Penggunaan *Fingerprint Authentication Key* untuk MAC Pada Kartu Tanda Pengenal Berbasis *Smart Card*

Dimas Aditiya Nurahman-13508093
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18093@students.if.itb.ac.id

Abstraksi— Sebagaimana kita ketahui tanda pengenal zaman sekarang ini sudah menggunakan sistem digital. Sistem kartu tanda pengenal ini biasa kita kenal dengan *smart card*. Penggunaan sistem ini tentunya dikarenakan untuk memudahkan proses autentikasi dan validasi dari pemilik kartu tersebut. Selain itu dengan adanya sistem digital ini juga memudahkan dalam proses pengolahan data. Salah satu kekurangan dari penggunaan sistem digital ini adalah data dari autentikasi tersebut dapat dimanipulasi apabila tidak menggunakan atau tidak didukung dengan sistem keamanan yang kuat. Hal ini dibuktikan oleh maraknya pemalsuan kartu tanda pengenal yang dilakukan oleh pihak-pihak yang tidak berwenang. Mengangkat masalah tersebut, makalah ini akan membahas bagaimana cara untuk meningkatkan keamanan dari sistem keamanan pada *smart card* dengan cara menggunakan metode kriptografi. Metode yang diusulkan kali ini adalah metode MAC atau kita kenal dengan *Message Authentication Code*. MAC merupakan fungsi *hash* satu arah namun menggunakan suatu *key* dalam proses *digest* pada pesan. Adapun penggunaan kunci yang diusulkan di sini adalah penggunaan sidik jari atau *fingerprint* karena sifatnya yang unik.

Kata Kunci— MAC, *smart card, fingerprint*

I. PENDAHULUAN

Dewasa ini, penggunaan kartu tanda pengenal digital sudah tidak asing lagi, bahkan hampir semua menggunakannya. Pada umumnya perbedaan kartu tanda pengenal digital dengan kartu tanda pengenal biasa terletak pada penggunaan *chip* yang digunakan untuk menyimpan data. Penggunaan kartu tanda pengenal digital ini tentu saja dikarenakan tingkat keamanan yang lebih terjamin serta menyediakan kemudahan dalam pengolahan data. Agar data yang didimpan dalam *chip* tersebut aman dan hanya dapat diakses oleh pihak yang berwenang maka diperlukan suatu metode pengemanan. Salah satu metode keamanan yang dapat digunakan pada kasus seperti ini adalah penggunaan metode kriptografi.

Berdasarkan pemaparan di atas, pada dasarnya banyak algoritma kriptografi yang digunakan pada kasus tersebut. Namun makalah ini akan membahas penggunaan metode MAC (*Message Authentication Code*) dimana merupakan suatu metode kriptografi yang akan melakukan *message digest* pada pesan yang diinginkan menggunakan suatu kunci. MAC merupakan salah satu fungsi hash yang sifatnya digunakan untuk autentifikasi seperti dalam kegiatan berkirim pesan juga untuk melakukan integrasi dan validasi dari suatu file apakah valid atau tidak. MAC digunakan karena menggunakan kunci untuk melakukan fungsi hash, apabila suatu file ditandai dengan menggunakan fungsi hash biasa maka dapat timbul ancaman dari virus yang dapat mengubah isi hash dengan cara melakukan *brute force* pemetaan *string*. Namun hal ini dapat diatasi dengan menggunakan MAC karena virus tidak mengetahui kunci yang digunakan.

Penggunaan metode MAC tersebut pada kasus kartu tanda pengenal berbasis *smart card* adalah bagaimana pemilik *smart card* diautentikasi apakah kartu yang dibawa tersebut adalah miliknya atau bukan dengan cara melakukan pencocokan autentifikasi MAC dengan menggunakan sidik jari sebagai kunci. Apabila hasil hash dari MAC cocok dengan kunci sidik jari orang tersebut maka dia merupakan pemilik kartu tanda pengenal yang sebenarnya. Konsep ini juga dapat digunakan untuk mencegah penggandaan yang ada pada kartu tanda pengenal seperti manipulasi KTP misalnya. Untuk kasus seperti KTP yang digunakan oleh banyak orang maka akan dibuat sistem database pusat yang menyimpan semua data. Untuk setiap penduduk yang ingin membuat

kartu tanda pengenal akan dicocokkan di database, apabila belum terdapat informasi mengenai dirinya maka kartu tanda pengenal dapat dibuat.

Dari segi teknis, data yang berasal dari sidik jari akan dikonversi ke dalam array of byte, selanjutnya akan digenerasi sebuah kunci dari array of byte tersebut. Mengenai konversi data dari sidik jari ke array of byte, dapt digunakan bantuan dari fungsi hash satu arah seperti SHA-1 atau MD5 yang akan di-*digest* ke dalam array of byte tersebut. Metode ini merupakan salah satu tambahan atau modifikasi yang dapat digunakan untuk MAC dalam menggunakan kunci yang juga akan di-*hash* menggunakan fungsi *hash* lainnya

II. LANDASAN TORI

A. *Smart Card*

Smart card adalah kartu berukuran saku yang memiliki IC atau *integrated circuit* didalamnya. Ada dua kategori besar *smart card* yaitu

- Memory cards, merupakan kartu yang hanya berisi komponen *non-volatile storage memory*.
- Microprocessor cards, yang berisi *volatile memory* dan *microprocessor components.*

Gambar 1. Ilustrasi *chip smart card*

Bagian internal kartu memori mikroprosesor seperti halnya komputer mini yang mencakup: RAM - penyimpanan sementara di mana prosesor melakukan perhitungan; ROM - memori permanen yang merupakan tempat sistem operasi untuk *smart card*; dan EEPROM (*Electrically Erasable Programmable Read Only Memory*) - memori yang dapat ditulis ulang untuk data aplikasi (termasuk juga kode).

Pada umumnya *smart card* terbuat dari plastik, polyvinyl chloride, tapi kadang-kadang Acrylonitrile Butadiene stirena atau polikarbonat . *Smart card* Juga biasa digunakan untuk menyediakan keamanan yang kuat otentikasi untuk *single sign-on* (SSO) dalam organisasi besar.

Kartu *Smart* ini dapat digunakan untuk memberikan identifikasi, autentikasi, penyimpanan data dan pengolahan aplikasi. Manfaat dari kartu ini secara langsung berkaitan dengan volume informasi dan aplikasi yang diprogram untuk digunakan pada kartu. Informasi ini dapat digunakan untuk tujuan yang bermacam-macam. Pada kasus yang dibahas pada makalah ini, *smart card* digunakan sebagai pengolahan dan penyimpanan data informasi dari seseorang. Karena *smart card* yang dimaksuda adalah *smart card* identitas seseorang. Jenisnya dapat bermacam-macam seperti untuk SIM, KTP, kartu ATM, kartu keanggotaan suatu perusahaan, dan lain-lain.

Informasi yang disimpan dalam *chip smart card* akan diamankan menggunakan proses enkripsi untuk mencegah adanya manipulasi dari pihak yang tidak berwenang. Oleh karena itu peningkatan keamanan dari data yang disimpan ditawarkan oleh penggunaan *smart card* Penggunaan *smart card* dirancang untuk interoperabilitas antara layanan. Sebagai contoh, pengguna hanya perlu mengganti satu kartu jika dompet mereka hilang atau dicuri. Selain itu, penyimpanan data akan tetap aman dan kartu penting seperti ATM tetap tidak dapat digunakan oleh si pencuri karena informasi autentikasi di dalam *chip smart card* telah dienkripsi.

Aplikasi kriptografi yang umum digunakan pada *smart card* adalah *Single sign-on* (SSO). Kebanyakan *smart card* dirancang khusus dengan perangkat keras canggih termasuk kriptografi yang menggunakan –algoritma tertentu. *Smart card* tersebut terutama digunakan untuk tanda tangan digital dan identifikasi kepemilikan kartu ketika kartu tersebut digunakan untuk mengakses sesuatu yang penting.

Single sign-on (SSO) adalah properti atau akses kontrol yang terkait dengan beberapa sistem perangkat lunak independen. Dengan properti ini pengguna hanya dapat login. *Single-off* adalah properti kebalikan dimana tindakan tunggal *sign out* dari keberakhiran akses ke sistem dari beberapa perangkat lunak. Jika aplikasi yang berbeda dan sumber daya yang mendukung mekanisme autentikasi ini akan menjamin dari segi keamanan pada kasus pengguna atau *user* yang melakukan proses *sign in* ke dalam sistem yang sama dari tempat yang berbeda secara bersamaan.

B. MAC

MAC atau *Message Authentication Code* adalah fungsi satu-arah yang menggunakan kunci rahasia (*secret key*) dalam pembangkitan nilai *hash.* Berbeda dengan fungsi *hash* lainnya seperti MD5 dan SHA tidak perlu menggunakan kunci untuk menghasilkan *message digest*. Nilai hash yang dihasilkan selalu berukuran tetap (*fixed*) untuk ukuran pesan berapa saja *MAC* dilekatkan (*embed*) pada pesan. Selanjutnya, *MAC* digunakan untuk otentikasi tanpa perlu merahasiakan pesan. MAC bukanlah tanda-tangan digital. MAC hanya menyediakan otentikasi pengirim dan integritas pesan saja. Otentikasi arsip yang digunakan oleh dua atau lebih pengguna MAC berguna untuk memvalidasi apakah suatu informasi atau pun data terjaga keasliannya atau tidak melalui suatu kunci.

MAC secara matematis:

$$MAC = C_K(M)$$

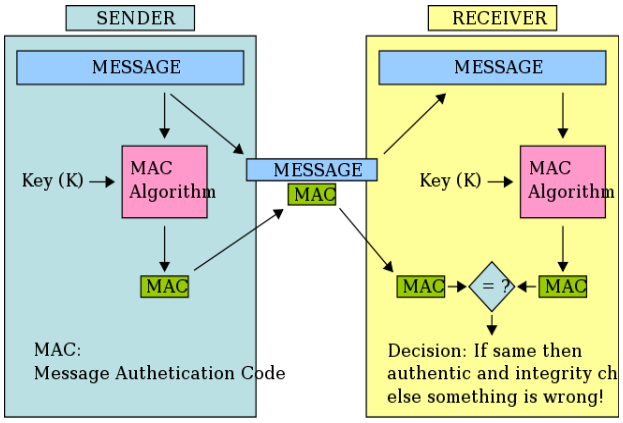
MAC = nilai *hash*
C = fungsi *hash* (atau algoritma *MAC*)
K = kunci rahasia

MAC ini akan menjaga integritas (keaslian) isi arsip terhadap perubahan, misalnya karena serangan virus.Caranya sbb:

- Hitung nilai *MAC* dari suatu arsip atau data informasi.
- Simpan hasil *MAC* di dalam sebuah tabel atau *database* informasi data.

Jika pengguna menggunakan fungsi *hash* satu-arah biasa (seperti *MD5*), maka virus dapat menghitung nilai *hash* yang baru dari arsip yang sudah diubah, lalu mengganti nilai *hash* yang lama di dalam tabel. Tetapi, jika digunakan *MAC*, virus tidak dapat melakukan hal ini karena ia tidak mengetahui kunci. Hal ini menjadi salah satu kelebihan *MAC* dari fungsi *hash* yang lainnya.Fungsi *hash* seperti *MD5* dapat digunakan sebagai *MAC*. Caranya:

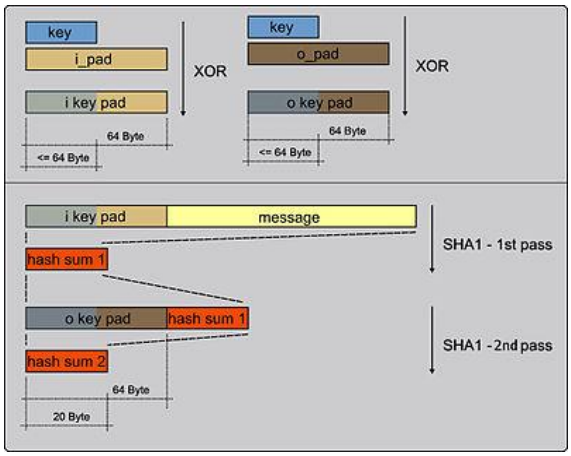
- Misalkan *A* dan *B* akan bertukar pesan. *A* dan *B* berbagi sebuah kunci rahasia *K*.
- *A* menyambung (*concate*) pesan *M* dengan *K*, lalu menghitung nilai *hash* dari hasil penyambungan itu *H*(*M*, *K*)
- Nilai *hash* ini adalah *MAC* dari pesan tersebut. *A* lalu mengirim *M* dan *MAC* kepada *B*.
- *B* dapat melakukan otentikasi terhadap pesan karena ia mengetahui kunci *K*.



Gambar 2. Ilustrasi bertukar pesan menggunakan MAC

Fungsi MAC yang menggunakan *secret key* ini dapat dimodifikasi menggunakan algoritma *hash* yang lainnya. Dalam kriptografi , HMAC (Hash Message berbasis Authentication Code) adalah sebuah konstruksi khusus untuk menghitung kode otentikasi pesan (MAC) yang melibatkan fungsi hash kriptografi dalam kombinasi dengan rahasia kunci. Setiap fungsi hash kriptografi, seperti MD5 atau SHA-1 , dapat digunakan dalam perhitungan HMAC, algoritma MAC yang dihasilkan disebut HMAC-MD5 atau HMAC-SHA1 sesuai. Kekuatan kriptografi dari HMAC tergantung pada kekuatan kriptografi fungsi hash yang mendasari, ukuran panjang output hash dalam bit dan pada ukuran dan kualitas kunci kriptografi.

Sebuah fungsi *hash* iterative akan memecah pesan menjadi blok ukuran. Sebagai contoh, MD5 dan SHA-1 beroperasi di blok 512-bit. Ukuran output dari HMAC adalah sama dengan fungsi hash yang mendasari (128 atau 160 bit dalam kasus MD5 atau SHA-1, masing-masing).



Gambar 3. *Padding block* pada HMAC

C. Fingerprint Biometric

Biometrik merupakan metode untuk mengenali manusia berdasarkan satu atau lebih intrinsik fisik atau perilaku sifat. Dalam ilmu komputer , banyak digunakan untuk melakukan bentuk akses pengelolaan identitas dan akses kontrol Pada umumnya karakteristik dari Biometric terbagi menjadi dua kelas yaitu

- Fisiologis berhubungan dengan bentuk tubuh. Contohnya adalah sidik jari namun tidak terbatas pada sidik jari, contoh lainnya adalah pengenalan wajah , DNA , retina, dan lain-lain.
- Perilaku berkaitan dengan perilaku seseorang. Contoh irama mengetik , dan suara . Beberapa peneliti telah menciptakan istilah behaviometrics istilah untuk kelas *Biometrics* ini.

Adapun parameter yang digunakan dalam hal penentuan karakteristik *biometric* manusia:

- Universalitas - setiap orang harus memiliki karakteristik.
- Keunikan - adalah seberapa baik *Biometric* yang dimaksud memisahkan individu yang satu dari yang lain.
- Permanen - Mengukur seberapa baik suatu *Biometric* menolak penuaan dan varians lainnya dari waktu ke waktu.
- Kolektibilitas - Kemudahan akuisisi untuk pengukuran.
- Kinerja - akurasi, kecepatan, dan ketahanan teknologi yang digunakan.

- Akseptabilitas - derajat atau persetujuan dari teknologi.
- Pengelakan - Kemudahan penggunaan pengganti.

Sebuah sistem Biometric dapat beroperasi dalam 2 metode yaitu

- Verifikasi, perbandingan informasi yang diambil dari *Biometric* dengan *template* yang dalam kasus makalah ini adalah nilai dari MAC yang disimpan untuk memverifikasi bahwa individu tersebut adalah individu yang sesuai dengan data komparasi. Data komparasi ini merupakan bentuk validasi apakah pembawa *smart card* adalah orang yang benar-benar memilikinya. Informasi ini disesuaikan dengan data seperti ID, *username*, dan lain-lain.
- Identifikasi, perbandingan informasi yang diambil dari *Biometric* dengan *template* yang dalam kasus ini adalah *database* terpusat dalam upaya untuk validasi identifikasi individu. Proses ini hanya berhasil mengidentifikasi individu jika perbandingan sampel *Biometric* untuk *template* dalam database cocok atau sesuai dengan nilai MAC.

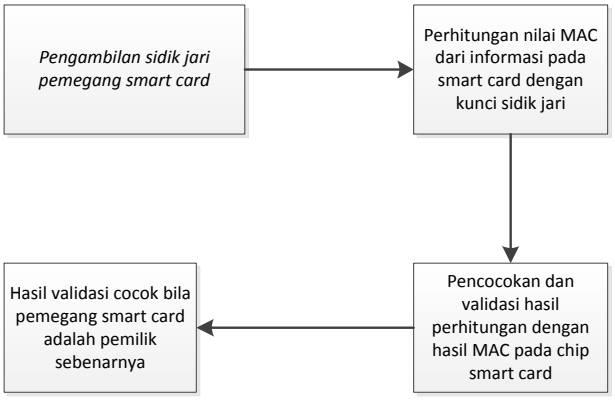
Pertama kali seseorang menggunakan sistem *Biometric* disebut sebuah *enrollment.* Pada proses ini data dari *biometric fingerprint* dikumpulkan untuk dapat digunakan selanjutnya, informasi *Biometric* yang terdeteksi akan dibandingkan dengan informasi yang tersimpan pada saat proses *enrollment* ini. Perhatikan bahwa sangat penting proses penyimpanan dan pengambilan data *biometric* pada sistem. Agar pengambilan atau penyimpanan data ini aman, diperlukan sistem *biometric* yang kuat.Dalam kasus *fingerprint biometric,* sebagian besar waktu digunakan sistem untuk akuisisi gambar. Data yang dikumpulkan haruslah akurat karena perbedaan untuk beberapa kasus dapat mengakibatkan hasil validasi yang tidak sesuai. Pada proses *enrollment* atau pun pengumpulan data *biometric,* data yang didapat akan diolah menggunakan fungsi MAC sebagai kunci. Penggunaan sidik jari sebagai kunci tentu saja dikarenakan sifatnya yang unik.

III. METODE

Sebagaimana pemaparan pada bagian landasan teori, sistem *biometric* yang dalam kasus ini adalah *biometric fingerprint,* dapat diterapkan pada 2 metode yaitu metode verifikasi yang melakukan pencocokan nilai hasil MAC menggunakan *biometric fingerprint* dengan informasi yang tertera pada *smart card* dan metode identifikasi yang melakukan pencocokan pada tabel *database* sistem dari hasil nilai MAC tersebut.

Pada dasarnya data yang disimpan dalam *chip* dapat bervariasi mulai dari *username, ID,* tanggal lahir dan data lainnya. Yang terpenting adalah informasi *biometric* yang akan digunakan untuk melakukan fungsi *hash* bersamaan dengan data tersebut. Memori mikroprosesor *smart card* lebih kompleks daripada kartu tradisional. Semua akses ke memori kartu akan dan harus melewati mikroprosesor. Selain itu, mikroprosesor dapat mendukung perlindungan nomor PIN misalnya dan fitur keamanan lainnya. Kecanggihan dari teknologi inilah yang akan digunakan untuk mengamankan informasi yang ada pada pemilik kartu.

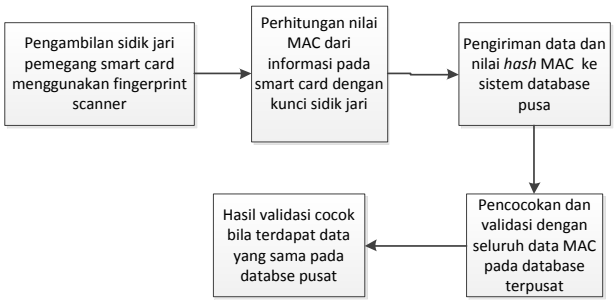
Pada metode verifikasi, chip pada *smart card* akan menyimpan informasi dari pemilik kartu beserta nilai dari MAC-nya menggunakan kunci sidik jari si pemilik kartu pada saat proses awal pembuatan kartu. Proses pembuatan kartu akan menggunakan metode identifikasi yang akan dijelaskan kemudian. Untuk melakukan pengecekan apakah pembawa *smart card* yang dimaksud adalah orang yang sebenarnya atau bukan dapat dilakukan dengan cara mengambil data sidik jari orang tersebut menggunakan *fingerprint scanner* digital, kemudian data informasi di dalam kartu akan di *hash* menggunakan prinsip bantuan HMAC yang sudah dijelaskan pada bagian teori. Pesan yang di-*hash* ditambah dengan nilai *hash*-nya akan dibandingkan dengan data yang terdapat pada *chip smart card.* Karena menggunakan sidik jari sebagai kunci, maka untuk setiap orang yang berbeda akan menghasilkan nilai *hash* yang berbeda pula. Apabila hasil keduanya cocok maka pembawa *smart card* tersebut adalah pemilik sebenarnya begitu juga sebaliknya. Berikut skema dari mekanisme yang dijelaskan



Gambar 4. Skema metode verifikasi

Metode kedua yaitu metode identifikasi. Dalam pembuatan kartu tanda pengenal seperti KTP misalnya tidak mungkin ada kasus dimana 1 orang dapat memiliki KTP dengan identitas ganda. Oleh karena itu setiap orang yang melakukan pembuatan kartu tanda pengenal akan dicatat dalam *database* terpusat untuk kemudian dibandingkan ketika adanya proses pembuatan kartu tanda pengenal yang baru. Hal ini untuk mencegah adanya pembuatan kartu tanda pengenal dengan identitas ganda.Karena menggunakan MAC maka salah satu keuntungannya dalam kasus ini adalah manipulasi *database* oleh pihak yang tidak berwenang karena seperti yang dipaparkan pada sub pokok bahasan sebelumnya yaitu landasan teori, MAC dapat mengantisipasi serangan

virus. Adapun ilustrasi atau skema dari metode identifikasi adalah sebagai berikut.



Gambar 5. Skema metode identifikasi

IV. PENGUJIAN

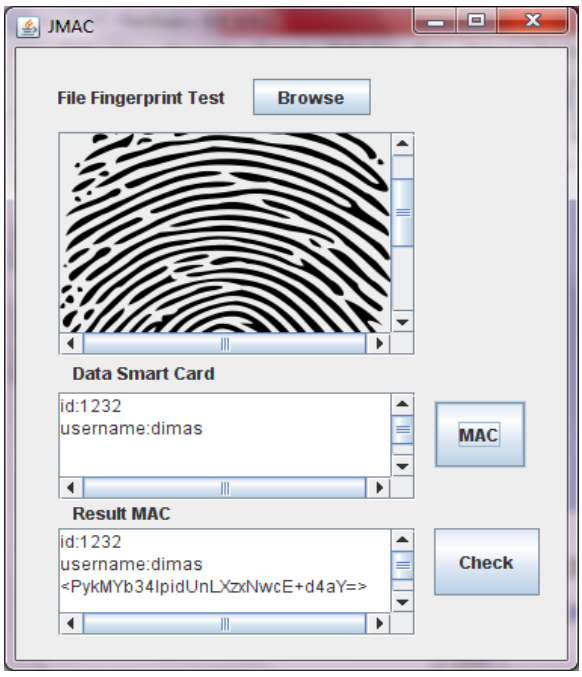
Pada bagian ini, pembuat makalah akan mencoba untuk melakukan pengujian menggunakan aplikasi *desktop* yang dibuat menggunakan bahasa java dengan IDE Netbeans. Adapun kasus yang diuji adalah melakukan *generate* kunci yang berasal dari *array of byte* yang dalam pengujian ini diasumsikan sebagai kumpulan *byte* gambar dari sidik jari pengguna. *Array of byte* ini tidak langsung digunakan, melainkan akan dilakukan *hash* terlebih dahulu menggunakan fungsi *hash* 1 arah SHA-1. Hal ini dilakukan untuk mendapatkan ukuran *byte* kunci *Generate* kunci dilakukan menggunakan lib yang ada pada java sedangkan fungsi *hash* dilakukan menggunakan bantuan HMAC SHA-1.

Kasus yang akan diuji di sini adalah dengan mengganti nilai *array of byte* dari setiap data tes. Hal ini untuk membuktikan bahwa fungsi *hash* MAC pada implementasi ini akurat untuk perubahan yang sedikit sekalipun. *Pseudocode* dari HMAC SHA-1 adalah sebagai berikut.

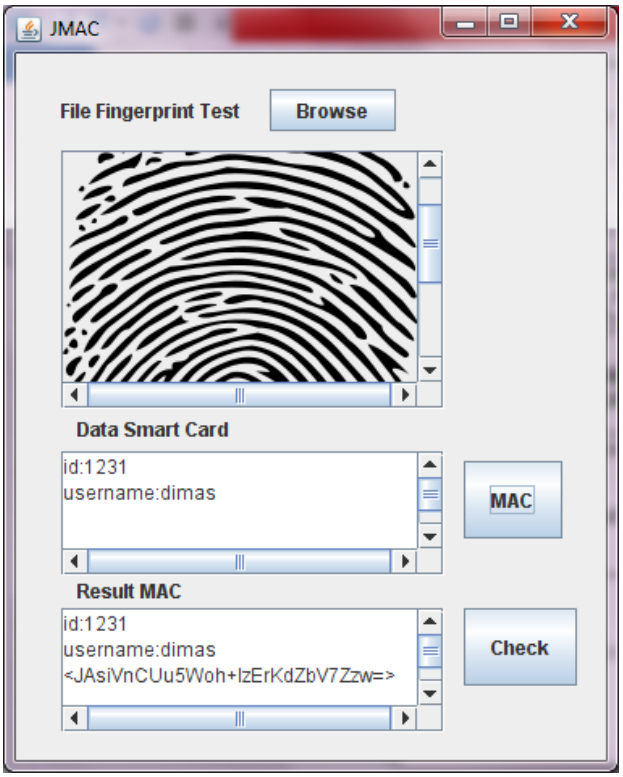
```
  function hmac (kunci, pesan)
      if (length(kunci) > panjang_blok) then
          kunci = hash(kunci)
      end if
      if (length(kunci) < panjang_blok) then
          kunci = kunci ? [0x00 * (panjang_blok
- length(kunci))]
      end if

      o_kunci_pad  =  [0x5c  *  panjang_blok]  ?
kunci
      i_kunci_pad  =  [0x36  *  panjang_blok]  ?
kunci

      return          hash(o_kunci_pad          ?
hash(i_kunci_pad ? pesan))
  end function
```

Pengimplementasian *pseudocode* di atas menggunakan bahasa java pada aplikasi JMAC adalah sebagai berikut.

```
Logger.getLogger(JMAC.class.getName()).log(Lev
el.SEVERE, null, ex);
          }
          inputByte[0] = 0;
          md.update(inputByte);
          byte[] sha = new byte[40];
          SecretKeySpec      key      =      new
SecretKeySpec(inputByte, "HMACSHA1");
          Mac mac = null;
          try {
              mac                              =
Mac.getInstance("HmacSHA1");
          } catch (NoSuchAlgorithmException ex)
{

Logger.getLogger(JMAC.class.getName()).log(Lev
el.SEVERE, null, ex);
          }
          try {
              mac.init(key);
          } catch (InvalidKeyException ex) {

Logger.getLogger(JMAC.class.getName()).log(Lev
el.SEVERE, null, ex);
          }
          try{
mac.update(jTextArea1.getText().getBytes("UTF8
"));
          } catch (UnsupportedEncodingException
ex) {

Logger.getLogger(JMAC.class.getName()).log(Lev
el.SEVERE, null, ex);
          }
          byte[] result = mac.doFinal();
          res                =                new
BASE64Encoder().encode(result);
          String    MAC    =    "<"    +    new
BASE64Encoder().encode(result) + ">";
```

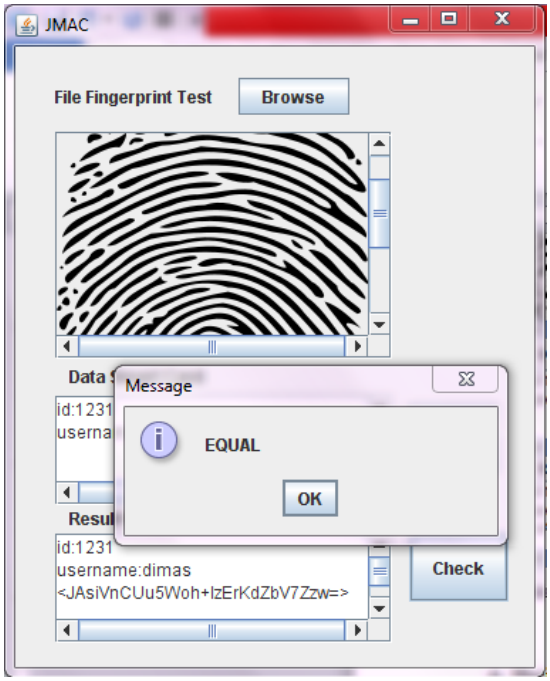


Gambar 6. *Screenshot* hasil MAC

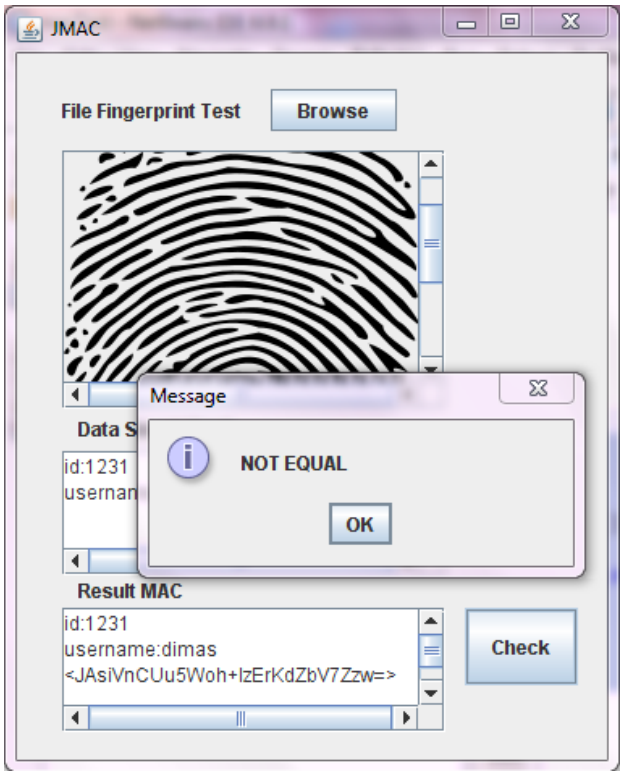


Gambar 7. *Screenshot* hasil MAC dengan perubahan pesan informasi

Dapat dilihat dari 2 *screenshot* di atas, perubahan nilai informasi data yang akan digunakan sebagai nilai input MAC akan menghasilkan nilai yang berbeda pula. Hal ini membuktikkan bahwa pada pengujian kali ini fungsi MAC akurat untuk perunahan 1 karakter sekalipun.



Gambar 8. *Screenshot* pencocokan hasil MAC



Gambar 9. *Screenshot* pencocokan hasil MAC dengan perubahan *file fingerprint*

Dapat dilihat dari 2 *screenshot* di atas, perubahan nilai *byte* pada input file *fingerprint test* akan menghasilkan ketidakcocokan. Hal ini dapat menjadi suatu simulasi validasi bahwa si pembawa kartu tanda pengenal adalah pemilik asli atau bukan.

A. Analisis Hasil dan Perbandingan

Melihat hasil dari pengujian yang diimplementasikan menggunakan *library* dalam bahasa java, *generate secret key* yang didapat dari *array of byte* (*array of byte* dari *fingerprint scan*) akan menghasilkan suatu nilai yang berbeda bahkan untuk perubahan nilai satu *byte* pun. Hal ini menunjukkan bahwa penggunaan MAC ini cukup *visible* untuk dapat diimplementasikan.

Dapat kita lihat juga untuk kasus gambar *fingerprint* yang berbeda ada *screenshot* di atas akan menunjukkan ketidaksamaan hasil dari MAC. Hal ini merupakan salah satu skema simulasi dari validasi apakah pemilik dari *smart card* adalah merupakan pemegang dari *smart card* tersebut. Hal ini untuk mengantisipasi penggunaan *smart card* oleh pihak yang tidak berwenang. Hal ini juga dilakukan untuk mencegah pembuatan kartu tanda pengenal ganda.

Sebagaimana kita ketahui MAC ini merupakan modifikasi dari fungsi *hash* namun menggunakan kunci dalam melakukan *digest* pada pesannya. Oleh karena itu MAC ini cukup aman mengingat fungsi *hash* yang sifatnya satu arah (tidak dapat dikembalikan). Selain itu juga kunci yang digunakan di sini menggunakan prinsip *biometrics* yang tentu saja untuk setiap orang memiliki

kunci yang berbeda-beda. Ini jauh lebih aman disbanding apabila hanya menggunakan mode keamanan seperti nomor PIN saja. Bukan tidak mungkin pihak yang tidak berwenang dapat mengetahui nomor PIN yang kita miliki.

MAC yang merupakan salah satu modifikasi dari fungsi *hash* ini dibandingkan dengan algoritma lain seperti RSA misalnya tentu saja memiliki performa yang lebih cepat. Banyak penggunaan *smart card* menggunakan implementasi dari RSA. Ini dapat menjadi kelebihan dari penggunaan modifikasi fungsi *hash* yaitu dari segi performa yang diberikan terutama juka berhadapan dengan *file database* dalam skala besar. Selain itu juga, pada MAC ini pesan yang di-*hash* pada dasarnya sifatnya tidak rahasia. Keuntungan lainnya adalah jika menggunakan fungsi *hash* satu-arah biasa (seperti *MD5*), maka virus dapat menghitung nilai *hash* yang baru dari nilai informasi yang berubah seperti alamat rumah pada kartu tanda penduduk, lalu mengganti nilai *hash* yang lama di dalam tabel *database* pusat dari sistem. Tetapi, jika digunakan *MAC*, virus tidak dapat melakukan hal ini karena ia tidak mengetahui kunci.

Namun terdapat permasalahan mengenai bagaimana MAC ini agar dapat diimplementasikan. Permasalahan utamanya adalah bagaimana sistem dapat mentoleransi *fingerprint* yang didapat pada galat-galat atau *range* nilai tertentu. Sebagaimana kita ketahui bahwa *fingerprint* yang didapat akan relatif memiliki perbedaan. Walaupun pada dasarnya *fingerprint* di sini hanya digunakan untuk melakukan *generate* suatu nilai kunci.

Penerapan *smart card* ini sudah sangat luas, bahkan KTP sekarang pun suda dibuat versi digitalnya. Pemanfaatan lainnya adalah seperti pencegahan manipulasi penggunaan hak pilih pada pemilu yang mana hanya dapat digunakan satu kali untuk setiap penduduk. Dalam dunia perbankan metode validasi seperti ini sangat dibutuhkan seperti kartu ATM yang dapat digunakan untuk pengambilan dana pada mesin ATM dan juga sistem pembayaran *online.* Validasi dengan menggunakan *biometric fingerprint* dapat meningkatkan keamanan dari penerapan-penerapan tersebut.

V. KESIMPULAN

Seiring perkembangan dunia digital, penggunaan kartu tanda pengenal sudah tidak lagi menggunakan kartu biasa lagi. Hampir semua kartu tanda pengenal menggunakan *smart card* dimana terdapat *chip* untuk menyimpan berbagai jenis informasi termasuk mekanisme autentikasi yang bertujuan untuk menjaga keamanan dari penyalahgunaan oleh pihak yang tidak berwenang.

Dari hasil analisis dan percobaan yang kita dapat mengenai penggunaan MAC sebagai salah satu fungsi *hash* yang memanfaatkan *biometric fingerprint* sebagai kunci diantaranya adalah penggunaan fungsi MAC ini akurat terhadap perubahan yang berarti nilai *hash* yang dihasilkan akan berbeda walaupun perubahan yang dilakukan cukup sedikit. Hal ini tentu menjadi salah satu syarat utama agar MAC ini dapat digunakan atau diimplementasikan mekanisme autentikasi pada *smart card*. Selain itu juga walaupun terdapat permasalahan mengenai pengambilan nilai sidik jari yang berbeda-beda metode ini masih cukup *visible* untuk dapat diimplementasikan. Mekanisme ini juga cukup aman karena kunci yang digunakan untuk autentikasi adalah *biometric fingerprint* yang sifatnya unik untuk setiap individu.

REFERENSI

[1] http://www.informatika.org/~rinaldi/Kriptografi/2010-2011/kripto10-11.htm.
diakses tanggal : 24 April 2011

[2] http://en.wikipedia.org/wiki/Smart_card
diakses tanggal : 24 April 2011

[3] http://en.wikipedia.org/wiki/Message_authentication_code
diakses tanggal : 24 April 2011

[4] http://www.bppt.go.id/index.php?option=com_content&view=article&id=313:penerapan-awal-kartu-tanda-penduduk-elektronik-di-indonesia&catid=55:teknologi-informasi-komunikasi-dan-kendali.
diakses tanggal : 6 Mei 2011

[5] http://en.wikipedia.org/wiki/Biometrics.
diakses tanggal : 6 Mei 2011

[6] http://en.wikipedia.org/wiki/HMAC.
diakses tanggal : 6 Mei 2011

[7] http://en.wikipedia.org/wiki/Single_sign-on\
diakses tanggal : 6 Mei 2011

[8] http://javaandcryptosmartcards.blogspot.com/
diakses tanggal : 6 Mei 2011

[9] http://www.securingjava.com/chapter-eight/chapter-eight-5.html
diakses tanggal : 6 Mei 2011

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, 7 Mei 2011

ttd

Dimas Aditiya Nurahman-13508093