

# PENGEMBANGAN SISTEM TANDA TANGAN ELEKTRONIK MENGUNAKAN FUNGSI *HASH* SHA-512 DAN ALGORITMA KUNCI PUBLIK RSA DI UNIVERSITAS AL AZHAR INDONESIA (STUDI KASUS DI LINGKUNGAN FAKULTAS SAINS DAN TEKNOLOGI)

Malia Arismaya Ichsan Putri dan Denny Hermawan

*Program Studi Informatika, Fakultas Sains dan Teknologi, Universitas Al Azhar Indonesia Jl.  
Sisingamangaraja No. 2, Kebayoran Baru, DKI Jakarta 12110 Indonesia  
maliaarismayaichsanputri5@if.uai.ac.id, denny@if.uai.ac.id*

## Abstrak

Pada masa pandemi COVID-19 ini, seiring dengan penggunaan dokumen *digital*, tanda tangan tidak lagi dibuat di atas kertas atau yang biasa disebut tanda tangan basah, melainkan tanda tangan yang dibuat secara *digital* atau tanda tangan elektronik. Hal ini membuat tanda tangan elektronik dapat menjadi teknologi yang memberi solusi untuk mengatasi masalah pada masa pandemi COVID-19 ini. Sivitas akademika Universitas Al Azhar Indonesia termasuk Fakultas Sains dan Teknologi harus beradaptasi dan melakukan seluruh kegiatan pendidikan dari rumah masing-masing, sehingga tanda tangan elektronik dapat menghemat waktu serta membuat manusia terhindar dari kontak fisik yang dapat menekan angka penyebaran virus COVID-19. Dalam *sign* dan *verify* tanda tangan elektronik, algoritma SHA-2 merupakan fungsi *hash* satu arah yang mempunyai waktu paling cepat dan baik dalam melakukan proses otentikasi, salah satu varian dari algoritma SHA-2, yaitu SHA-512. Algoritma RSA merupakan algoritma kriptografi kunci publik yang dapat digunakan untuk pembuatan tanda tangan elektronik. Sistem ini dapat memfasilitasi penggunaan tanda tangan elektronik pada dokumen *digital* untuk keperluan internal Universitas Al Azhar Indonesia khususnya Fakultas Sains dan Teknologi.

**Kata kunci:** *Tanda Tangan Elektronik, Universitas Al Azhar Indonesia, Algoritma SHA-2, Algoritma RSA.*

.

## Pendahuluan

Pandemi COVID-19 telah banyak mengubah berbagai aspek kehidupan manusia pada saat ini, terutama pada bidang pendidikan. Pembelajaran *online* merupakan solusi yang efektif untuk tetap membuat kegiatan belajar dan mengajar tetap berjalan, walaupun sekolah dan universitas telah ditutup karena waktu dan tempat yang beresiko selama pandemi berlangsung [1]. Di lingkungan Universitas Al Azhar Indonesia, Rektor Universitas Al Azhar Indonesia telah mengeluarkan Surat Edaran Nomor 02 pada tahun 2021 tentang Pemberlakuan Pembatasan Kegiatan Masyarakat dalam Rangka Pengendalian COVID-19 di Lingkungan Universitas Al Azhar Indonesia [13]. Jika

terdapat kegiatan yang membutuhkan persetujuan atau pengesahan berupa tanda tangan, maka permintaan tanda tangan tersebut juga harus menyesuaikan dengan keadaan yang berlaku.

Pada masa pandemi COVID-19 ini, seiring dengan penggunaan dokumen *digital*, tanda tangan tidak lagi dibuat di atas kertas atau yang biasa disebut tanda tangan basah, melainkan tanda tangan yang dibuat secara *digital* atau tanda tangan elektronik. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi [2]. Hal ini membuat tanda tangan elektronik dapat menjadi teknologi yang memberi solusi untuk mengatasi masalah pada masa pandemi COVID-19 ini. Tanda tangan elektronik menghemat waktu serta membuat manusia terhindar dari kontak fisik yang dapat menekan angka penyebaran virus COVID-19. Walaupun tidak adanya tatap muka, tanda tangan elektronik ini tetap menjadi alat bukti yang sah selama pihak yang bersangkutan sudah membuat kesepakatan [3].

Peneliti telah melakukan penyebaran kuisioner mengenai pengetahuan tanda tangan *digital* kepada sivitas akademika FST UAI yang diisi oleh 37 responden. Hasil dari kuisioner mengatakan bahwa 94,6% mengatakan *scan* tanda tangan merupakan tanda tangan *digital*. Ketika membutuhkan tanda tangan pada dokumen *digital* sebagian besar responden menjawab akan menandatangani dokumen tersebut dengan cara menempelkan *scan* tanda tangan basah pada dokumen *digital*. Saat verifikasi tanda tangan tersebut valid atau tidak sebagian besar responden menjawab hanya mengecek pada tanda tangannya saja. Untuk harapan yang diinginkan responden, seluruh responden berharap dengan adanya sistem yang dapat memfasilitasi kebutuhan tanda tangan *digital* yang dapat diverifikasi keasliannya. Kesimpulan dari kuisioner ini adalah peneliti akan membuat sistem tanda tangan *digital* yang dapat digunakan untuk memenuhi kebutuhan penandatanganan dokumen *digital* di lingkup FST UAI.

Universitas Al Azhar Indonesia sebelumnya telah mencapai peringkat 78 dari 868 Perguruan Tinggi yang ada di dunia dalam acara *UI GreenMetric World University Rankings* [16]. Sistem ini dapat meningkatkan potensi untuk Universitas Al Azhar Indonesia dalam meraih peringkat yang lebih baik dari sebelumnya.

## Tinjauan Pustaka

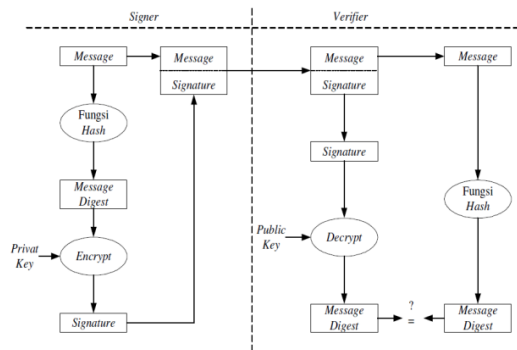
Tanda tangan elektronik secara umum dapat didefinisikan sebagai tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Definisi tersebut sesuai dengan yang tertulis pada Peraturan Pemerintah Nomor 71 tahun 2019 [2].

Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:[2]

- 1) Data Pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan;
- 2) Data Pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan;
- 3) segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;

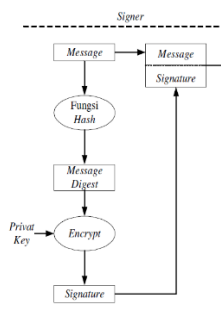
- 4) segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;
- 5) terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penanda Tangannya; dan
- 6) terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

Tanda tangan elektronik secara teknis merupakan suatu nilai kriptografis yang bergantung pada isi berkas *digital* dan kunci pemilik berkas *digital*. Tanda tangan ini dapat diletakkan menjadi satu dengan dokumen atau terpisah dengan dokumen yang ditandatangani. Tanda tangan elektronik tidak sama dengan tanda tangan yang didigitasi dengan *scan* atau foto kemudian ditempel pada dokumen, tanda tangan yang dibuat seperti ini dinamakan *digitized signature* [4]. Berikut merupakan ilustrasi alur pembuatan dan verifikasi tanda tangan elektronik secara garis besar:



Gambar 1. Tahapan pembuatan dan verifikasi tanda tangan elektronik [4]

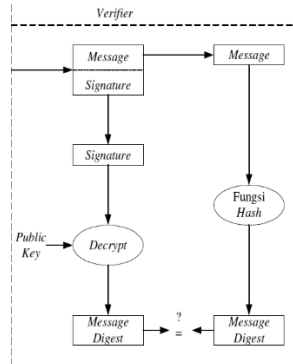
Berikut merupakan ilustrasi pemberian tanda tangan elektronik:



Gambar 2. Proses Pemberian Tanda Tangan [4]

Proses pemberian tanda tangan oleh penanda tangan [4]. Berikut tahapan prosesnya:

- 1) *Message* ditransformasi oleh fungsi *hash* menjadi *message digest*
- 2) *Message digest* dienkripsi menggunakan kunci privat penanda tangan, kemudian diperoleh tanda tangan elektronik
- 3) Tanda tangan elektronik dilekatkan dengan *message* dan siap dikirim ke penerima tanda tangan.

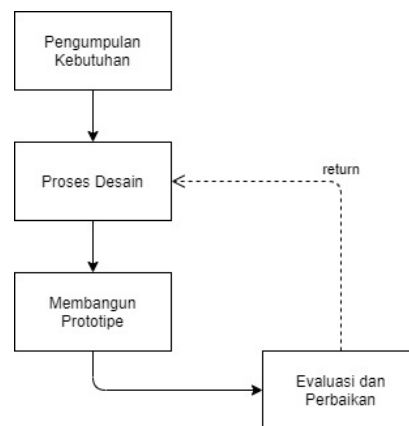


Gambar 2. Proses verifikasi tanda tangan [4]

Proses verifikasi tanda tangan untuk memastikan otentikasi yang dilakukan oleh penerima tanda tangan [4]. Berikut tahapan prosesnya:

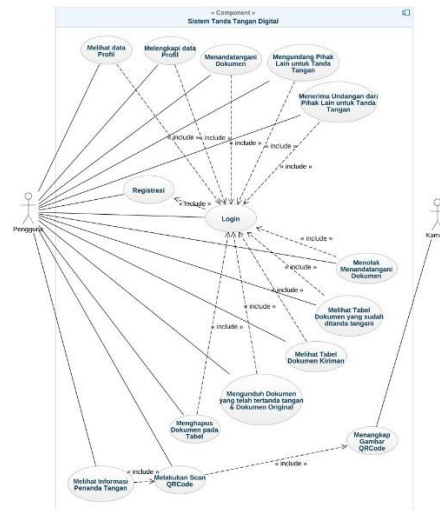
- 1) Penerima tanda tangan telah menerima dokumen dari penandatanganan
- 2) *Message* dan tanda tangan dipisahkan
- 3) *Message* yang telah terpisah dari tanda tangan akan ditransformasi menggunakan fungsi *hash* menjadi *message digest*
- 4) Tanda tangan yang telah terpisah dari *message* akan didekripsi menggunakan kunci publik penanda tangan menjadi *message digest*
- 5) Kedua *message digest* dari *message* dan tanda tangan akan dibandingkan, jika keduanya sama persis, maka *message* yang diterima merupakan *message* asli yang dikirim oleh orang yang sebenarnya

## Metodologi Penelitian



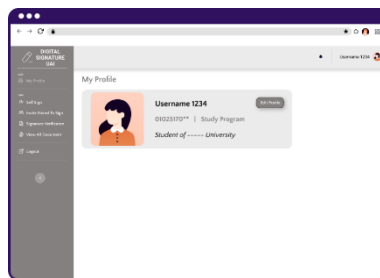
Gambar 4. Tahapan Penelitian

Sistem yang dibuat oleh penulis adalah sistem tanda tangan elektronik. Dalam menampilkan gambaran fungsional sistem dibutuhkan *Use Case Diagram*. Pada *use case* ini terdapat dua aktor, yaitu *user* dan kamera. *User* dapat menggunakan fitur yang ada pada sistem seperti fitur tanda tangan, fitur verifikasi tanda tangan, profil, dan data dokumen. Berikut ini merupakan *use case diagram*.



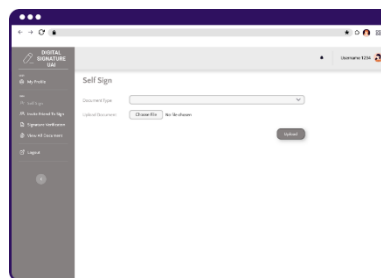
Gambar 5. Usecase Diagram Sistem Tanda Tangan Digital

### Rancangan Antarmuka Halaman Profil Saya



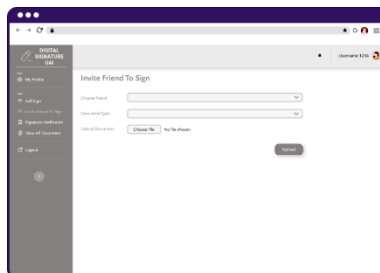
Gambar 6. Rancangan Antarmuka Halaman Profil Saya

### Rancangan Antarmuka Halaman Tandatangani Sendiri



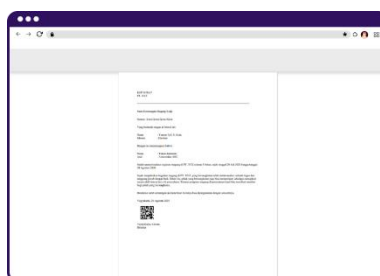
Gambar 7. Rancangan Antarmuka Halaman Tandatangani Sendiri

## Rancangan Antarmuka Halaman Undang Pihak Lain



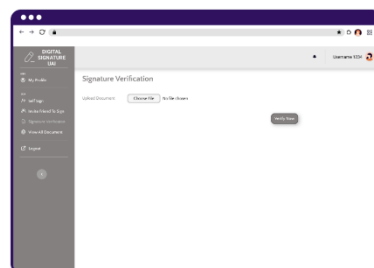
Gambar 8. Rancangan Antarmuka Halaman Undang Pihak Lain

## Rancangan Antarmuka Halaman Signing Process



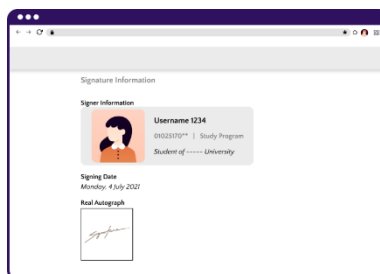
Gambar 9. Rancangan Antarmuka Halaman Signing Process

## Rancangan Antarmuka Halaman Verifikasi Tanda Tangan



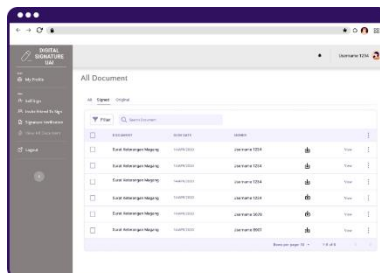
Gambar 10. Rancangan Antarmuka Halaman Verifikasi Tanda Tangan

## Rancangan Antarmuka Halaman Signature Information



Gambar 11. Rancangan Antarmuka Halaman Signature Information

## Rancangan Antarmuka Halaman Dokumen

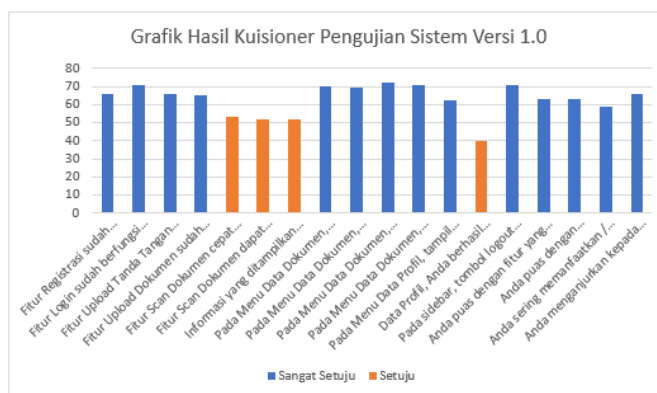


Gambar 12. Rancangan Antarmuka Halaman Dokumen

## Hasil dan Pembahasan

Berdasarkan hasil kuisiner responden setuju sistem tanda tangan *digital* diperlukan pada saat ini, karena responden setuju penggunaan sistem tanda tangan yang ada saat ini dapat berpotensi untuk digunakan ulang dan disalahgunakan, walaupun hampir seluruh responden tidak pernah mengalami penyalahgunaan *scan* tanda tangan. Selain karena dibutuhkan, pekerjaan sehari-hari responden sebagian besar berhubungan dengan dokumen *digital* yang perlu ditandatangani dan seluruh responden setuju bahwa kondisi pandemi COVID-19 mendorong penggunaan dokumen dan tanda tangan *digital* menjadi lebih tinggi.

Berdasarkan hasil kuisiner pada pengalaman penggunaan sistem tanda tangan *digital* versi 1.0, fungsionalitas pada sistem ini sudah cukup baik dengan mendapatkan penilaian paling rendah pada skala Setuju (S). Berikut ini merupakan grafik dari hasil kuisiner pada penilaian pada penggunaan sistem tanda tangan *digital* versi 1.0.



Gambar 13. Grafik Hasil Kuisiner Pengujian Sistem Versi 1.0.

Berdasarkan hasil kuisiner pada pengalaman penggunaan sistem tanda tangan *digital* versi 2.0, fungsionalitas pada sistem ini sudah cukup baik dengan mendapatkan penilaian paling rendah pada skala Sangat Setuju (SS). Berikut ini merupakan grafik dari hasil kuisiner pada penilaian pada penggunaan sistem tanda tangan *digital* versi 2.0.

