Penggunaan Autentifikasi Sidik Jari untuk Pengamanan Transaksi ATM (*Automated Teller Machine*)

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*—Perkembangan teknologi yang semakin pesat dapat mempermudah manusia dalam melaksanakan berbagai aktivitasnya, termasuk aktivitas keuangan melalui ATM (*Automatic Teller Machine*). Namun demikian, maraknya kasus pembobolan ATM belakangan ini cukup menimbulkan kerisauan pada masyarakat yang memanfaatkan jasa layanan bank ini. Terdapat berbagai macam modus pembobolan ATM yang pernah dilakukan, dan beberapa di antaranya memiliki keterkaitan dengan kriptografi pada sistem keamanan ATM itu sendiri, salah satunya adalah penggunaan algoritma DES (*Data Encryption Standard*) untuk enkripsi data autentifikas.**

Usulan yang diusung dalam makalah ini adalah penggunaan sidik jari sebagai pengganti autentifikasi berupa PIN (*Personal Identification Number*) yang selama ini telah diterapkan. Sidik jari merupakan alat autentifikasi yang tidak mudah untuk ditiru, tidak seperti PIN. Terlebih lagi PIN yang digunakan untuk pengamanan ATM hanya terdiri dari beberapa digit, karena terbatasi dengan kemampuan ingatan manusia. Penggunaan sidik jari ini diharapkan dapat meningkatkan keamanan di ATM dan mempersulit upaya-upaya pembobolan yang dilakukan oleh para pelaku kejahatan.

Namun demikian, masih terdapat beberapa kekurangan pada mekanisme ini, salah satunya adalah kemampuan pencitraan sidik jari yang tidak selalu memberikan hasil yang identik. Implementasi lebih lanjut dari solusi yang ditawarkan ini masih memerlukan penelitian lanjut yang aktual dan komperehensif dengan mempertimbangkan aspek kompleksitas dan fisibilitas implementasi.

***Kata Kunci*—ATM (*Automatic Teller Machine*), Autentifikasi, Sidik Jari, Algoritma DES (*Data Encryption Standard*).**

I. PENDAHULUAN

Seiring dengan perkembangan teknologi yang semakin pesat, berbagai kegiatan manusia dapat dipermudah dan dipercepat, termasuk di antaranya dalam kegiatan transaksi perbankan. Kini untuk sekedar melakukan transaksi keuangan, kita tidak harus datang ke bank, dan mengantri cukup lama untuk mendapatkan giliran pelayanan, karena kita dapat melakukan transaksi tersebut di luar bank dengan menggunakan salah satu teknologi canggih yang sering disebut dengan ATM (*Automated Teller Machine*, di Indonesia terkadang merupakan singkatan bagi Anjungan Tunai Mandiri).

ATM adalah sebuah alat elektronik yang mengijinkan nasabah bank untuk melakukan transaksi perbankan (penarikan tunai, pengecekan saldo, transfer, dsb.) mereka tanpa perlu dilayani oleh seorang *teller* manusia. Bahkan kini beberapa jenis ATM sudah mampu melakukan penyetoran uang, pembayaran tagihan listrik, telepon, dsb.

Konsep ATM pertama kali lahir pada tahun 1968. Mesin ini ditemukan oleh Don Wetzel, *Vice President of Product Planning* pada perusahaan Docutel, bersama dengan rekan-rekannya yaitu Tom Barnes, Kepala Mekanik, dan George Chastian, seorang insinyur listrik. Pada perkembangannya, demi menjaga keamanan nasabah, ATM ini tidak terlepas dari kriptografi, terutama pada saat transmisi nomor PIN dari mesin ATM ke pusat data bank [2].

Dewasa ini, maraknya kasus pembobolan ATM di Indonesia cukup menimbulkan kerisauan pada masyarakat yang memanfaatkan jasa layanan bank ini. Salah satu modus pembobolan ATM yang pernah dilakukan dan cukup menimbulkan kegemparan di Indonesia adalah *ATM skimming & PIN capturing*. *ATM skimming* adalah metode di mana pelaku kejahatan menempelkan alat *card skimmer/card reader* di tempat memasukkan kartu, metode ini digunakan untuk mencuri data magnetis pada kartu ATM yang dimasukkan.

Sedangkan *PIN capturing* adalah metode yang digunakan untuk memperoleh PIN (*Personal Identification Number*) pemilik kartu ATM yang telah dicuri datanya, dengan cara menggunakan kamera tersembunyi untuk membaca gerakan jari pengguna ATM. Dengan dimilikinya data magnetik kartu ATM, maka pelaku dapat membuat duplikat kartu ATM tersebut, dan ditambahkan dengan informasi PIN yang dimiliki, transaksi ilegal pun dapat dilakukan oleh pelaku [4].

Selain metode di atas, salah satu metode lain yang pernah digunakan dalam pembobolan ATM adalah dengan melakukan serangan terhadap kriptografi yang digunakan untuk mengamankan transaksi informasi PIN dari mesin ATM ke komputer *server* bank. Kriptanalis menyadap transmisi dari mesin ATM ke host bank pusat, kemudian melakukan *chosen plaintext attack* terhadap nomor PIN yang dimasukkan pengguna.

Dalam makalah ini, pembahasan difokuskan pada pengamanan PIN, yang akan dicoba dilakukan dengan cara mengganti media autentifikasi dari sekedar 4 – 6 digit angka ke dalam bentuk sidik jari yang jauh lebih sulit untuk dicuri. Pembahasan solusi dalam makalah ini dibatasi hanya pada penerapan solusi secara teoritis tanpa disertai dengan studi fisibilitas terhadap implementasi praktisnya, karena masih diperlukan penelitian lanjut yang lebih aktual dan komperehensif mengenai fisibilitas implementasi metode ini.

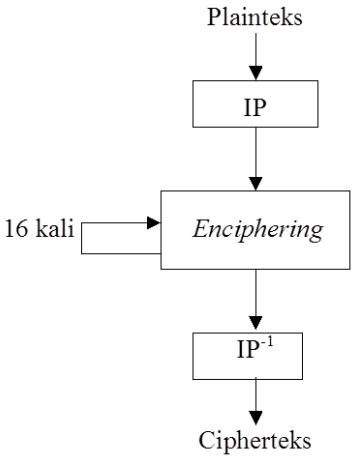
II. PRINSIP DASAR

Sebelum melangkah ke solusi yang ditawarkan, penulis akan menjelaskan beberapa algoritma kriptografi yang digunakan pada mesin ATM, serta sistem biometrik yang akan ditawarkan dalam solusi ini. Data sensitif dalam transaksi ATM (seperti PIN) biasanya dienkripsi dengan menggunakan algoritma DES, bahkan beberapa prosesor transaksi saat ini telah mengharuskan penggunaan algoritma Triple DES [5].

A. Algoritma DES (Data Encryption Standard)

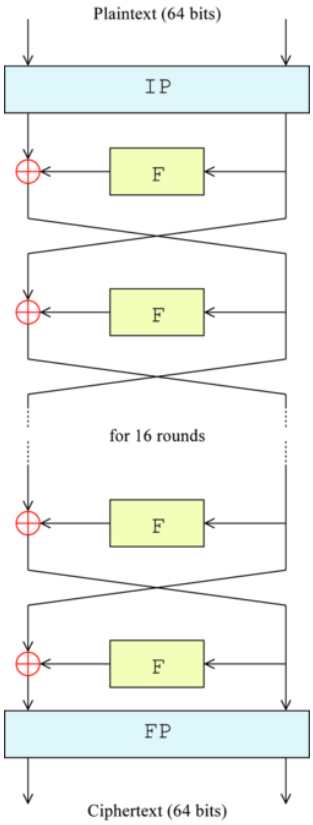
Algoritma DES atau *Data Encryption Standard* ini dikembangkan di IBM pada tahun 1972 [1]. Algoritma ini merupakan sebuah *block cipher* yang merupakan kriptografi kunci simetri dan menggunakan algoritma DEA (*Data Encryption Algorithm*). DES beroperasi pada ukuran blok 64 bit, dengan panjang kunci sama dengan ukuran blok, yaitu 64 bit juga, tetapi hanya terpakai 56 bit (8 bit lainnya tidak terpakai) [6].

Pada algoritma DES, setiap blok dienkripsi sebanyak 16 kali putaran dengan kunci internal yang berbeda-beda yang dibangkitkan dari kunci eksternal. Selain itu juga dilakukan permutasi awal dan inversi permutasi awal (kadang disebut permutasi akhir). Skema global DES dapat dilihat pada skema di bawah ini:



Gambar 1. Skema Global Algoritma DES

Sedangkan diagram algoritma DES secara lengkap dapat dilihat pada gambar berikut ini:



Gambar 2. Skema Jaringan Feistel dalam DES

B. Triple DES (Triple Data Encription Standard)

Triple DES merupakan nama lain dari algoritma *block cipher Triple Data Encryption Algorithm* (TDEA atau Triple DEA). Algoritma ini merupakan algoritma *Data Encryption Standard* (DES) yang diterapkan tiga kali terhadap masing-masing blok data. Seiring dengan perkembangan kemampuan komputasi komputer yang semakin cepat, ukuran kunci pada algoritma DES biasa (56 bit) menjadi semakin rawan diserang dengan menggunakan serangan *brute force*. Algoritma Triple DES ini dirancang untuk memperbesar ukuran kunci untuk melindungi dari serangan *brute force* tersebut, tanpa perlu merancang algoritma *block cipher* baru yang lebih kompleks [7].

Algoritma Triple DES menggunakan kumpulan kunci yang mewakili tiga kunci DES: K1, K2, dan K3 yang masing-masing panjangnya 56 bit. Algoritma enkripsi yg digunakan adalah sebagai berikut:

$$cipherteks = E_{K3}(D_{K2}(E_{K1}(plainteks)))$$

Sedangkan algoritma dekripsi yang digunakan merupakan kebalikan dari algoritma di atas, yakni sebagai berikut:

$$plainteks = D_{K1}(E_{K2}(D_{K3}(cipherteks)))$$

Tiga kali enkripsi ini dilakukan pada setiap blok (64 bit) data. Ketiga kunci tersebut (K1, K2, K3) dapat dibangkitkan dengan tiga cara, yakni:

1. Ketiga kunci independen satu sama lain.
2. K1 dan K2 independen, dan K3 = K1.
3. Ketiga kunci identik, K1 = K2 = K3.

Cara pertama memberikan keamanan yang paling baik, dengan panjang kunci 3 x 56 = 168 bit yang saling independen satu sama lain. Sedangkan cara kedua lebih lemah, dengan panjang kunci hanya 2 x 56 = 112 bit yang saling independen satu sama lain. Tetapi cara ini lebih kuat daripada sekedar melakukan DES sebanyak dua kali, dan ini dapat melindungi serangan *man-in-the-middle*. Cara yang ketiga mirip dengan DES, dengan panjang kunci yang hanya 56 bit. Cara ini sudah tidak lagi direkomendasikan oleh National Institute of Standards and Technology (NIST) [7].

C. Sistem Biometrika

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 3. 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 autentifikasi sidik jari untuk pengamanan transaksi ATM ini, terdapat tiga komponen utama yang memiliki peranan penting. Yakni metode pengolahan citra digital sidik jari dari bentuk gambar ke bentuk lain (kumpulan bit) yang lebih mudah untuk dienkripsi, metode enkripsi dan dekripsi menggunakan algoritma DES atau Triple DES terhadap data digital yang diperoleh, dan skema umum penerapannya untuk kepentingan autentifikasi akun bank di ATM. 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 alat autentifikasi untuk transaksi perbankan di ATM.

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 4. 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].

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

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.

B. Penggunaan Algoritma DES dan Triple DES

Kumpulan bit yang diperoleh dari hasil pencitraan sidik jari tersebut selanjutnya dienkripsi dengan menggunakan algoritma DES. Algoritma yang akan digunakan tersebut dapat berupa DES ataupun Triple DES.

Pada dasarnya penggunaan algoritma DES dan Triple DES untuk enkripsi sekumpulan bit hasil pencitraan sidik jari ini tidak jauh berbeda dengan penggunaan untuk enkripsi terhadap PIN (*Personal Identification Number*) yang biasa dilakukan oleh mesin ATM selama ini. Perbedaan mendasar yang ada antara kedua mekanisme autentifikasi ini adalah pada panjang bit yang dienkripsi dan digunakan sebagai alat autentifikasi.

Pada mekanisme autentifikasi PIN, data yang dienkripsi dan digunakan sebagai alat autentifikasi hanya sepanjang PIN yang ditentukan, pada umumnya PIN untuk kartu ATM hanya memiliki panjang 4 – 6 karakter, karena terbatas dengan daya ingat manusia. Dengan demikian, panjang bit yang dienkripsi hanya sekitar 32 – 48 bit. Panjang bit ini bahkan kurang dari satuan blok yang digunakan pada algoritma DES dan Triple DES, yakni 64 bit.

Sedangkan pada mekanisme autentifikasi sidik jari, data hasil pencitraan sidik jari dapat terdiri dari kumpulan bit yang lebih besar. Apabila diasumsikan dari setiap sidik jari dapat diperoleh himpunan solusi bobot simpul dengan banyaknya elemen sekitar 15 – 20 buah dengan tipe data integer, maka setidaknya data yang nantinya akan dienkripsi dan digunakan sebagai alat autentifikasi memiliki panjang 15 byte x 8 = 120 bit, atau bahkan dapat mencapai 20 byte x 8 = 160 bit. Data ini sudah cukup panjang dan cukup aman untuk dienkripsi dengan algoritma DES dan Triple DES.

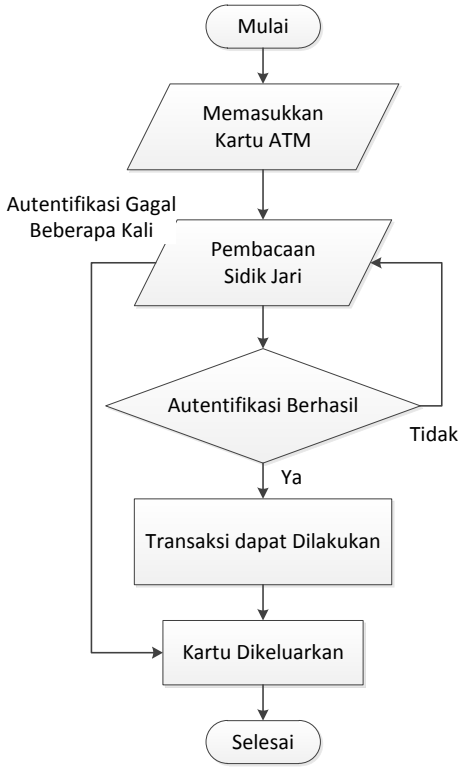
C. Penggunaan Sidik Jari untuk Pengamanan Transaksi di ATM

Pada bagian ini akan dijelaskan gambaran umum dari solusi yang ditawarkan, yakni penggunaan autentifikasi sidik jari untuk pengamanan transaksi ATM. Sidik jari di sini akan digunakan sebagai alat autentifikasi, menggantikan PIN (*Personal Identification Number*) yang selama ini digunakan.

Prosedur penggunaan dari sisi pengguna akan sama dengan prosedur penggunaan ATM sebelumnya, hanya saja pada saat proses autentifikasi dilakukan, yang digunakan adalah sidik jari. Secara umum, berikut merupakan prosedur penggunaan ATM yang memiliki mekanisme autentifikasi sidik jari.

1. Pengguna memasukkan kartu ATM ke dalam mesin ATM.
2. Pengguna menempelkan salah satu jarinya (misalnya, ibu jari kanan) ke alat pembaca sidik jari (*fingerprint reader*) yang terintegrasi dengan mesin ATM.
3. Apabila sidik jari cocok (autentifikasi diterima), maka pengguna dapat melakukan transaksi perbankan di ATM tersebut, seperti pengecekan saldo, penarikan tunai, transfer, dsb.
4. Apabila sidik jari tidak cocok (autentifikasi ditolak), maka pengguna harus melakukan pembacaan ulang sidik jarinya, karena kemungkinan ada kesalahan yang terjadi pada pembacaan sidik jari, baik karena posisi jari yang kurang tepat, jari yang tertutup debu, maupun alasan lainnya. Langkah ini akan berulang sebanyak beberapa kali, selama autentifikasi tetap gagal dilakukan.
5. Apabila setelah pembacaan sidik jari dilakukan beberapa kali autentifikasi tetap gagal dilakukan, pengguna tidak dapat melakukan transaksi, karena tidak dikenali sebagai pemilik kartu ATM yang telah dimasukkan.
6. Setelah penggunaan ATM selesai, kartu ATM dikeluarkan kembali.

Demikianlah prosedur penggunaan ATM dengan autentifikasi sidik jari. Langkah-langkah di atas dapat digambarkan dengan diagram alir sebagai berikut.

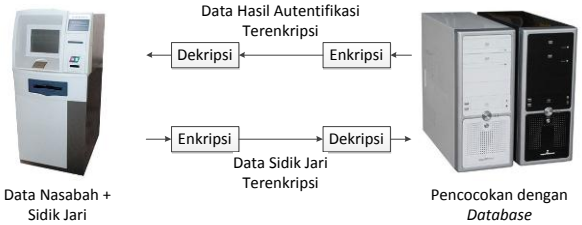


Gambar 5. Prosedur Penggunaan ATM dengan Mekanisme Autentifikasi Sidik Jari

Berikut merupakan cara kerja ATM dalam melakukan autentifikasi terhadap nasabah bank yang bersangkutan.

1. Mesin ATM menerima kartu ATM dari pengguna.
2. Mesin ATM meminta pengguna untuk menempelkan salah satu jarinya ke alat pembaca sidik jari (fingerprint reader) yang terintegrasi dengan ATM.
3. Mesin ATM melakukan pembacaan data magnetis yang terdapat dalam kartu ATM yang telah dimasukkan.
4. Mesin ATM melakukan konversi gambar hasil pencitraan sidik jari menjadi sekumpulan bit autentifikasi.
5. Bit hasil pembacaan sidik jari tersebut kemudian dienkripsi oleh mesin ATM dengan menggunakan algoritma DES atau Triple DES.
6. Hasil enkripsi dari kumpulan bit tersebut beserta data nasabah yang diperoleh dari kartu ATM kemudian dikirimkan ke komputer server yang terdapat di bank pusat.
7. Komputer server bank pusat melakukan dekripsi terhadap kumpulan bit autentifikasi yang diterima tersebut dengan menggunakan algoritma DES atau Triple DES.
8. Data nasabah yang diterima dan hasil dekripsi dari kumpulan bit tersebut kemudian dicocokkan dengan database yang ada pada komputer server bank.
9. Apabila kedua data tersebut memiliki kecocokan dengan tingkat toleransi galat pada kumpulan bit sidik jari sebesar 15%, maka autentifikasi dinyatakan berhasil.
10. Apabila kumpulan bit sidik jari yang berkorespondensi dengan data nasabah yang bersangkutan memiliki galat lebih dari 15%, maka autentifikasi dinyatakan gagal.
11. Komputer server mengirimkan hasil autentifikasi ke mesin ATM dengan terlebih dahulu mengenkripsi pesan yang dikirimkan, untuk menghindari serangan man-in-the-middle yang hendak mengubah pesan hasil autentifikasi tersebut. Enkripsi dapat dilakukan dengan algoritma DES, Triple DES, atau algoritma lainnya.
12. Pesan hasil autentifikasi yang diterima oleh mesin ATM kemudian didekripsi dengan menggunakan algoritma yang sama seperti yang digunakan pada komputer *server*.
13. Apabila pesan autentifikasi yang diterima oleh mesin ATM menyatakan bahwa autentifikasi berhasil, maka transaksi lebih lanjut dapat dilakukan (pengecekan saldo, penarikan tunai, transfer, dsb.).
14. Sebaliknya, apabila pesan autentifikasi yang diterima oleh mesin ATM menyatakan bahwa autentifikasi gagal, maka mesin ATM akan meminta pengguna untuk kembali melakukan pembacaan sidik jari. Langkah ini akan berulang sebanyak beberapa kali, selama autentifikasi tetap gagal dilakukan.
15. Apabila setelah pembacaan sidik jari dilakukan beberapa kali autentifikasi tetap gagal dilakukan, maka mesin ATM tidak akan mempersilahkan pengguna untuk melakukan transaksi selanjutnya, karena pengguna tidak dikenali sebagai pemilik kartu ATM yang telah dimasukkan.
16. Setelah penggunaan ATM selesai, kartu ATM dikeluarkan kembali oleh mesih ATM.

Demikianlah cara kerja ATM yang menggunakan mekanisme autentifikasi sidik jari. Prosedur lebih jelasnya, dapat dilihat pada gambar berikut.



Gambar 6. Cara Kerja ATM dengan Mekanisme Autentifikasi Sidik Jari

IV. ANALISIS

Penggunaan sidik jari sebagai alat autentifikasi dalam pengamanan transaksi di ATM ini merupakan suatu usulan baru yang perlu dipertimbangkan lebih jauh. 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 dipaparkan kelebihan dan kekurangan dari solusi yang ditawarkan pada makalah ini. Berhugung pembahasan pada makalah ini hanya mencakup penjelasan teoritis mengenai penerapan autentifikasi sidik jari pada ATM, maka aspek kelebihan dan kekurangan yang akan dipaparkan hanyalah aspek-aspek yang bersifat teoritis.

A. *Kelebihan*

Berikut merupakan kelebihan dari solusi yang ditawarkan:

1. Alat autentifikasi berupa kumpulan bit sidik jari lebih panjang daripada alat autentifikasi yang hanya terdiri dari beberapa digit angka seperti pada PIN (*Personal Identification Number*) yang telah digunakan selama ini. Hal ini akan mempersulit para pelaku kejahatan dalam melakukan serangan terhadap kriptografi. Oleh karena itu, tingkat keamanan autentifikasi berbasis sidik jari ini lebih tinggi daripada autentifikasi berbasis PIN.
2. Kemungkinan pencurian alat autentifikasi seperti yang terjadi pada PIN menjadi jauh lebih kecil, karena alat autentifikasi tidak dapat ditiru hanya dengan sekedar menggunakan kamera tersembunyi, seperti pada metode *PIN capturing* yang telah dijelaskan sebelumnya. Pencurian sidik jari sangat sulit dilakukan, karena mengharuskan adanya interaksi langsung dengan nasabah. Demikian pula peniruannya, sidik jari tidak dapat dengan mudah ditiru, karena merupakan bagian tubuh dari manusia. Walaupun dalam kenyataannya, ditemukan beberapa teknik yang dapat dilakukan untuk meniru sidik jari, tetapi hal tersebut masih tergolong sangat sulit untuk dilakukan.
3. Pengguna ATM tidak perlu lagi mengingat beberapa digit angka yang digunakan sebagai PIN, dan tidak perlu khawatir dengan pencurian terhadap alat autentifikasinya.

B. *Kekurangan*

Berikut merupakan kekurangan dari solusi yang ditawarkan:

1. 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 yang terjadi cukup besar, dan apabila ini terjadi, maka autentifikasi sidik jari semacam ini justru mempersulit para nasabah yang hendak melakukan transaksi.
2. Penentuan batas toleransi galat harus dilakukan dengan baik dan akurat. Apabila toleransi galat yang diberikan terlalu kecil, maka hal ini dapat mempersulit nasabah. Tetapi apabila toleransi galat yang diberikan terlalu besar, tingkat keamanan autentifikasi ini menjadi semakin rendah.

IV. KESIMPULAN

1. Serangan terhadap kriptografi, terutama terhadap algoritma DES dan Triple DES, dapat dikurangi tingkat keberhasilannya, dengan cara memperpanjang data yang dienkripsi.
2. Penggunaan autentifikasi sidik jari untuk pengamanan transaksi perbankan di ATM (*Automatic Teller Machine*) mungkin untuk dilakukan.
3. Digunakannya alat autentifikasi biometrik berupa sidik jari dapat meningkatkan keamanan proses autentifikasi yang dilakukan, khususnya pada autentifikasi untuk transaksi di ATM.
4. Implementasi lebih lanjut dari sistem yang ditawarkan ini masih memerlukan penelitian lebih lanjut yang aktual dan komperehensif, dengan mempertimbangkan aspek kompleksitas dan fisibilitas implementasi.

REFERENSI

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

[2] Nugraha, M. Pasca. Tugas Makalah 1: Kriptografi pada Kejahatan Pembobolan ATM di Indonesia. Program Studi Teknik Informatika STEI ITB. 2010.

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

[4] http://bang-anuh.blogspot.com/2010/01/atm-security.html Diakses pada tanggal 22 Maret 2011, Pukul 20.35.

[5] http://en.wikipedia.org/wiki/Automated_teller_machine Diakses pada tanggal 22 Maret 2011, Pukul 21.34.

[6] http://en.wikipedia.org/wiki/Data_Encryption_Standard Diakses pada tanggal 22 Maret 2011, Pukul 21. 56.

[7] http://en.wikipedia.org/wiki/Triple_DES Diakses pada tanggal 22 Maret 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, 22 Maret 2011

Zain Fathoni
13508079