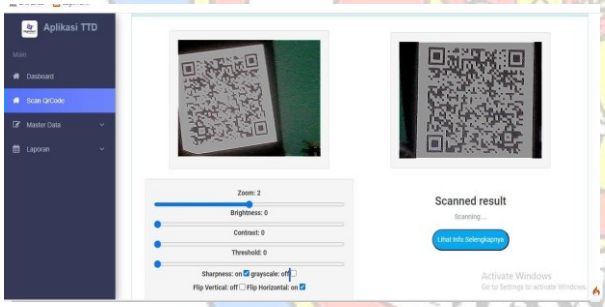
Gambar 3 Tampilan Awal Sistem Tanda Tangan Digital

2. Halaman akses admin

Halaman akses admin merupakan halaman yang dirancang hanya untuk izin akses oleh admin sebagai pengolah sistem dan penambahan Admin menggunakan username dan password yang valid sesuai dengan yang diatur dalam database.

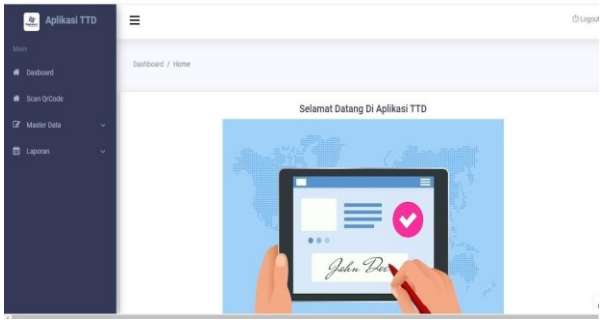
Gambar 4 Halaman Akses Admin

Halaman yang dapat dikelola oleh admin untuk menambah, menghapus, mengedit dan mencetak data surat sesuai dengan alur yang telah dibuat pada sistem.

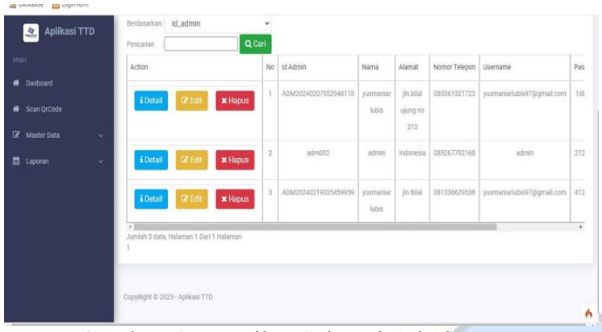


Gambar 5 Halaman Akses Admin

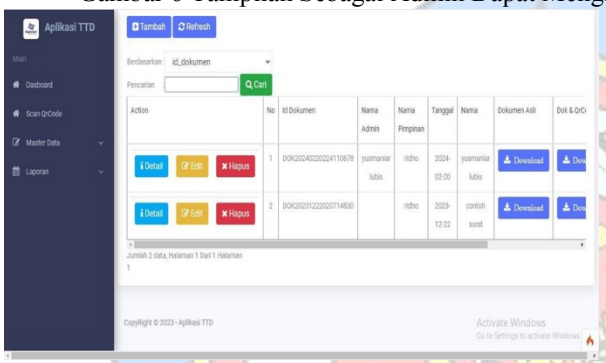
Berikut adalah Tampilan awal sebagai Admin ketika msuk pada sistem tersebut kita dapat memilih pilihan yang ada pada tool bar kiri pada sistem, ketika ingin untuk menjalankan sistem.



Gambar 5 Tampilan Awal Sebagai Admin



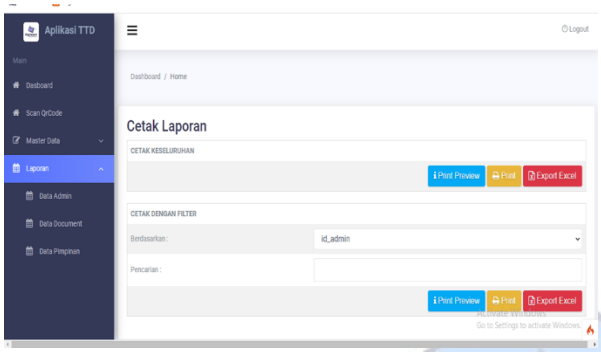
Gambar 6 Tampilan Sebagai Admin Dapat Menghapus, Mengedit,dan Melihat Detail



Gambar 7 Tampilan Untuk Dapat Mendownload Qr Code Dan Dokumen

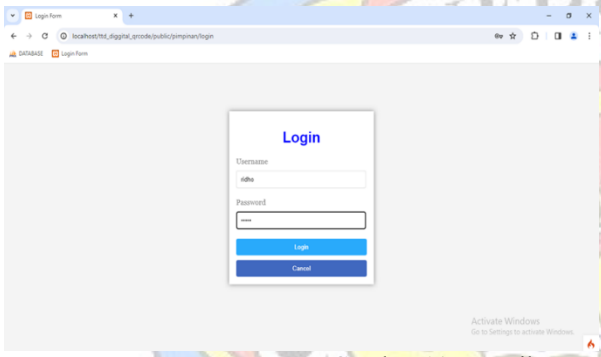
Gambar 8 tampilan untuk dapat melihat tanda tangan yang telah diupload

Tampilan Data Pimpinan dapat menghapus, mengedit serta melihat detail data yang sudah diinput untuk dibaca kembali, melihat tanda tangan manual yang sudah tertera, serta dapat juga melihat user name maupun password yang telah terenskripsi pada system. Laporan terdiri dari 3 yaitu laporan data admin, laporan data dokumen, dan laporan data pimpinan, tiap- tiap masing – masing laporan dapat melihat dokumen dari print privew, print maupun data dari excel.



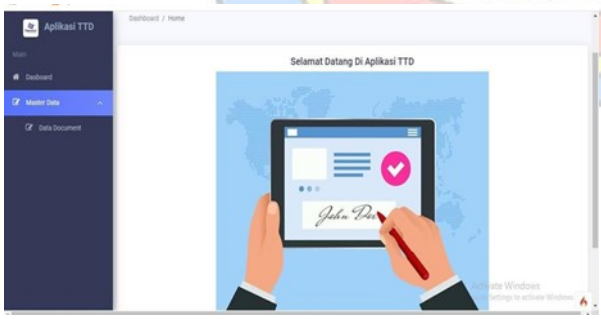
Gambar 9 Dapat Melihat Hasil Laporan

Berikut di bawah ini merupakan tampilan login untuk masuk ke halaman pimpinan dengan cara masukkan username dan password.



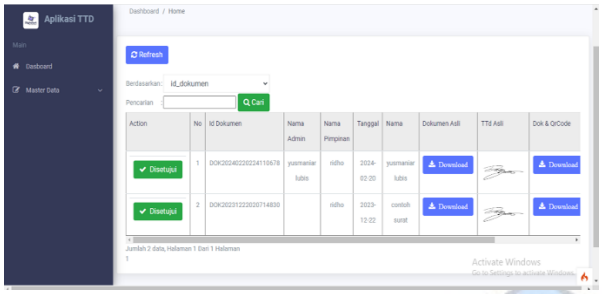
Gambar 10 Tampilan Login Pimpinan

Setelah berhasil login dengan menggunakan username pimpinan , maka dibawah ini merupan tampian awa l halaman pimpinan dimana terdapat menu master data dan data dokumen.



Gambar 11 Tampilan Awal Pimpinan

Dari gambar berikut terdapat pada login pimpinan, terbagi atas 2 bagian yaitu, master data, yang didalamnya terdapat data dokumen seperti pada gambar dibawah ini.



Gambar 12 Tampilan Pimpinan untuk memberikan setuju

SIMPULAN

Hasil penelitian ini menyimpulkan bahwa keamanan sistem kriptografi dapat ditingkatkan dengan mengembangkan tanda tangan digital menggunakan kombinasi algoritma RSA dan fungsi hash standar (SHA-3). Algoritma RSA, dengan kunci publik dan kunci privat, digunakan untuk proses enkripsi yang menghasilkan tanda tangan digital unik untuk setiap dokumen, tergantung pada isi dokumen dan kunci pribadi pengirim. Tanda tangan digital ini menjamin bahwa dokumen yang tidak berubah menghasilkan nilai dekripsi yang sama, sedangkan dokumen yang diubah akan memiliki nilai dekripsi berbeda. Pengujian kualitas enkripsi menunjukkan hasil yang baik berdasarkan waktu enkripsi-dekripsi, nilai entropi, korelasi, dan efek avalanche. Algoritma RSA memastikan keamanan transmisi pesan meskipun kunci publik disebarluaskan, karena hanya pemilik kunci privat yang dapat mendekripsi pesan tersebut.

SARAN

Berdasarkan hasil penelitian, disarankan agar pengembangan lebih lanjut dari sistem ini dilakukan dengan memperhatikan beberapa hal. Karena penelitian ini dilakukan dalam kurun waktu sekitar tiga bulan, masih banyak aspek yang dapat ditingkatkan untuk menyempurnakan sistem. Penelitian selanjutnya diharapkan dapat menambahkan fitur-fitur yang lebih mendukung kualitas sistem, seperti fitur grafik diagram untuk visualisasi data, fitur notifikasi untuk meningkatkan interaksi pengguna, serta pengembangan fitur keamanan yang lebih baik dalam sistem tanda tangan digital. Hal ini akan membantu menciptakan sistem yang lebih lengkap, efisien, dan user-friendly.

REFERENSI

Abdurrachman, T., & Suteja, B. R. (2021). Pengembangan sistem informasi dengan tanda tangan digital. Jurnal Teknik Informatika dan Sistem Informasi, 7(1), 261-273. https://doi.org/10.28932/jutisi.v7i1.3431

Cristy, N., & Riandari, F. (2021). Implementasi metode Advanced Encryption Standard untuk pengamanan data. Jurnal Ilmu Komputer dan Sistem Informasi, 4(2), 75-85.

Dermawan, R. (2021). Pemanfaatan tanda tangan digital tersertifikasi. Jurnal Hukum Lex Generalis, 2(8), 762-781. https://doi.org/10.56370/jhlg.v2i8.95

Munir, R. (2019). Kriptografi 2nd Edition. Bandung: Informatika.

Nadzifarin, A., & Asmunin, A. (2022). Penerapan algoritma digital signature dengan ECDSA. Jurnal Informatika dan Ilmu Komputer, 4(1), 1-9.

Putra, N. B. N., Raihana, F. A., Mondong, W. M. A., & Kardian, A. R. (2023). Analisis enkripsi kriptografi RSA berbasis batch programming. Jurnal Riset Sistem Informasi dan Teknologi Informasi, 8(1), 142-154.

Rizki, M., & Ariyani, F. (2021). Penerapan kriptografi dengan RSA untuk pengamanan data berbasis desktop. Sistem Komputer dan Teknologi Informasi, 4(2), 1-6.

Saepulrohman, A., & Negara, T. P. (2021). Implementasi algoritma digital signature berbasis Diffie-Hellman. Komputasi: Jurnal Ilmu Komputer dan Matematika, 18(1), 22-28. https://doi.org/10.33751/komputasi.v18i1.2569

Sholihah, W., Indriasari, S., Noviyanti, I., Mardiyono, A., & Aziezah, N. (2022). ESVISIGN: Implementasi tanda tangan digital. Jurnal Teknologi Informasi dan Multimedia, 3(4), 217-226. https://doi.org/10.35746/jtim.v3i4.188

Simbolon, I. A. R., Gunawan, I., Kirana, I. O., Dewi, R., & Solikhun, S. (2020). Penerapan algoritma AES dalam pengamanan data kependudukan. Jurnal Sistem Komputer dan Informatika, 1(2), 54-60.