Implementasi Sistem Pendataan dan Penandatanganan Dokumen Dengan Sertifikat Digital

Implementation of Data Collection System and Document Signing With Digital Certificate

1st Raihan Febian Bahy
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
raihanbahy@student.telkomuniversity.ac.id

2nd Yudha Purwanto
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
omyudha@telkomuniversity.ac.id

3rd Muhammad Faris Ruriawan
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
muhammadfaris@telkomuniversity.ac.id

Abstrak—Bentuk fisik dokumen telah banyak berubah, yang sebelumnya dokumen hanya dapat digunakan apabila telah dicetak, maka sekarang dokumen juga dapat digunakan dari bentuk digitalnya saja. Namun seiring dengan perubahan bentuk fisik dokumen, tidak menutup juga tindakan kejahatan yang terjadi, seperti pemalsuan dokumen terutama pada bagian pengesahan atau penandatanganannya. Proses validasi dokumen digital menggabungkan teknik penandatanganan dokumen digital dengan algoritma kriptografi, algoritma kriptografi yang digunakan adalah algoritma Base64. Dengan menggabungkan algoritma kriptografi Base64 dan hashing MD5, maka diharapkan akan terciptanya metode untuk memvalidasi dokumen digital yang aman dan tetap menjaga aspek C.I.A (Confidentiatlity, Integrity, and Availability) di dalam dunia kriptografi. Oleh karena itu, hasil yang diperoleh dari tugas akhir ini adalah terciptanya sebuah platform digital atau website yang berfungsi untuk memudahkan proses input dan validasi dokumen digital dengan tingkat keamanan yang tinggi dengan menggunakan algoritma kriptografi dalam proses validasinya.Sehingga data yang ada dapat di akui kebsahannya.
Kata kunci—kriptografi, MD5, base64, validasi.

Abstract—The physical form of documents has changed a lot, previously documents can only be used if they have been printed, now documents can also be used in digital form only. However, along with the change in the physical form of the document, it also does not close the crimes that occur, such as falsifying documents, especially in the ratification or signing section. The digital document validation process combines digital document signing techniques with cryptographic algorithms, the cryptographic algorithm used is the Base64 algorithm. By combining the Base64 cryptographic algorithm and MD5 hashing, it is hoped that a method will be created to validate secure digital documents while maintaining the C.I.A (Confidentiatlity, Integrity, and Availability) aspects in the world of cryptography. Therefore, the result obtained from this final project is the creation of a digital platform or website that functions to facilitate the input and validation process of digital documents with a high level of security by using cryptographic algorithms in the validation process. So that the existing data can be recognized as valid.
Keywords—cryptography, MD5, Base64, validation.

I. PENDAHULUAN

Dokumen adalah surat yang tertulis atau tercetak yang dapat digunakan sebagai bukti ataupun keterangan. Sejak dahulu dokumen telah menjadi sesuatu yang penting diseluruh dunia, karena dengan sebuah dokumen kita dapat menunjukkan validitas dari sebuah hal, dokumen juga dapat memberitahukan kita tentang hal yang penting. Perkembangan zaman juga telah mempengaruhi tipe fisik dokumen, sebelumnya dokumen hanya dapat digunakan apabila telah tercetak, tetapi pada saat ini dokumen juga dapat digunakan hanya dengan bentuk digitalnya saja.

Namun seiring dengan perkembangan zaman juga, banyak orang yang memanfaatkan bentuk digital dari dokumen tersebut untuk tindakan kejahatan. Salah satunya adalah dengan memalsukan dokumen, terutama pada bagian pengesahan atau penandatanganan dokumen. Oleh karena itu diperlukan sebuah cara agar bagian validasi pada dokumen tersebut tidak dapat dipalsukan atau dokumen tersebut digunakan oleh orang yang salah. Validasi dokumen digital merupakan salah satu metode untuk membuktikan keaslian sebuah dokumen digital, metode ini memanfaatkan algoritma kiptografi untuk keamanan datanya, sehingga dokumen yang divalidasi akan sulit untuk dipalsukan atau ditiru karena telah terenkripsi dengan baik oleh algoritma kriptografi.

Oleh karena itu, penelitian ini akan difokuskan pada perancangan dan pembuatan aplikasi berbasis *web* yang dapat digunakan untuk memvalidasi dokumen digital. Aplikasi ini direncanakan akan menggunakan proses validasi yang terenkripsi sebagai solusi validasi dokumen digital.

II. KAJIAN TEORI DAN METODE

A. Validasi Dokumen Digital

Validasi merupakan suatu tindakan pembuktian yang dilakukan berdasarkan dengan tata cara yang sudah disetujui atau disepakati. Validasi juga merupakan suatu usaha agar suatu objek dapat di katakan benar atau valid. Validasi dokumen merupakan suatu tindakan yang

dilakukan oleh seorang verifikator/validator untuk menilai keabsahan dari sebuah dokumen, apakah sah atau tidak. Validasi dokumen digital merupakan validasi dokumen yang dilakukan secara digital, yang melibatkan suatu sistem yang dirancang untuk melakukukan proses validasi tersebut.

Banyak metode yang dapat di implementasikan dalam melakukan proses validasi dokumen digital, diantaranya:

1. *QR Code*

   QR Code adalah suatu kode matriks dua dimensi yang didalamnya mampu menyimpan informasi hingga ribuan karakter alfanumerik[1]. *QR Code* disini dapat digunakan untuk menyimpan sebuah kode enkripsi dari sebuah data yang apabila nantinya di *scan* untuk melakukan validasi, akan merujuk kepada sebuah hasil dari data yang tersimpan pada *QR Code* tersebut.

2. *Digital Signature*

   Digital signature atau tanda tangan digital merupakan sebuah metode yang dapat digunakan untuk menggantikan tanda tangan secara manual pada dokumen cetak seperti kertas[2].

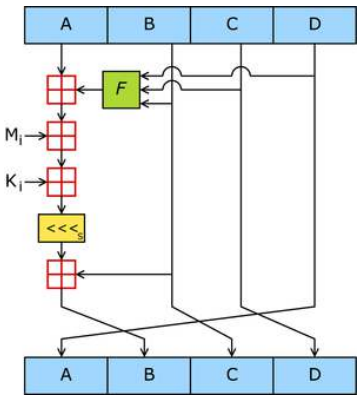
3. *Barcode*

   Barcode merupakan data optik yang di dalamnya terdapat bentuk garis atau *bar* yang mampu dibaca oleh mesin. Berbagai kode ini memiliki fungsi dalam membedakan satu jenis produk dengan produk lain[3].

B. *MD5 Hashing*

Dalam kriptografi, *MD5 (Message-Digest Algortihm 5*) ialah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. Pada standar Internet *(RFC 1321)*, *MD5* telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan *MD5* juga umum digunakan untuk melakukan pengujian integritas sebuah berkas[2].

Untuk lebih jelasnya, *MD5* merupakan sebuah fungsi hashing kriptografik yang mudah digunakan dan diimplementasikan. Keamanan *MD5* terletak pada pengacakan karakter yang dijadikan hasil *hashing*, hasil *hashing* tersebut berasal dari data yang digunakan untuk di *hashing*. Untuk cara kerja *MD5* sendiri dilakukan dengan mengolah blok yang berisi 512-bit, lalu dibagi ke dalam 16 sub-blok yang berukuran 32-bit. Hasil dari keluaran tersebut akan menjadi 4 blok yang berukuran 32-bit yang apabila digabungkan akan berjumlah 128-bit.



GAMBAR 1
(Algoritma MD5)

Pesan diberi tambahan sedemikian sehingga panjang menjadi k-bit, dimana k = 512n – 64 bit, dan n merupakan blok masukan. Tambahan ini diperlukan hingga pesan menjadi k-bit. Kemudian 64-bit yang masing kosong, dibagian akhir, diisi panjang pesan. Inisiasi 4 variabel dengan panjang 32-bit yaitu a, b, c, d. Variabel a, b, c, d dikopikan ke variable a, b, c, d yang kemudian diolah melalui 4 tahapan yang sangat serupa. Setiap tahapan menggunakan 16 kali operasi berbeda, menjalankan fungsi nonlinear pada tiga variabel a, b, c, atau d. Hasilnya ditambahkan ke variabel keempat, sub-blok pesandan suatu konstanta. Kemudian dirotasi kekiri beberapa bit yang kemudian ditambahkan ke salah satu dari a, b, c, atau d. Kemudian nilai a, b, c, dan d menggantikan nilai a, b, c, dan d. Kemudian dikeluarkan output yang merupakan gabungan dari a, b, c, dan d. Fungsi kompresi yang digunakan oleh algoritma MD5 adalah sebagai berikut

$$a \leftarrow b + ((a + g(b,c,d) + X[k] + T[i] <<< s)$$

Dimana g adalah salah satu fungsi primitif F, G, H, I seperti dibawah ini :

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$$

GAMBAR 2
(Fungsi Primitif F, G, H, dan I)

Lalu untuk operasi XOR, AND, OR, dan NOT adalah sebagai berikut[3] :

$$\oplus, \wedge, \vee, \neg$$

GAMBAR 3
(Operasi Logika MD5)

C. *Base64 Algorythm*

Algoritma Base64 merupakan salah satu algoritma untuk *Encoding* dan *Decoding* suatu daya ke dalam format *ASCII*, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan *encoding* (penyadian) terhadap data *binary*. Umumnya digunakan pada berbagai aplikasi seperti *e-mail via MME*, data *XML*, atau untuk keperluan encoding *URL*[4].

Untuk lebih jelasnya, algoritma *Base64* ini merupakan algoritma kriptografi yang digunakan untuk penyandian *(encoding*) dan penafsiran kode *(decoding)* sebuah data. Cara kerja dari algoritma ini adalah sebagai berikut[5]:

1. Input data diubah kedalam Bilangan *ASCII* dan diambil nilai binernya
2. Nilai biner semua bilangan *ASCII* digabungkan dan dikelompokkan kedalam 1 kelompok mengandung 6-bit.
3. Setiap kelompok yang berisi 6-bit dipetakan ke-1 karakter yang dapat dicetak dan didasarkan pada nilai 6-bit menggunakan peta set karakter *Base64*.
4. Karakter *padding* "=" juga digunakan padaakhir teks yang dikodekan jika jumlah bit (atau jumlah karakter pada *plaintext*) tidak banyak dari 3. Jika jumlah bit dalam teks adalah 3n + 1, maka *encoder* menempatkan satu "=" pada akhir teks yang

dikodekan, dan jika jumlah bit dalam teks adalah 3n + 2, maka akan menempatkan dua "=" pada akhir keluaran.

D. *HTML*

Hypertext Markup Language atau yang biasa disebut *HTML*, merupakan sebuah bahasa *markup* yang biasa digunakan untuk membuat sebuah *web* atau aplikasi. *HTML* memungkinkan *user* untuk membuat dan menyusun bagian *paragraph, heading, link,* dan *blackquote* yang nantinya dapat diakses oleh user dan ditampilkan pada halaman *web* atau aplikasi yang dibuat.

Dokumen *HTML* juga memiliki struktur dasar, struktur dasar ini berfungsi agar dokumen dapat terbaca dan dapat ditampilkan pada halaman *web*, struktur *HTML* dapat dilihat pada gambar berikut.

Dengan penjelasan sebagai berikut[5]:

1. <!DOCTYPE>

!Doctype atau biasa disingkat menjadi DTD merupakan sebuah singkatan dari *Document Type Declaration*. Fungsi dari penulisan DTD ini adalah untuk memberikan informasi pada bagian *web browser* mengenai jenis dokumen yang nantinya akan diproses pada bagian *HTML.*

2. <html>

Bagian berikutnya adalah bagian <html>, tag pembuka ini harus menggunakan kode <html> seperti yang sudah dibuat sebelumnya. hal tersebut disebabkan tag <html> merupakan wadah yang nantinya akan diisi oleh berbagai macam isi yang kita sebut dengan *CSS*. Pada bagian ujungnya ditambahkan penulisan </html>. Hal tersebut dimaksudkan sebagai penutup *HTML* dan wajib ditulis.

3. <head>

Pada bagain tag <head>, kita dapat menuliskan judul dan berbagai macam kode-kode yang tidak tampil pada browser. Kode-kode yang dapat ditulis pada bagian <head> ini adalah *CSS* dan juga JavaScript. Hal tersebut membuat kita dapat melakukan kreasi pada bagian head ini.

4. <title>

Kode ini digunakan sebagai judul website atau penjelasan singkat mengenai website yang kita buat. Oleh sebab itu, pada bagian “title”, kita bebas mengisinya dengan nama yang relevan dengan *website* yang dibuat.

5. <body>

Pada bagian ini, kita dapat memasukan beberapa unsur elemen yang nantinya akan muncul pada tampilan *website*. Kita dapat mengisinya dengan gambar, tautan, tulisan, dan berbagai macam isi *website* lainnya. Sama halnya dengan bagian lainnya, kita harus menutupnya dengan penulisan </body> untuk mengunci isi yang terdapat di dalam *body website*.

E. *PHP-MySQL*

PHP merupakan bahasa pemrograman berbasis *web*. Umumnya *PHP* digunakan untuk membuat *website* yang dinamis. Bahasa pemrograman *PHP* biasanya disisipkan pada dokumen *HTML*, tetapi tag *HTML* juga bisa disisipkan pada *PHP*. Sedangkan MySQL merupakan sebuah perangkat lunak sistem manajemen basis data *SQL (Database Management System)* atau *DBMS* yang *multithread*, *multi-user*. Intinya Sistem yang digunakan untuk mengolah *database*[6].

III. HASIL DAN PEMBAHASAN

Pengujian pada aplikasi ini dilakukan dengan tiga jenis pengujian, yaitu *Whitebox Testing, Blackbox Testing,* dan *Performance Test.*

.

A. *Whitebox Testing*

Whitebox testing dilakukan untuk menguji setiap skenario yang terdapat pada aplikasi ketika *user* mengakses aplikasi tersebut. Skenario pengujian yang pertama dilakukan untuk menguji skenario *register* dan *login*. Pada skenario ini, fungsionalitas skenario *register* dan *login* berjalan lancar. Skenario yang kedua adalah menguji halaman lihat data. Skenario pada halaman ini berjalan lancar karena halaman dapat menampilkan seluruh komponennya. Skenario yang ketiga dilakukan untuk menguji halaman *input* data. Pengujian ini cukup krusial, dikarenakan skenario ini merupakan skenario inti dari aplikasi ini. Hasil dari skenario ketiga ini berjalan lancar, data yang di *input* dapat masuk *database* dan nomor dokumen yang di enkripsi dapat di *generate* menjadi *QR Code*. Skenario keempat juga merupakan skenario inti dari aplikasi ini, dikarenakan ini merupakan fitur inti dari aplikasi ini. Hasil dari skenario ini berjalan lancar, *QR Code* yang di scan oleh sistem dapat terbaca dan data di dalamnya dapat tervalidasi.

Skenario kelima adalah pengujian *edit* dan *delete* data. Skenario ini berjalan lancar, data yang ada di *database* berhasil untuk di update lalu berikutnya data juga berhasil di hapus dari *database*. Skenario yang terakhir adalah skenario untuk menguji *Side Bar* dan *Navigation Bar* yang terdapat pada aplikasi ini. Hasil dari skenario ini berjalan lancar, masing-masing *bar* dapat berjalan sesuai dengan ekspektasi.

B. *Blackbox Testing*

Blackbox testing adalah pengujian untuk menguji setiap fitur yang terdapat pada aplikasi, apakah dapat berjalan sesuai ekspektasi atau tidak. Pengujian yang pertama adalah pengujian dari fitur *register* dan *login*. Hasil dari pengujian pertama ini berjalan lancar, setiap komponen dan fitur yang terdapat pada masing-masing halaman ini dapat berjalan sesuai dengan fungsinya. Pengujian yang kedua adalah pengujian halaman lihat data. Pengujian kedua ini berjalan lancar, setiap komponen dan fitur yang ada dapat berjalan sesuai dengan fungsionalitasnya. Pengujian yang ketiga dapat dikatakan sebagai pengujian inti, karena pengujian ini merupakan pengujian fitur inti dari aplikasi ini, yaitu pengujian *input* data. Pengujian ketiga dapat berjalan lancar, setiap komponen dan fitur pada halaman *input* data dapat berjalan seusai dengan fungsinya. Pengujian yang keempat juga merupakan pengujian fitur inti dari aplikasi, yaitu pengujian validasi data. Pengujian yang keempat dapat berjalan lancar, *scanner* yang ada dapat melakukan scanning *QR Code* yang ada dan

berikutnya setelah nomor dokumen di *submit*, aplikasi dapat memvalidasi dokumen tersebut.

Pengujian kelima adalah pengujian fitur *edit* dan *delete* data. Pengujian ini berjalan lancar, masing-masing fitur dapat berjalan sesuai dengan ekspektasi. Fitur *edit* dapat melakukan update data pada *database*, dan fitur *delete* dapat menghapus data pada *database*. Pengujian terakhir adalah pengujian *Side Bar* dan *Navigation Bar*. Peengujian ini berjalan lancar, karena masing-masing fitur dapat menampilkan dan menjalankan perintah dari *user*.

C. Performance Test

Performance test adalah pengujian untuk menguji performa dari masing-masing fitur yang terdapat pada aplikasi. Satuan yang digunakan adalah /detik *(/s)* dan disajikan dalam bentuk grafik. Uji performansi yang pertama adalah pengujian performa dari *input* data. Hasil yang di dapat adalah setiap *input*-an memiliki waktu yang berbeda berdasarkan jumlah data yang di input oleh *user*. Uji performansi yang kedua adalah uji performa dari validasi dokumen. Hasil waktu dari pengujian ini juga berbeda-beda berdasarkan jumlah data dari dokumen yang divalidasi. Uji performansi yang ketiga adalah pengujian *edit* data. Hasil yang didapat juga berbeda-beda, didasarkan banyaknya jumlah data yang di *update*. Uji performansi yang terakhir adalah uji performa dari *delete* data. Hasil uji performa *delete* data ini memiliki rerata hasil yang paling cepat dibandingkan dengan tiga uji performansi sebelumnya. Hal ini dikarenakan sistem hanya diperintahkan untuk menghapus data yang terdapat pada *database*.

IV. KESIMPULAN

Berdasarkan seluruh hasil pengujian yang telah dilakukan terhadap aplikasi "IMPLEMENTASI SISTEM PENDATAAN DAN PENANDATANGANAN DOKUMEN DENGAN SERTIFIKAT DIGITAL", didapatkan bahwa aplikasi ini dapat berjalan sesuai dengan ekspektasi tanpa menemui kendala yang mengakibatkan tidak berjalannya sistem atau algoritma dan logika pada aplikasi ini. Fitur-fitur inti seperti *input* data dan validasi dokumen beserta fitur-fitur pendukung pada aplikasi ini dapat berjalan sesuai dengan fungsionalitasnya. Kendala seperti *bug* ataupun kesalahan logika dan algoritma pada aplikasi ini tidak terjadi, karena sudah dilakukan *testing* terhadap *source code* aplikasi ini.

REFERENSI

[1] https://accurate.id/ekonomi-keuangan/qr-code-adalah/ [Diakses 22 Juli 2021].

[2] R. Munir, *Pengantar Kriptografi IF5054 Kriptografi*, Departemen Teknologi Informasi Institut Teknologi Bandung, Vol. 1, pp.320, 2004.

[3] https://accurate.id/marketing-manajemen/barcode-adalah/ [Diakses 22 Juli 2021].

[4] M. I. D. Ramdhani, "*Perbandingan Kriptografi Klasik (Caesar Cipher) dan Kriptografi Modern (MD5)",* Teknik Informatika Sains dan Teknologi, Universitas Islam Negeri Sunan Gunung Djati, Bandung, 2009.

[5] S. Mujaddid, "*Kriptoanalisis Pada Fungsi Hash Kriptografi MD5"*, Teknik Informatika ITB, Bandung, 2009.

[6] Azlin, F. Musadat, J. Nur, *APLIKASI KRIPTOGRAFI KEAMANAN DATA MENGGUNAKAN ALGORITMA BASE64*, Jurnal Informatika, Vol. 7, No. 2, pp.1-5, Baubau, Desember 2018.