Analisis Penerapan Kriptografi dalam Pengembangan *Single-Identity Card*

Lyco Adhy Purwoko / 13508027
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If18027@students.if.itb.ac.id

Abstract* – masalah pengelolaan data dan informasi SDM menjadi hal yang serius untuk ditangani oleh sebuah organisasi atau perusahaan. Kebutuhan sebagai identitas tunggal dari seseorang serta fungsionalitas autentifikasi data diperlukan dalam sistem pengelolaan sumber daya manusia secara keseluruhan. Penggunaan *contactless smart card* sebagai media implementasi konsep *single identity card* mempunyai faktor keamanan yang lebih dapat diandalkan. Tetapi bukan berarti tanpa celah keamanan dan tidak dibutuhkan pengembangan sistem keamanan. Metode pengaman data dan informasi yang dilakukan di dalam sebuah *chip (embedded system)* memberikan kecepatan pemrosesan yang lebih. Kehadiran kriptografi sebagai seni untuk mengamkan data dan informasi memberikan kesempatan leluasa untuk bereksperimen, menemukan metode dan algoritma yang paling efektif dan efisien dalam mengamankan data. Tidak hanya unggul dari segi algoritma, tetapi juga dituntut berpikir untuk menerapkan metode praktis agar mampu meningkatkan keamanan data dan informasi di dalam *contactless smart card* sebagai *single identity card.

***Key word* : kriptografi, contactless smart card, single-identity card**

1. PENDAHULUAN

Teknologi informasi dan komunikasi yang berkembang begitu pesatnya saat ini, memberikan dampak pula terhadap bidang-bidang lain untuk ikut berkembang. Segala bidang kehidupan manusia dibuat lebih mudah, efektif, dan efisien oleh kehadiran teknologi informasi dan komunikasi. Namun, dampak yang dihasilkan pun tidak hanya dampak positif saja. Banyak pula dampak negative berupa model-model kejahatan baru yang muncul akibat perkembangan teknologi informasi dan komunikasi ini. Perlu adanya sebuah analisis mendalam terkait kebutuhan dan faktor keamanan dalam penerapannya..

Perkembangan ini seolah membawa perubahan besar menuju dunia digital. Era digital memberikan dunia baru bagi manusia dalam menjalani kehidupan sehari-hari. Salah satu hal yang terlihat di era digital ini adalah pengolahan data dan informasi. Hampir sebagian besar data dan informasi saat ini dikelola menggunakan penerapan teknologi informasi, agar dapat berjalan lebih efektif dan efisien. Salah satunya adalah data dan informasi mengenai identitas diri seseorang. Data dan informasi seseorang akan menyimpan hal-hal unik yang seharusnya akan berbeda satu sama lainnya. Pengelolaan identitas diri secara digital diharapkan dapat memberikan manfaat dan kemudahan bagi manusia dalam menjalani pekerjaannya.

Namun, seiring dengan perkembangan serta inovasi dalam pengelolaan data dan informasi, tentu saja tidak lepas dari hadangan beberapa masalah yang harus dihadapi. Permasalahan umum yang sering terjadi ketika berbicara mengenai pengolahan data adalah redudansi data. Oleh karena itu salah satu tujuan dari pengelolaan data dan informasi identitas diri seseorang secara digital adalah untuk menjaga agar tidak terjadi redudansi data tersebut. Karena data dan informasi identitas diri adalah hal yang sensitif dan berpotensi menimbulkan tindak kejahatan yang tidak diinginkan bila disalahgunakan oleh pihak yang tidak bertanggung jawab.

Salah satu solusi yang diterapkan saat ini untuk mengatasi permasalahan redudansi data dan informasi identitas diri yang dikelola secara digital adalah dengan membuat repository terpusat (*data center*). Kemudian dengan melekatkan sebuah kartu tanda pengenal elektronik kepada setiap orang, sebagai tanda pengenal mereka di era-digital saat ini (*single identity card*). Dengan adanya tanda pengenal elektronik dan repository terpusat tersebut akan memudahkan dalam pengelolaan data, mencegah adanya redudansi data, serta memudahkan kinerja manusia diberbagai hal. Diantaranya adalah pemanfaatan *single identity card* tersebut sebagai penanda tunggal seseorang yang menyimpan informasi singkat orang tersebut.

Dalam perkembangannya saat ini, solusi tersebut

sudah banyak dilakukan di lingkup organisasi, lembaga pemerintahan, dan perusahaan. Hal tersebut dilakukan untuk mempermudah organisasi, lembaga, dan perusahaan dalam mengelola sumber daya manusianya. Konsep tersebut diimplementasikan dengan memberikan kartu tanda pengenal kepada setiap orang yang menyimpan beberapa data unik dari si pemilik kartu. Secara teknis kartu tersebut (*smart card*) terdapat sebuah *chip* atau *magnetic line* yang menyimpan data pribadi atau data unik yang digunakan sebagai identitas elektronik dari pemilik kartu.

Bukan teknologi informasi dan komunikasi namanya apabila dalam perjalanan perkembangannya tidak diiringi oleh permasalahan-permasalahan yang mengancam. Permasalahan utama dari konsep ini adalah masalah keamanannya (*security*). Ancaman besar terhadap keamanan dari data yang tersimpan di kartu tersebut. Seperti yang sudah disinggung diawal bahwa data identitas diri seseorang itu hal yang sensitif. Penyalahgunaan data akan sangat mungkin terjadi dan akan menimbulkan kerugian atau masalah lain bagi si pemilik kartu ataupun orang dan lingkungan disekitarnya. Oleh karena itu perlu adanya sebuah mekanisme dan metode pengamanan terhadap data yang ada di dalam kartu pengenal elektronik tersebut. Kriptografi sebagai seni menjaga kerahasiaan dan keamanan suatu data dan informasi menjadi salah satu alternatif solusi keamanan dari *single-identity card.*

Kriptografi memiliki beberapa algoritma yang dapat digunakan untuk mengamankan data dan informasi yang tersimpan di dalam smart card tersebut. Dapat diterapkan dengan kombinasi algoritma yang ada ataupun dengan kreasi metode pengamanan, sehingga data dan informasi di dalam kartu tersebut tidak disadap oleh orang yang tidak bertanggung jawab. Tetapi tetap perlu diperhatikan dalam penerapan kriptografi agar tidak mengurangi kebermanfaatan dari *single-identity card* tersebut.

2. LANDASAN TEORI

2.1. Electronic Identity Card (Smart Card)

Sebuah organisasi baik dalam konteks pemerintahan ataupun perusahaan – perusahaan swasta sebagian besar kewalahan dalam mengelola sumber daya manusianya. Istilah umumnya yang digunakan pada organisasi pemerintahan ataupun perusahaan adalah pengelolaan sumber daya manusia. Data dan informasi personal harus dikelola semaksimal mungkin untuk tujuan pemanfaatan sumber daya manusia yang efektif dan efisien. Data dan informasi personal SDM tersebut pasti bersinggungan dengan berbagai bidang lainnya dalam keberjalanan sebuah organisasi atau perusahaan secara keseluruhan. Misal bersinggungan dengan bidang keuangan, infrastruktur, dan sarana prasarana. Oleh karena itu, masalah data dan informasi SDM menjadi hal yang perlu diperhatikan lebih karena keberjalanannya akan mempengaruhi banyak bidang.

Salah satu hal utama yang menjadi sorotan dalam masalah pengelolaan SDM adalah identitas unik yang melekat di masing-masing individu pegawai. Identitas tersebut menjadi sebuah tanda pengenal unik yang mampu menjaga integritas data dan informasi personal pemilik kartu tersebut. Selain itu dalam penerapannya dapat terintegrasi dengan sistem lainnya yang akan menunjang kinerja organisasi dan perusahaan lebih efektif dan efisien. Kenapa membutuhkan sebuah identitas elektronik yang unik antara satu dengan lainnya? Hal tersebut dikarenakan potensi tindakan kejahatan ataupun tindakan yang tidak diinginkan dapat bermula dari manipulasi dati diri. Tidak adanya teknologi informasi sebagai penerapan di kartu identitas elektronik ini akan sangat memungkinkan seseorang untuk leluasa memanipulasi identitas diri yang digunakan untuk melakukan tindakan negative dan tidak dapat dipertanggung jawabkan. Seiring perkembangan teknologi informasi tersebut, terciptalah sebuah konsep *electronic identity card* dengan karakteristik tertentu. Konsep tersebut akan meminimalisir seseorang untuk melakukan manipulasi identitas diri. Bahkan di lingkup ketatanegaraan Indonesia, masalah identitas ini menjadi isu yang hangat dibicarakan. Pemerintah Indonesia kewalahan dengan munculnya kasus-kasus tindak kejahatan yang berawal dari manipulasi, pemalsuan, atau penggandaan identitas diri. Dengan manipulasi tersebut, pihak yang berwajib kewalahan untuk melacak si pelaku, sehingga dilemparlah konsep e-ktp di Indonesia.

Secara umum *electronic-identity card* merupakan salah satu implementasi dari konsep *smart card.* Teknologi *smart card* sendiri pertama kali dibuat oleh orang jepang bernama Kunitaka Arimura pada tahun 1970. Perkembangan teknologoi *smart card* adalah pengembangan dari konsep *mangnetic line.* Tetapi berbeda dengan *magnetic line* yang hanya bisa menyimpan data. Pada *smart card,* dapat menyimpan, kemampuan memroses, menginterpetasikan data, serta

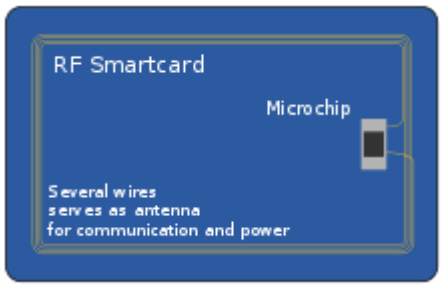
menyimpan data tersebut lebih aman., dengan diiringi pula ilmu kriptografi yang membuat data dan informasi tersebut mudah dibaca oleh orang lain. Di dalam *smart card* menyimpan sebuah ID unik dari chip kartu tersebut serta beberapa data dan informasi. Komponen dasar dari *smart card* diantaranya adalah material dasar yang digunakan yaitu PVC (*polyvynil chloride*) atau *thermoplastic* sejenis. Kemudian komponen utama adalah *IC (chip)* yang dipasang di dalam kartu. Isi dari *chip* secara umum terdiri dari *memory* dan *microprocessor*. Terdapat sebuah *card reader* untuk membaca dan menangkap data serta informasi yang tersimpan di dalam *smart card* tersebut.

2.2. Contactless Smart Card

Berdasarkan cara komunikasi antara *smart card* dengan aplikasi lain yang membaca data dan informasi di dalamnya, dapat dibagi menjadi dua tipe *smart card*, yaitu:

- *Contact smart card* – koneksi atau komunikasi yang terjadi antara *chip* pada *smart card* dengan *reader* melalui sentuhan.
- *Contactless smart card* – komunikasi yang terjadi dapat menggunakan antenna (frekuensi radio). Dengan *contactless card* yang perlu dilakukan hanya perlu mendekatkan kartu tersebut ke *reader(RFID,* sehingga proses komunikasi yang terjadi pun dapat berjalan dengan cepat, efektif, dan efisien serta mengurangi potensi kerusakan kartu apabila dibandingkan dengan *contact card.*

Berikut adalah sebuah gambar ilustrasi dari konsep *contactless card* (gambar 1)



gambar 1: *contactless smart card*

secara dimensi kartu ini memiliki ukuran sama dengan ukuran standart kartu kredit (85.6 x 53.98 x 0.76mm). Kelebihan dari *contactless smart card* diantaranya adalah kartu ini dapat digunakan sebagai identifikasi (*single-identity card*), autentifikasi, dan tempat penyimpanan data serta lebih tahan lama. Kontak antara kartu dan *reader* akan sangat tergantung dari kepekaan *reader* itu sendiri, banyak dipakai pada proses bisnis yang menekankan pada unsur kecepatan. Kelebihan tersebut yaitu:

- Dari segi keamanan lebih dapat diandalkan
- Teknis perawatan lebih sedikit dan memiliki masa hidup yang lebih lama dari *contact card.*

Kemudian kekurannya adalah:

- Tidak cocok untuk diterapkan pada pertukaran data yang besar
- Ukuran lebih besar sedikit
- Provider yang masih minim, sehingga jenis kartu ini terbatas dan mahal.

Dari segi teknis teknologi pembacaan data dan informasi, *contactless card* menggunakan frekuensi radio (RFID - *Radio Frequency Identification*) untuk berkomunikasi antara kartu dan *reader* ataupun *writer* (gambar 2). Sinyal yang digunakan mempunyai frekuensi 135kHz atau 13.56 MHz. Apabila dalam penggunaannya menggunakan frekuensi rendah, maka energi dan kecepatan transfer data rendah, tetapi memiliki jangkauan radius 1m. sedangkan jika menggunakan frekuensi tinggi, maka akan menggunakan energi lebih tinggi dan kecepatan transfer data tinggi.

gambar 2: Komunikasi antara *contactless smart card* dengan *reader*

Standarisasi komunikasi (*protocols*) dari *contactless smart card* adalah ISO/IEC 14443. Hal tersebut mendefinisikan ada dua tipe *contactless smart card* dan mampu melakukan komunikasi dalam radius hingga 10cm. Selain itu, standarisasi lainnya adalah ISO/IEC 15693 yang mampu melakukan komunikasi dengan radius hingga 50cm.

Dari segi keamanan *contactless smart card* ini menamankan fungsi kemanan data dan informasi di *chip* yang tertanam pada kartu tersebut. Pada penerapan enkripsi data dan informasi

diimplementasikan pada perangkat keras *chip* tersebut (*embedded system*). Beberapa kelebihan enkripsi di *embedded system*, diantaranya adalah dari segi kecepatan dalam melakukan aktivitas proses. Enkripsi dan dekripsi dilakukan ketika transfer data pada komunikasi antara kartu dengan *reader*.

2.3. Algoritma Kriptografi Modern

Kriptografi merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secata aman (*cryptography*). Esensi dasar dari penggunaan kriptografi adalah untuk melakukan validasi terhadap tiga hal di bawah inim yaitu:

1. Kerahasian – data yang ditransmisikan harus terjaga kerahasiaannya dari pengirim pesan hingga ke penerima pesan, tanpa diketahui oleh orang lain isi asli dari pesan tersebut (*plain text*).
2. Autentifikasi (keaslian) – penerima mampu menjamin bahwa data yang dikirimkan adalah asli dari sang pengirim tanpa adanya intervensi atau perubahan dan pengrusakan pesan yang ditransmisikan.
3. Integritas – data yang dikirimkan harus tahan terhadap ancaman-ancaman serangan yang ada.

Keamanan dari algoritma kriptografi seharusnya berdasarkan kunci kriptografinya, bukan berdasarkan kerahasian dari algoritma kriptografinya. Hal ini berarti bahwa algoritma seharusnya dibuat terbuka dan disebarluaskan untuk dikembangkan dalam lingkup komunitas pengembang.

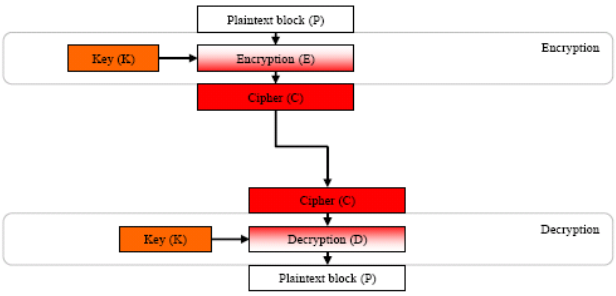
Algoritma kriptografi memiliki banyak macamnya. Secara garis besar, algoritma kriptografi dapat dibagi menjadi dua yaitu algoritma kriptografi klasik dan algoritma kriptografi modern. Masing-masing kelompok tersebut juga masih terdapat berbagai macam algoritma yang mempunyai karekteristiknya masing-masing. Pada pembahasan kali ini, algoritma kriptografi yang akan dibahas lebih lanjut dan dianalisis untuk diterapkan adalah algoritma block cipher (algoritma kriptografi modern). Algoritma block cipher adalah metode algoritma dengan membagi teks data atau informasi yang ingin dienkripsi menjadi blok dengan jumlah atau panjang bit tertentu. Apabila pesan yang berukuran besar, pesan akan dibagi menjadi blok-blok dengan ukuran sama dan menggunakan kunci yang sama pula. Pemilihan algoritma block cipher disebabkan karena beroperasi dalam bentuk bit sehingga tidak dapat dipecahkan dengan teknologi pemecahan kode sederhana. Pada dasarnya pembangunan algoritma block cipher terdiri dari tiga aktivitas beriktu, yaitu:

1. *Substitution Cipher*
2. *Transposition Cipher*
3. *Exclusive –OR Cipher*

Beberapa algoritma cipher block yang digunakan dalam pengamanan data dan informasi adalah sebagai berikut:

1. *Electronic Code Book*

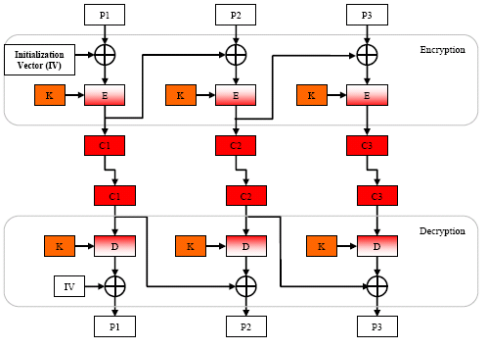
Metode enkripsi setiap block plainteks secara individual dan independen menjadi block cipherteks dengan fungsi enkripsi tertentu dan kunci tertentu (misal XOR). Metode ini mempunyai ancaman keamanan yaitu untuk plainteks yang sama akan selalu dienkripsi menjadi cipherteks yang sama. Gambar 3 memperlihatkan diagram blok dari metode ECB



gambar 3: metode enkripsi ECB

2. *Cipher Block Chaining*

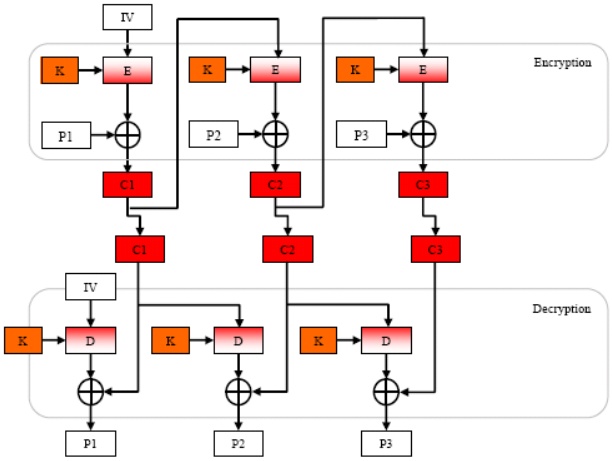
Setiap block cipherteks bergantung pada keseluruhan block plainteks sebelumnya karena hasil enkripsi blo yang sebelumnya dijadikan *feedback* untuk enkripsi blok berikutnya. Konsekuensi dari metode ini adalah ketika terjadi kesalahan pada salah satu blok pada proses enkripsi akan berdampak ke blok-blok selanjutnya. Namun, pada proses dekripsi ketika terjadi kesalahan dalam satu blok hanya akan berdampak pada blok tersebut. Gambar 4 memperlihatkan diagram blok dari proses CBC.



gambar 4: metode enkripsi CBC

3. *Cipher Feedback Mode*

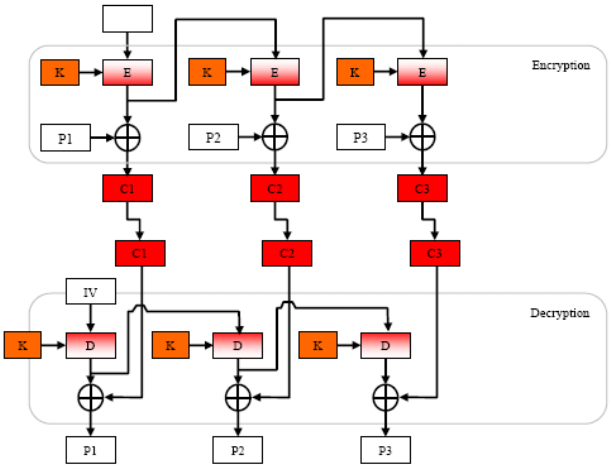
CFB digunakan ketika sebuah data yang harus dienkripsi memiliki ukuran lebih kecil daripada ukuran blok. Pada asumsi pembahasan kali ini ukuran yang digunakan adalah 8 bit. Ilustrasi alur proses pada CFB dapat dilihat di gambar 5.



gambar 5: metode enkripsi CFB

4. *Output Feedback Mode*

Metode OFB mirip dengan CFB, hanya saja metode ini n-bit dari hasil enkripsi terhadap antrian disalin menjadi elemen posisi paling kanan antrian. Dekripsi dilakukan sebagai kebalikan dari proses enkripsi. Gambar 6 menggambarkan proses dari OFB.



gambar 6: metode enkripsi OFB

3. ANALISIS

3.1. Ancaman Serangan Keamanan

Berdasarkan hasil analisis penulis terhadap ancaman keamanan pada *contactless card* sebagai *single-identity card*, dengan melihat karakteristik yang dimiliki oleh *contactless card* serta celah-celah keamanannya. Terdapat beberapa hal yang mengancam keamanan dari data dan informasi yang tersimpan serta penggunaannya, diantaranya sebagai berikut:

- Kemungkinan duplikasi kartu identitas elektronik yang tidak dikeluarkan oleh institusi resmi yang bersangkutan.
- Data dan informasi yang disimpan dapat diduplikasi apabila tidak mendapat proteksi keamanan yang layak. Penggandaan kartu identitas ini dapat merugikan si pemiliki kartu asli dan entitas-entitas yang mempunyai keterhubungan dengan pengunaan kartu tersebut.
- Dapat disalah gunakannya kartu identitas *smart card* tersebut oleh orang yang tidak bertanggung jawab apabila tidak sengaja kartu tersebut hilang dari tangan si pemilik. Perlu adanya sebuah mekanisme untuk mengetahui bahwa si pemegang kartu adalah orang yang benar-benar berhak menggunakan kartu tersebut.
- Menyimpan data di dalam *smart card* terlalu banyak dapat meningkatkan kerawanan penyalahgunaan data ketika kemanan data dapat dibongkar.
- *Smart card* pada umumnya tidak dapat menyimpan data terlalu besar. Tidak semua informasi identitas diri dapat disimpan.
- Apabila dalam mekanisme enkripsi data pada tiap *smart card* SDM memiliki kunci yang sama, maka ketika dapat terbongkar kunci dari salah satu kartu saja maka data dari semua kartu dapat terbongkar.
- Algoritma kriptografi pengaman data pada *smart card* terlalu mudah untuk dicari kuncinya (*brute forces*), sehingga data dapat dengan mudah untuk dibaca oleh orang lain.
- Algoritma yang terlalu kompleks dapat memberatkan kinerja dari *smart card* ketika sedang melakukan komunikasi dan transmisi data dengan *reader*.

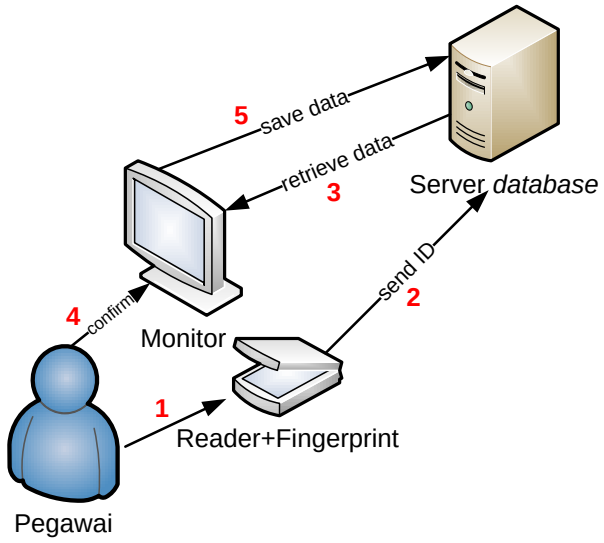
3.2. Analisis Peningkatan Keamanan

Dalam melakukan peningkatan keamanan data dan informasi pada *contactless smart card* tidak cukup hanya dengan melakukan pengamanan dari segi kriptografi atau enkripsi data. Diperlukan metode-metode keamanan yang harus diterapkan sejak perancangan *contactless smart card* sebagai *single-identify card* dengan melihat karakteristik khususnya. Metode peningkatan keamanan yang merupakan hasil analisis dari penulis sebagai bentuk jawaban dari permasalahan keamanan yang ada merupakan hasil analisis dari penulis.

Contactless smart card memiliki karakteristik bahwa data dan informasi yang dapat disimpan sangatlah terbatas. Rata-rata *contactless smart card* hanya berkapasitas 16Kb. Hal tersebut tentu perlu strategi penggunaan kapasitas secara maksimal dan juga memberikan keamanan data yang maksimal. Pada pembahasan kali ini, penulis memilih untuk menggunakan tipe *smart card* 16K2 *card.* Dengan keterbatasan kapasistas penyimpanan yang dimiliki oleh kartu, penulis menerapkan konsep strategi penyimpanan data identitas unik saja pada kartu. Data yang disimpan pada *smart card* adalah:

- ID card
- Key enkripsi-dekripsi data (ter-enkripsi)
- ID user pemilik kartu (misal NIP)
- Biometric data (*fingerprint data*)

Untuk mendapatkan data identitas lengkap dari pemilik kartu, cukup hanya dengan mengambil data ID unik user pemilik kartu dan kemudian menarik data lengkapnya di *database* terpusat untuk melakukan konfirmasi. Dengan begitu kinerja proses dari kartu tidak berat dan dapat berjalan dengan cepat. Sedangkan mesin *reader* cukup menyimpan ID unik user pemilik kartu sebagai identitas diri pemilik kartu (apabila dalam implementasi absensi sumber daya manusianya).



gambar 7: alur penggunaan *single-identity card*

Dengan konsep seperti ini, data lengkap personal akan lebih terjamin keamanannya karena tidak melekat di dalam kartu identitas elektronik tersebut.

Sebagai fungsi kontrol dan memastikan bahwa orang yang menggunakan kartu tersebut memang orang yang berhak menggunakannya (pemilik kartu), peningkatan keamanan autentifikasi dengan mengombinasikan konsep *contactless smart card* dengan *fingerprint recognition.* Ketika pemilik kartu mendekatkan *contactless smart card* ke *reader*, pemilik kartu juga meletakan jarinya di alat *fingerprint.* Kemudian akan dilakukan pencocokan antara biometrics yang tersimpan di dalam kartu dengan hasil scanning *fingerprint* saat itu. Alur penggunaan *single-identity card* tersebut dapat dilihat pada ilustrasi gambar 7.

3.3. Enkripsi pada *Contactless Smart Card*

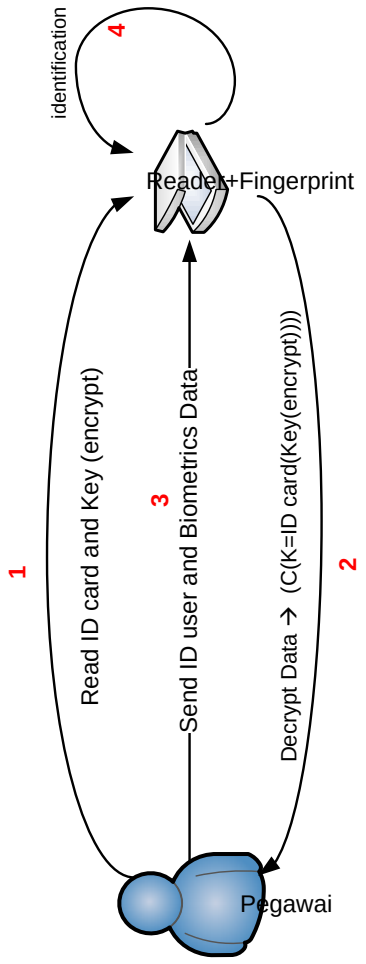
Penerapan kriptografi pada konsep *single identity card* adalah melakukan enkripsi data dan informasi yang tersimpan di dalam kartu dengan menggunakan metode algoritma block cipher. Dalam penerapan yang dilakukan oleh penulis adalah dengan melakukan kombinasi enkripsi bertingkat metode algoritma block cipher, yaitu metode EBC dan CBC. Kombinasi algoritma EBC dan CBC ini dipilih karena dalam penerapan ilmu kriptografi pada *embedded system*, hal yang utama bukan dari serumit apa algoritma kriptografi yang digunakan tetapi tingkat kerahasian dan kesukaran dari kunci enkripsi dan dekripsinya untuk didapatkan. Oleh karena itu penulis lebih memilih untuk mengombinasikan kedua metode algoritma tersebut, bukan dengan membuat algoritma baru. Karena dari segi keamanan sendiri, algoritma block cipher memiliki tingkat pemecahan kunci yang sukar, apalagi dengan pengimplementasian enkripsi block cipher bertingkat ini. Dimana kedua metode tersebut mempunyai karakter yang berbeda, hal tersebut dapat makin mempersulit kriptanalis untuk memecahkan kunci enkripsi – dekripsi agar mendapatkan plainteks data.

Solusi berikutnya agar dapat meningkatkan keamanan data dan informasi di dalam *single-identity card* tersebut adalah dengan tidak memberikan kunci enkripsi dan dekripsi yang sama di semua *identity card* pada sebuah organisasi atau perusahaan. Hal ini dilakukan untuk mencegah terjadinya penjarahan data secara massal, dalam artian apabila ada salah satu kartu yang terbongkar datanya, kunci yang ditemukan tidak dapat digunakan untuk membongkar data dari kartu lainnya. Untuk meningkatkan keamanan tersebut harus diterapkan konsep bahwa tiap *single-identity card* memiliki kunci enkripsi dan dekripsi yang berbeda-beda antara satu dengan yang lainnya. Pada penerapannya akan melakukan modifikasi pada alat *reader* sehingga mampu melakukan sebuah proses pengolahan data kecil. Kemudian akan melibatkan data-data yang melekat di dalam *single-identity card* masing-masing orang (tiap kartu pasti memiliki data

yang unik dan berbeda-beda) data tersebut diantaranya adalah:

- ID Card
- Key enkripsi-dekripsi data (ter-enkripsi)
- *Fingerprint* (autentifikasi)

Pada mesin reader akan ditanamkan sebuah algoritma kriptografi block cipher CFB yang digunakan untuk mendekripsi kunci enkripsi-dekripsi data *smart card.* Pada setiap kartu memiliki sebuah kunci enkripsi-dekripsi data yang ter-enkripsi terlebih dahulu oleh algoritma metode CFB dengan ID card sebagai kuncinya. Setelah membaca data dari kartu (ID card dan key ter-enkripsi) mesin *reader* akan mendekripsi kunci yang ter-enkripsi tersebut menggunakan ID card sebagai kunci dekripsi. Kemudian dengan kunci data yang sudah didekripsi oleh mesin *reader*, akan didapatkan data ID user pemilik kartu dan *biometrics* data untuk melakukan identifikasi. Secara garis besar, alur tersebut dapat dilihat di ilustrasi gambar 8.



gambar 8: Alur pembacaan data pada *single-identity card*

3.4. Potensi Pengembangan

Menurut analisis penulis bahwa konsep *single-identity card* ini tidak hanya sebatas sebagai kartu indetitas tunggal elektronik. Namun, banyak hal pengembangan dan inovasi melalui *single-identity card*, khususnya di dalam lingkup dan lingkungan organisisa pemerintahan ataupun perusahaan. Berikut beberapa pengembangan dan inovasi yang dapat dilakukan menurut analisis penulis:

- Dapat diimplementasikan sebagai sarana terintegrasi dengan sistem absensi karyawan atau pegawai.
- Menjadi kartu yang dapat digunakan untuk melakukan pengambilan gaji (terintegrasi dengan sistem keuangan).
- Sebagai tanda pengenal untuk *door-access* di lingkungan perkantoran.

Seiring dengan pengembangan dan inovasi penggunaan *single-identity card*, perlu juga untuk terus memperhatikan dan meningkatkan faktor keamanan data.

4. KESIMPULAN

Berdasarkan hasil analisis yang dilakukan oleh penulis, dapat diambil beberapa kesimpulan sebagai berikut:

1. Penggunaan *contactless smart card* sebagai *single-identify card* masih rawan terhadap tindak kejahatan dan penyalahgunaan data.
2. Sudah diterapkannya beberapa algoritma kriptografi untuk mengamankan data dan informasi di dalam *contactless smart card.*
3. Algoritma kriptografi modern mampu meningkatkan keamanan data pada *smart card* dengan mengkombinasikan metode algoritma ECB dan CBC secara bertingkat.
4. Tingkat keamanan dari enkripsi pada *embedded system* tergantung dari tingkat kesukaran dan kerahasian dari kunci enkripsi-dekripsi data, bukan dilihat dari kerumitan algoritma yang digunakan.
5. Kombinasi *contactless smart card* dengan fungsi autentifikasi *fingerprint* mampu meningkatkan keamanan penggunaan *single-identify card.*
6. Penerapan *unique key* untung masing-masing kartu dengan memanfaatkan ID card yang unik dapat meningkatkan keamanan data pada *single-identity card.*
7. Potensi pengembangan dan inovasi dari *single-identity card* yang begitu luas serta mampu meningkatkan kinerja sebuah

organisasi atau perusahaan, khususnya dalam bidang pengelolaan sumber daya manusianya.

REFERENCES

Agung, Gamma, Yusuf. 2005. *"Kajian Perkembangan Teknologi Smart Card dari Segi Keamanan dan Implementasinya di Kehidupan Sehari-hari".* Departemen Teknik Informatika, Institu Teknologi Bandung. Bandung.

Grand, Joe. 2004. *"Introduction to Embedded Security".* USA.

http://en.wikipedia.org/wiki/Electronic_identity_card (waktu akses: 19 Maret 2012, 05.00)

http://en.wikipedia.org/wiki/Contactless_smart_card (waktu akses: 19 maret 2010, 15.20)

Kandi, Jayavardhan. 2003. *"Embedde Cryptography: An Analysisi and Evaluation of Performance and code Optimization Techniques for Encryption and Decryption in Embedded Systems".* Departemen of Electrical Engineering, College of Engineering, University of South Florida.

Sariasih, Christine. 1999. *Rancangan Keamanan Data Sistem Smartcard Kesehatan, Sesuai Kebutuhan di Indonesia".* Fakultas Ilmu Komputer, Universitas Indonesia, Depok.

Securitie, Sagem. 2007. *"Contactless Card Specification".* Sarfan Group.

PERNYATAAN

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

Bandung, 20 Maret 2012

Lyco Adhy Purwoko – 13508027