Penggunaan Sidik Jari dalam Algoritma RSA sebagai Tanda Tangan Digital

Zain Fathoni
13508079
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If18079@students.if.itb.ac.id

***Abstrak*—Tanda tangan digital (*digital signature*) belakangan ini sudah bukan lagi menjadi suatu hal yang langka. Dewasa ini, hampir seluruh transaksi digital yang dilakukan telah disertai dengan alat bantu verifikasi berupa tanda tangan digital. Algoritma yang digunakan dalam penandatanganan digital ini adalah algoritma kriptografi kunci-publik, yang mempersyaratkan adanya kunci privat yang bersifat rahasia, dan kunci publik yang bersifat umum.**

Namun demikian, karena kunci privat tersebut disimpan dalam sebuah file, maka ada peluang bagi orang lain untuk mengambil kunci privat tersebut dan menyalahgunakannya. Oleh karena itu, dalam makalah ini diusulkan bahwa kunci privat yang digunakan berasal dari hasil pembacaan sidik jari, sehingga tidak perlu lagi disimpan dalam file, dengan harapan dapat mengurangi resiko penyalahgunaan tanda tangan oleh pihak yang tidak bertanggung jawab.

Algoritma yang digunakan dalam mekanisme tanda tangan digital ini adalah algoritma RSA, dengan pembangkitan kunci yang berbeda dengan pembangkitan kunci pada umumnya. Pembangkitan kunci diawali dengan mengetahui bilangan *d* sebagai salah satu kunci privat terlebih dahulu, kemudian baru dibangkitkan bilangan-bilangan lainnya untuk membentuk kunci publiknya. Dengan demikian, dimungkinkan pembangkitan kunci privat dengan menggunakan sidik jari manusia yang notabene sudah demikian adanya dan tidak akan berubah lagi.

Setelah dianalisis lebih lanjut secara teoritis, dapat disimpulkan proses penandatanganan digital dapat ditingkatkan keamanannya dengan menggunakan sidik jari sebagai media penyimpanan kunci privat. Implementasi lebih lanjut dari metode yang diajukan ini masih memerlukan penelitian lanjut yang aktual dan komperehensif, dengan mempertimbangkan aspek kecanggihan teknologi komputasi terkini, kecanggihan dan keringkasan teknologi pembacaan sidik jari, serta kemudahannya untuk diintegrasikan dengan aplikasi penandatanganan digital terkini.

***Kata Kunci*—Tanda Tangan Digital (*Digital Signature*), Kunci Privat, Sidik Jari, Algoritma RSA.**

I. PENDAHULUAN

Internet telah menyumbangkan berbagai kemudahan dan kenyamanan bagi manusia untuk beraktivitas, termasuk di dalamnya adalah dalam bertukar data/dokumen penting. Namun demikian, internet adalah suatu jaringan publik yang tidak terjamin keamanannya.

Saat pengiriman dokumen dilakukan melalui internet, seseorang bisa saja dengan ilegal mengubah isi dokumen tersebut tanpa sepengetahuan pengirim atau penerima. Tanpa fasilitas keamanan yang baik, sang penerima akan menerima dokumen tersebut tanpa mencurigai adanya perubahan. Hal ini dapat memberikan dampak negatif yang signifikan, terlebih apabila dokumen tersebut merupakan dokumen penting yang menyangkut kepentingan banyak orang.

Namun jika pengirim membubuhkan tanda tangan digital pada dokumen itu, penerima dapat merasa yakin bahwa setelah ditandatangani pengirim, dokumen itu tidak ada yang memanipulasi saat dalam perjalanan.

Sifat yang dimiliki oleh tanda tangan digital, yang juga sering disebut dengan *digital signature* adalah [5]:

- ✓ Otentik, tidak dapat/sulit ditulis/ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti, sehingga penanda tangan tidak dapat menyangkal bahwa dulu ia tidak pernah menandatanganinya.
- ✓ Hanya sah untuk suatu dokumen/pesan atau salinannya yang sama persis. Tanda tangan tersebut tidak dapat dipindahkan ke dokumen lainnya, meskipun dokumen lain tersebut hanya berbeda sedikit. Dengan demikian, apabila terjadi perubahan pada isi dokumen tersebut, maka tanda tangan digital dari pesan tersebut tidak lagi sah.
- ✓ Dapat diperiksa dengan mudah, termasuk oleh pihak-pihak yang belum pernah bertatap muka langsung dengan penanda tangan.

Dewasa ini, tanda tangan digital sudah bukan lagi menjadi suatu hal yang langka. Hampir seluruh transaksi digital yang dilakukan telah disertai dengan sistem verifikasi yang memanfaatkan sistem penandatanganan digital ini.

Algoritma yang biasa digunakan dalam sistem penandatanganan digital (*digital signaturing*) ini adalah algoritma kriptografi kunci-publik, di mana pihak penanda tangan memiliki kunci privat yang diperlukan untuk membangkitkan tanda tangan digitalnya, dan pihak yang hendak melakukan verifikasi terhadap tanda tangan digital tersebut perlu memiliki kunci publik untuk dapat memastikan keaslian dokumen tersebut.

Namun demikian, dalam algoritma RSA ini, kunci

publik dan kunci privat merupakan suatu bilangan, dan karena bilangan merupakan sesuatu yang tidak mudah untuk diingat/dihafalkan oleh manusia, maka kunci publik dan kunci privat tersebut biasanya disimpan dalam sebuah file.

Untuk kunci publik, hal tersebut tidak terlalu menjadi masalah, karena memang sifatnya yang terbuka bagi siapapun dan dapat disebarluaskan ke pihak mana pun. Berbeda halnya dengan kunci privat yang bersifat rahasia, dan hanya boleh dimiliki oleh orang yang berwenang untuk memberikan tanda tangan digital tersebut sebagai alat autentifikasi untuk memastikan keaslian suatu dokumen/data penting yang diterbitkan oleh orang tersebut.

Dengan disimpannya kunci privat tersebut dalam sebuah file, maka ada peluang bagi orang lain untuk mengambil kunci privat tersebut dan menyalah-gunakannya. Oleh karena itu, dalam makalah ini diusulkan bahwa kunci privat yang digunakan berasal dari hasil pembacaan sidik jari orang yang bersangkutan, sehingga tidak perlu lagi disimpan dalam file, dengan harapan dapat mengurangi resiko penyalahgunaan tanda tangan oleh pihak yang tidak bertanggung jawab.

II. PRINSIP DASAR

Sebelum melangkah ke solusi yang ditawarkan, penulis akan menjelaskan mengenai penggunaan algoritma RSA yang sering digunakan pada sistem penandatanganan digital, serta sistem biometrik yang akan digunakan untuk membangkitkan data digital dari sidik jari manusia.

A. Algoritma RSA

Algoritma RSA adalah salah satu dari algoritma kunci-publik yang sangat sering digunakan untuk memastikan keaslian suatu data/dokumen digital. Keamanan enkripsi/dekripsi data dari algoritma kriptografi ini terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar. Besarnya bilangan yang digunakan mengakibatkan lambatnya operasi yang melibatkan algoritma RSA ini [1].

Algoritma RSA memiliki besaran-besaran sebagai berikut:

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

Untuk penjelasan lebih lanjut mengenai metode enkripsi dan dekripsi pada algoritma RSA, dapat dilihat pada referensi [1].

B. Sistem Biometrik

Metode identifikasi dan autentifikasi pada seseorang dapat dilakukan dengan menggunakan sidik jari pada *fingerprint reading*, retina mata pada *retina scan*, dsb. Hal ini dilakukan untuk menjaga keamanan suatu hal yang berhubungan dengan orang tersebut. Penggunaan anggota badan sebagai input untuk identifikasi seseorang dalam keamanan disebut juga dengan sistem *biometric*.

Sistem *biometric* adalah studi tentang metode otomatis untuk mengenali manusia berdasarkan satu atau lebih bagian tubuh manusia atau kelakuan dari manusia itu sendiri yang meiliki keunikan. Tujuan utama dari penggunaan sistem *biometric* adalah untuk menjaga keaslian keunikan kunci, karena hampir tidak mungkin pembacaan input sidik jari atau retina orang yang berbeda menghasilkan hasil pembacaan yang sama [3].

Gambar 1. Contoh *Fingerprint Reader*

Penggunaan sistem *biometric* memungkinkan keunikan bagi setiap orang untuk dapat menjaga keamanan suatu hal miliknya, termasuk akun bank. Berangkat dari hal inilah, muncul gagasan untuk menggunakan sidik jari sebagai alat autentifikasi bagi para pengguna ATM, dalam upaya peningkatan keamanan transaksi perbankan yang dilakukan.

Pada makalah ini, tidak ada pembahasan mengenai sistem sensor yang digunakan, karena hal tersebut sudah menyangkut implementasi dari solusi yang diajukan, sehingga membutuhkan penelitian yang lebih mendalam dan komperehensif. Pembahasan hanya terbatas pada pengolahan citra yang diperoleh dalam bentuk gambar digital, untuk selanjutnya dienkripsi untuk kepentingan autentifikasi transaksi perbankan melalui ATM.

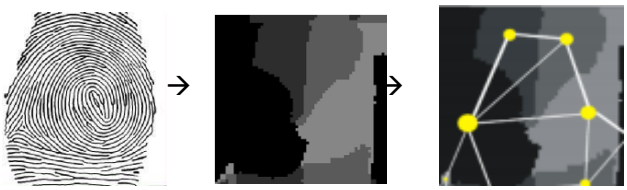
III. RANCANGAN SISTEM

Pada sistem penandatanganan digital dengan menggunakan sidik jari ini, terdapat tiga komponen utama yang memiliki peranan penting. Yakni metode pengolahan citra digital sidik jari dari bentuk gambar ke bentuk digital (kumpulan bit) untuk selanjutnya digunakan sebagai kunci privat, metode pembangkitan kunci publik untuk algoritma RSA dengan sebelumnya telah terlebih dahulu diketahui kunci privatnya, dan skema umum penerapannya untuk kepentingan proses pembubuhan tanda tangan digital beserta proses verifikasinya. Berikut merupakan pembahasan lebih jauh mengenai cara kerja masing-masing komponen tersebut.

A. Konversi dari Citra Sidik Jari ke Kumpulan Bit

Sistem pencitraan sidik jari menghasilkan keluaran berupa citra digital dalam bentuk gambar. Hasil pembacaan sidik jari dari orang yang sama hampir tidak mungkin dapat menghasilkan citra digital yang tepat sama. Oleh karena itu, gambar ini tidak dapat secara langsung dikonversi ke dalam bentuk kumpulan bit dan digunakan sebagai alat autentifikasi pemilik akun bank. Maka diperlukanlah metode lain untuk melakukan konversi dari gambar ke sekumpulan bit, sedemikian sehingga pencitraan sidik jari dari orang yang sama akan menghasilkan kumpulan bit yang sama, dan dapat digunakan sebagai media penyimpanan kunci privat untuk penandatanganan digital.

Salah satu metode yang dapat digunakan yakni mengonversi citra digital tersebut menjadi sebuah graf berbobot terlebih dahulu, dengan masing-masing simpul dan sisi di dalamnya memiliki "bobot" masing-masing. "Bobot" inilah yang nantinya akan dikonversi menjadi sekumpulan bit dan digunakan sebagai alat autentifikasi.



Gambar 2. Proses Konversi dari Hasil Pencitraan Sidik Jari ke Graf Berbobot

Pada gambar di atas, diperlihatkan proses konversi sebuah citra sidik jari menjadi sebuah graf berbobot dengan "bobot" simpul dan sisi yang berbeda-beda. Graf berbobot tersebut didefinisikan sebagai berikut.

$$G = (V, E, \mu, \upsilon)$$

Keterangan: V adalah jumlah simpul, E adalah jumlah sisi, μ adalah bobot simpul, dan υ adalah bobot sisi.

Penentuan bobot dari sebuah simpul dilakukan berdasarkan beberapa parameter: titik tengah gravitasi untuk masing-masing region, jarak antar 2 titik tengah gravitasi, garis batas tiap region, dll. Berikut merupakan rumus yang dapat digunakan untuk mencari bobot dari sebuah simpul (Wn) dengan menggunakan parameter-parameter yang telah disebutkan di atas [3].

$$Wn = Area(Ri), i = 1, 2, 3, \ldots, n$$

Sedangkan untuk bobot dari sebuah sisi, parameter yang dapat digunakan antara lain:

- Adj-p, yakni batas antara 2 region yang bersinggungan atau saling bertetangga.
- Node-d, yakni jarak antarsimpul yang dihubungkan oleh sisi tersebut.
- Diff-v, yakni perbedaan *direction* dari dua region.

Dari ketiga parameter diatas, bobot dari sebuah sisi dapat ditentukan dengan menggunakan rumus berikut [3].

$$We = Adj - p \times Node - d \times Diff - v$$

Detail penurunan dan penggunaan dari kedua persamaan di atas tidak dibahas dalam makalah ini. Dalam bagian ini hanya ditunjukkan bagaimana cara memperoleh kumpulan bit dari gambar hasil pencitraan sidik jari di mesin ATM.

Masing-masing dari kedua persamaan di atas akan menghasilkan suatu himpunan solusi yang berisi bobot dari setiap simpul dan sisi. Salah satu dari kedua himpunan solusi tersebut, baik himpunan bobot simpul maupun himpunan bobot sisi, dapat dikonversi menjadi kumpulan bit yang akan digunakan sebagai alat autentifikasi transaksi perbankan di ATM.

Apabila diasumsikan dari setiap sidik jari dapat diperoleh himpunan solusi bobot simpul dengan banyaknya elemen sekitar 15 – 20 buah dengan tipe data integer, maka data yang nantinya akan dijadikan sebagai kunci privat akan memiliki panjang 15 byte x 8 = 120 bit, atau bahkan dapat mencapai 20 byte x 8 = 160 bit [4].

B. Metode Pembangkitan Kunci Publik untuk Algoritma RSA dari Kunci Privat yang Telah Diperoleh

Proses pembangkitan kunci ini cukup berbeda dengan proses pembangkitan kunci RSA yang biasa dilakukan. Pada umumnya, pembangkitan kunci pada RSA dimulai dengan pencarian 2 bilangan prima di awal, kemudian baru dilakukan beberapa perhitungan yang akhirnya akan menghasilkan bilangan-bilangan untuk kunci publik dan kunci privat [1].

Pada kasus ini, pembangkitan kunci dimulai dengan mengetahui salah satu komponen utama dari kunci privatnya terlebih dahulu (bilangan *d* pada algoritma RSA), kemudian baru dicari kunci publik yang sesuai dengan kunci privat tersebut supaya dapat digunakan sebagai pasangan dalam algoritma RSA untuk keperluan proses penandatanganan digital. Kunci privat diperoleh dari pengolahan hasil pencitraan sidik jari yang telah dijelaskan pada upa-bab di atas.

Berikut merupakan algoritma pembangkitan kunci publik yang diawali dengan diketahuinya bilangan *d* sebagai salah satu komponen utama kunci privat terlebih dahulu:

1. Diketahui bilangan *d* sebagai salah satu komponen kunci privat.
2. Cari φ(*n*) = (*p* - 1)(*q* – 1) yang memenuhi kondisi sebagai berikut:
   - ✓ *p* dan *q* merupakan bilangan prima.
   - ✓ φ(*n*) dan d relatif prima

   Pencarian dilakukan dengan cara membangkitkan bilangan acak prima yang tidak berulang kombinasinya untuk *p* dan *q*, hingga kedua kondisi di atas dapat terpenuhi.
3. Hitung *n*, di mana *n* = *pq*. Untuk memperkuat tingkat keamanan, usahakan nilai *p* berbeda dengan nilai *q*. Apabila kedua bilangan tersebut

sama, maka $n = p^2$, sehingga p dapat dengan mudah diperoleh dengan menarik akar pangkat dua dari nilai n.

4. Bangkitkan kunci publik dengan menggunakan persamaan:

$$ed \equiv 1(mod\ \varphi(n))$$

Perhatikan bahwa persamaan di atas ekivalen dengan persamaan:

$$ed \equiv 1 + k\varphi(n)$$

Dengan demikian, secara sederhana e dapat dihitung dengan

$$e = \frac{(1 + k\varphi(n))}{d}$$

Dengan metode di atas, akhirnya dapat diperoleh bilangan e beserta nilai n yang akan disebarkan sebagai kunci publik, dan dapat digunakan untuk melakukan verifikasi terhadap tanda tangan digital yang dibuat dengan menggunakan sidik jari yang telah diperoleh sebelumnya [2].

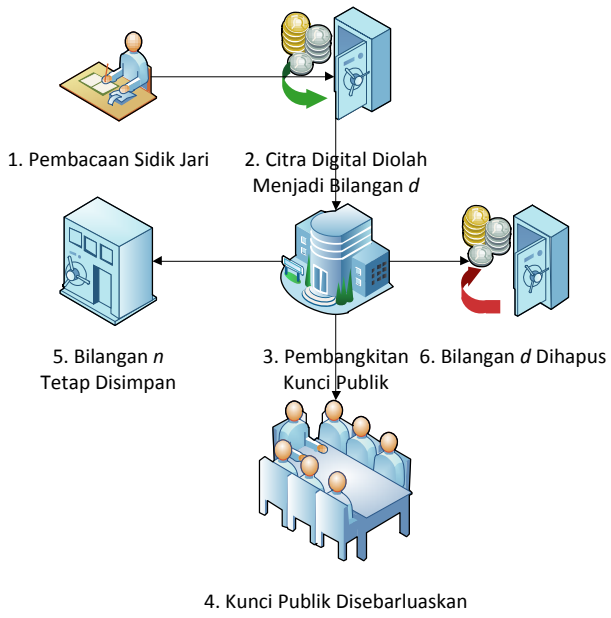
C. Skema Umum Penerapan Proses Pembubuhan Tanda Tangan Digital beserta Proses Verifikasinya

Pada bagian ini akan dijelaskan gambaran umum dari solusi yang ditawarkan, yakni proses pembangkitan kunci publik di awal, pembubuhan sidik jari, serta verifikasi terhadap tanda tangan digital sidik jari ini.

Berikut merupakan proses pembangkitan kunci publik yang akan disebarkan secara luas sebagai alat verifikasi tanda tangan digital tersebut.

1. Penanda tangan melakukan pembacaan sidik jari terlebih dahulu, untuk mendapatkan citra digital dari sidik jarinya.
2. Citra digital tersebut kemudian diolah dengan menggunakan aplikasi, untuk menghasilkan data dalam bentuk kumpulan bit, yang selanjutnya akan digunakan sebagai bilangan *d* pada kunci privat.
3. Dengan berbekal bilangan *d* yang telah diperoleh sebelumnya, aplikasi melakukan proses pembangkitan kunci publik menggunakan algoritma yang telah dijelaskan pada upa-bab di atas.
4. Kunci publik yang telah diperoleh dapat disebarluaskan sebagai alat verifikasi tanda tangan digital tersebut.
5. Bilangan *n* tetap disimpan oleh aplikasi sebagai komponen pelengkap kunci privat.
6. Bilangan *d* yang diperoleh dari hasil pengolahan sidik jari tersebut dihapus kembali, untuk tetap menjaga kerahasiaan kunci publik.

Demikianlah proses pembangkitan kunci publik yang perlu dilakukan di awal. Langkah-langkah di atas dapat digambarkan dengan diagram alir sebagai berikut.

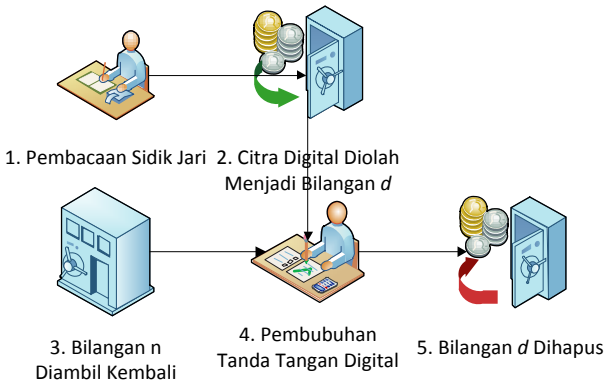


Gambar 3. Proses Pembangkitan Kunci Publik

Selanjutnya akan dijabarkan proses pembubuhan sidik jari sebagai tanda tangan digital.

1. Penanda tangan melakukan pembacaan sidik jari terlebih dahulu, untuk mendapatkan citra digital dari sidik jarinya.
2. Citra digital tersebut kemudian diolah dengan menggunakan aplikasi, untuk menghasilkan data dalam bentuk kumpulan bit, yang selanjutnya akan digunakan sebagai bilangan *d* pada kunci privat.
3. Bilangan *n* yang disimpan oleh aplikasi dipanggil kembali
4. Bilangan *n* tersebut kemudian digabungkan dengan bilangan *d* dan digunakan untuk melakukan proses pembubuhan tanda tangan digital, yakni sebagai kunci privat.
5. Setelah tanda tangan digital selesai dibubuhkan pada dokumen yang bersangkutan, bilangan *d* yang diperoleh dari hasil pengolahan sidik jari tersebut dihapus kembali, untuk tetap menjaga kerahasiaan kunci publik.

Untuk lebih jelasnya, prosedur di atas dapat dilihat pada gambar berikut.



Gambar 4. Proses Pembubuhan Tanda Tangan Digital

Demikian merupakan proses pembangkitan kunci publik di awal, serta proses pembubuhan tanda tangan digital dengan menggunakan sidik jari. Untuk proses verifikasi terhadap tanda tangan digital yang telah dibubuhkan tersebut, secara umum praktis sama sekali tidak berbeda dengan proses verifikasi tanda tangan digital pada umumnya.

Untuk dapat melakukan proses verifikasi tanda tangan digital ini, pihak yang memiliki kepentingan untuk melakukan verifikasi terhadap dokumen yang bersangkutan telah memiliki komponen-komponen yang cukup untuk dapat melakukan verifikasi tanda tangan digital, yakni dokumen yang telah ditandatangani, beserta kunci publik yang telah disebarluaskan sebelumnya oleh pihak penanda tangan dokumen. Oleh karena itu, tidak diperlukan tambahan mekanisme khusus di luar proses verifikasi tanda tangan digital seperti yang biasa dilakukan pada umumnya.

Alih-alih menyoroti proses verifikasi tanda tangan digital ini, hal lain yang cukup penting untuk dicermati lebih lanjut adalah adanya alat bantu tambahan yang diperlukan untuk dapat menjalankan kedua proses sebelumnya, yakni pembangkitan kunci publik dan pembubuhan tanda tangan digital dari sidik jari penanda tangan.

Dari kedua proses sebelumnya, kita menemukan adanya langkah pembacaan sidik jari dan pengolahan sidik jari menjadi kumpulan bit. Kedua langkah tersebut menuntut adanya tambahan perangkat untuk dapat menjalankan metode penandatanganan digital ini, yakni alat pembaca sidik jari atau *fingerprint reader* seperti yang ditampilkan di Gambar 2, serta aplikasi pendukung yang dapat mengolah hasil pencitraan sidik jari menjadi kumpulan bit.

Untuk dapat menjalankan fungsinya, aplikasi pendukung tersebut memiliki kebutuhan yang sama dengan aplikasi dasar penanda tangan digital, yakni menyimpan dan membaca bilangan n sebagai salah satu komponen pada kunci privat. Oleh karena itu, alangkah baiknya apabila aplikasi pendukung ini dapat diintegrasikan dengan aplikasi pembubuh tanda tangan digital beserta verifikasinya.

Demikian gambaran umum dari solusi yang ditawarkan oleh penulis, mengenai proses dan metode penandatanganan digital dengan menggunakan sidik jari sebagai kunci privat.

IV. ANALISIS

Penggunaan sidik jari sebagai pengganti file untuk menyimpan kunci privat ini merupakan suatu usulan baru yang perlu dipertimbangkan lebih jauh lagi. Terlebih dalam makalah ini aspek fisibilitas imlplementasi masih belum dipertimbangkan. Oleh karena itu, masih perlu penelitian lebih lanjut yang komperehensif untuk memastikan keberhasilan sistem yang ditawarkan ini.

Berikut akan penulis paparkan kelebihan dan kekurangan dari solusi yang ditawarkan pada makalah ini. Berhubung pembahasan pada makalah ini hanya mencakup penjelasan teoritis mengenai penerapan penandatanganan digital dengan menggunakan sidik jari, maka penjelasan mengenai kelebihan dan kekurangan di bawah ini cukup sekedar aspek-aspek yang dapat dinalar secara teoritis, tanpa disertai dengan pembuktian lapangan yang memadai.

A. Kelebihan

Berikut merupakan kelebihan dari solusi yang ditawarkan:

1. Penanda tangan dapat membubuhkan tanda tangan tanpa perlu menyimpan file kunci privat yang notabene cukup rentan untuk diambil/disalin oleh orang lain, dan dapat disalahgunakan. Dengan digunakannya sidik jari sebagai media penyimpan kunci privat, maka kemungkinan terjadinya hal tersebut dapat ditekan seminimal mungkin, karena penanda tangan tidak perlu lagi menyimpan file kunci privat yang rentan disalin tanpa sepengetahuannya.
2. Proses penandatanganan terasa natural bagi penanda tangan, karena dilakukan dengan menggunakan sidik jari. Ini sama halnya seperti dokumen *hardcopy* pada umumnya yang juga dapat ditandatangani dengan menggunakan sidik jari.

B. Kekurangan

Berikut merupakan kekurangan dari solusi yang ditawarkan:

1. Secara umum algoritma RSA hanya aman jika *n* cukup besar [1], sedangkan bilangan *n* sendiri diperoleh dari pembangkitkan dua bilangan acak prima yang harus memenuhi persyaratan "$\varphi(n)$ dan *d* relatif prima". Karena nilai *d* sudah ditentukan di awal, sehingga pembangkitan acak kedua bilangan prima tersebut memiliki batasan tertentu. Hal ini menuntut kemampuan proses komputasi yang cukup tinggi untuk melakukan pembangkitan kunci publik.

2. Di samping menawarkan kemudahan yang telah disebutkan di atas, metode ini juga menimbulkan kerumitan tersendiri. Untuk dapat menggunakan metode ini, penanda tangan harus memiliki alat pembaca sidik jari yang terhubung dengan komputer, dan dapat dengan mudah diintegrasikan dengan aplikasi penanda tangan digital. Sedangkan saat ini kebanyakan alat pembaca sidik jari yang ringkas hanya dapat ditemukan pada beberapa jenis komputer jinjing (*laptop*). Selain penyediaan perangkat tambahan tersebut, kerumitan juga dapat berupa proses menandatangani yang terasa dipersulit, karena tidak dapat hanya dilakukan dengan menggunakan alat bantu *mouse* seperti pada proses penandatanganan digital pada umumnya.
3. Kemungkinan terjadi kesalahan dalam pembacaan sidik jari cukup besar, sehingga belum tentu pembacaan sidik jari dari orang yang sama dapat menghasilkan citra sidik jari yang sama. Kemungkinan galat hasil pembacaan sidik jari yang terjadi cukup besar, dan apabila ini terjadi, maka penandatanganan digital dengan menggunakan sidik jari ini justru mempersulit pengguna (baik pihak penanda tangan maupun pihak yang melakukan verifikasi) dalam proses penandatanganan digital.

IV. KESIMPULAN

1. Proses penandatanganan digital dapat ditingkatkan keamanannya dengan menggunakan sidik jari sebagai media penyimpanan kunci privat.
2. Implementasi lebih lanjut dari metode yang diajukan ini masih memerlukan penelitian lanjut yang aktual dan komperehensif, dengan mempertimbangkan aspek kecanggihan teknologi komputasi terkini, kecanggihan dan keringkasan teknologi pembacaan sidik jari, serta kemudahannya untuk diintegrasikan dengan aplikasi penandatanganan digital terkini.

REFERENSI

[1] Munir, Rinaldi. Slide kuliah IF3058 Kriptografi. Program Studi Teknik Informatika STEI ITB. 2010.

[2] Muntaha, Amir. Tugas Makalah Kriptografi: Studi Pembangkitan Kunci pada RSA dengan Menggunakan Sidik Jari. Program Studi Teknik Informatika STEI ITB. 2009.

[3] Darusman, Amalfi Yusri. Tugas Makalah 1: Algoritma Kriptografi Klasik Berbasis Pencitraan Sidik Jari. Program Studi Teknik Informatika STEI ITB. 2010.

[4] Fathoni, Zain. Tugas Makalah 1 Kriptografi: Penggunaan Autentifikasi Sidik Jari untuk Pengamanan Transaksi ATM (Automated Teller Machine). Program Studi Teknik Informatika STEI ITB. 2011.

[5] http://www.google.co.id/url?sa=t&source=web&cd=6&ved=0CEQQFjAF&url=http%3A%2F%2Fkambing.ui.ac.id%2Fbebas%2Fv09%2Fonno-ind-1%2Fnetwork%2Fnetwork-security%2Ftanda-tangan-digital-sertifikat-digital-apa%2520itu-06-1998.rtf&rct=j&q=tanda%20tangan%20digital&ei=WPXGTdrNNs-urAeNqc3NBA&usg=AFQjCNGHDmvCIbd3K275fTGgU8mrm07pQQ&cad=rja
Diakses pada tanggal 8 Mei 2011, Pukul 22.01

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 9 Mei 2011

Zain Fathoni
13508079