Skema Pembangkitan Kunci Menggunakan Metode Biometrik Hibrid

Nur Adi Susliawan Dwi Caksono / 13508081
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If18081@students.if.itb.ac.id

***Abstract*— Identifikasi biometrik pada dunia kriptografi sangat berkaitan dengan hal-hal yang bersifat fisik atau perilaku dari individu manusia seperti suara, sidik jari, struktur muka, dll. Di interaksi kehidupan sehari-hari kita dengan orang lain secara langsung maupun tidak langsung secara implisit kita menggunakan konsep biometrik untuk mengetahui, membedakan dan mempercayai orang. Indentifier biometrik merupakan suatu konsep untuk mendapatkan karakteristik vital dari setiap orang yang tentunya berbeda satu sama lain seperti retina atau sidik jari. Pada makalah ini akan dijelaskan kemungkinan untuk menggunakan kombinasi dari atribut-atribut biometrik untuk menyelesaikan masalah yang ada apabila hanya menggunakan skema biometrik single untuk autentikasi. Akan dijelaskan pula mengenai skema yang mungkin dan fitur-fitur yang berkaitan dengan variasi di atribut biometrik.**

***Index Terms*—Biometrik, Konsolidasi, Hibrid**

I. PENDAHULUAN

Dewasa ini, sistem biometric telah banyak digunakan untuk mengatur hak akses seseorang dalam melakukan aksi tertentu seperti untuk verifikasi dengan metode scan retina ketika akan mengambil dokumen yang sifatnya rahasia yang disimpan di bank atau syarat masuk untuk memasuki suatu gedung. Namun komplikasi dalam penerapan skema pengenalan atribut fisik seperti sidik jari atau retina yang akurat telah membatasi penggunaan biometrik untuk transaksi keuangan. Dengan kata lain, ketepatan sistem sangat bergantung pada seberapa baik sistem biometrik digital dalam mencocokkan sifat fisik pengguna dalam berbagai kondisi.

Seperti yang telah diketahui secara umum, identifikasi dengan metode single biometric dimana pencocokan hanya dilakukan dengan satu atribut fisik tidak membuat level yang signifikan dalam tingkat keamanannya karena tidak semua orang memiliki atribut yang diminta dalam sistem biometric ini contohnya bagi orang yang cacat yang disebabkan oleh faktor lingkungan tentu saja tidak akan bisa menggunakan sistem biometrik ini. Hal inilah yang menjadi salah satu kendala dari sistem identifikasi dengan menggunakan single biometrik.

Masalah ini tentu saja dapat diatasi dengan menggunakan koleksi/kumpulan dari atribut biometrik atau biasa disebut dengan metode biometrik hibrid. Tingkat keunikan dan ketahanan terhadap penyalahgunaan sistem tentu saja harus diperhatikan untuk metode biometrik hybrid ini sehingga diperlukan aplikasi kriptografi biometrik yang ideal dalam menangani masalah ini. Untuk itulah peru disusun suatu mekanisme yang menggunakan seperangkat karakteristik yang pada saat yang sama dapat memastikan bahwa sistem ini mampu melayani dan beradaptasi dengan berbagai kondisi.

II. MASALAH DI BIOMETRIK HIBRID

Dalam skenario yang sifatnya real-time, misalkan terdapat satu himpunan atribut biometric B dan dari satu himpunan atribut B tersebut, setiap orang tidak mungkin dapat menghasilkan subset baru dari atribut himpunan tersebut. Kita harus dapat menangani situasi tersebut secara jelas. Sebagai contoh, asumsikan sebuah aplikai mendefinisikan himpunan biometrik B = {Iris, sidik jari, suara, password, wajah}. Pada contoh tersebut, orang yang mungkin tidak autentik dapat menghasilkan seluruh atribut B dengan subhimpunan S = {sidik jari, wajah, password}. Hal ini bisa disebabkan oleh perubahan atribut fisik seseorang atau karena pengaruh dari faktor eksternal. Korelasi antara S dan B merupakan tantangan yang besar. Pada suatu kasus, orang yang asli mungkin memberikan data biometric yang tidak lengkap. Dalam kasus seperti ni sistem harus dapat memutuskan apakah proses identifikasi telah menyimpan cukup informasi untuk autentikasi seseorang. Hal ini sangatlah penting dalam kasus-kasus ketika data biomterik hybrid digunakan untuk kunci pembangkitan yang digunakan dengan algoritma kriptografi standar.

Secara garis besar, masalah-masalah yang ada pada biometric hybrid ialah sebagai berikut :

- Mengekstraksi dan mewakili data biometrik yang dilakukan ketika proses pembangkitan kunci biometrik hibrida
- Menangani verifikasi data yang salah dan tidak lengkap

Walaupun penggunaan kriptografi data biometric masih tergolong baru namun pelaksanaan pembuatannya akhir-akhir ini tergolong sukses. Salah satu sistem tersebut ialah BIO-IBS, yang merupakan singkatan dari Biometric Identity Based Signature Scheme (Identitas Skema Berdasarkan Tanda Tangan Biometrik). Sistem ini efektif dalam penanganan perubahan terhadap data biometrik yang bervariasi lebih dari satu waktu. Davida et. al. menciptakan sebuah sistem yang menggunakan biometric atribut sebagai kunci. Berbeda dengan penelitian utama F.Hao dan CW Chan yang mepresentasikan metode untuk menghasilkan kunci dari tanda tangan tulisan tangan.

III. EKSTRAKSI DATA BIOMETRIK

Pengaturan sistem autentikasi biometric hybrid akan tersebar luas dan mencakup individu sub-sistem untuk mendapatkan data vital dari beberapa atribut pengguna tertentu. Sub-sistem akan membutuhkan alat yang mewakili ciri-ciri fisik dan selanjutnya juga metode yang digunakan untuk membandingkannya dengan template. Kehadiran data yang mengganggu (noisy data) menyebabkan kompleksitas sub-sistem akan bertambah. Langkah pertama ialah membandingkan variasi-variasi untuk mendeteksi data yang mengganggu (noisy data) tersebut.

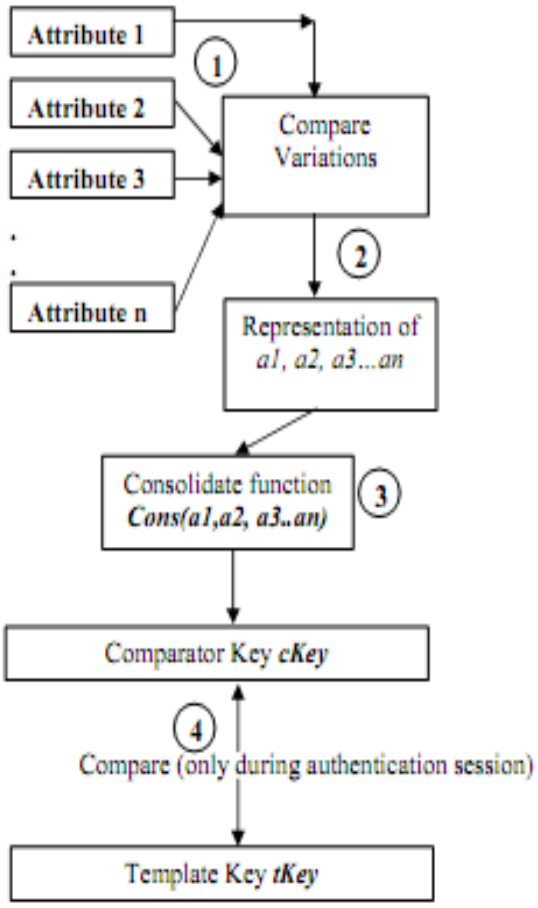
Dalam kasus mekanisme hibrida, template yang cocok untuk masing-masing sub-sistem hanya bagian dari seluruh proses keseluruhan. Pada tingkat yang lebih tinggi, perbandingan antara representasi dan template harus digunakan untuk konsolidasi hasil yang didistribusikan. Template utama akan menjadi kunci yang didefinisikan oleh pengguna dan harus cocok dengan agregasi pembentukan kunci yang diturunkan selama proses autentikasi. Perantara kunci pembanding dapat digenerasi berdasarkan beberapa fungsi yang dikenakan pada perkiraan ang saling tidak bergantung yang diperoleh dari berbagai sub-sistem. Sub-sistem dalam kasus ini dapat berupa perangkat seperti scanner sidik jari, scanner iris, dll.

Skema ini pada dasarnya memiliki empat tahapan penting yaitu :

- Memberikan informasi mengenai pendaftaran
- Melakukan perbandingan untuk mendetksi data-data yang mengganggu(noisy data).
- Aproksimasi representasi independent dari atribut-atribut yang diturunkan dari data yang mengganggu (noisy data).
- Konsolidasi dengan membuat perbandingan kunci yang ketat dari proses aproksimasi.

Perlu dicatat bahwa konsolidasi fungsi pertama kali diterapkan per individu pada proses pendaftaran. Selanjutnya, konsolidasi fungsi-fungsi ini diaplikasikan untuk setiap sesi autentikasi. Fungsi konsolidasi yang kompleks dapat menanamkan transformasi keamanan ekstra untuk menghindari serangan. Sebagai contoh, pada fungsi ini dapat ditambahkan bit ekstra untuk menghindari pembangkitan kunci yang sifatnya straight-forward.

IV. REPRESENTASI ATRIBUT



Gambar 1. Pembangkitan kunci hibrid

Seperti yang telah dijelaskan sebelumnya, skema representasi harus dapat mengatasi kemungkinan data yang menganggu(noisy data). Kombinasi yang aman untuk menangani noisy data pada pencocokan biometric ialah dengan mengkombinasikannya dengan menggunakan extractors fuzzy.

Setiap atribut biometric seperti password, wajah, sidik jari, atau retina diasumsikan memiliki ruang metric yang biasanya tidak terbatas. Namun untuk memudahkan dalam pengasumsian maka ruang metric dapat dijadikan dalam ruang metric yang terbatas. Hal ini akan membantu kita untuk mengetahui besar perbedaan antara setiap dua elemen dari ruang metric. Setiap elemen adalah representasi dari beberapa masukan biometric.Sebagai contoh variable M adalah metric ruang untuk semua jenis salah satu input biometric.

Sebuah sketsa yang aman misalkan dilambangkan dengan Sketsa SS dapat didefinisikan pada M. Sketsa yang aman adalah suatu peta yang betul-betul acak. Mari kita definisikan sebuah sketsa SS yang aman dimana SS memiliki parameter input w atau dalam notasi matematika dituliskan SS(w), dimana w adalah beberapa representasi (mungkin konstan). Menggunakan SS(w) dan beberapa pemulihan fungsi Rec deterministic mungkin untuk memperoleh w dari beberapa w' dimana w' sifatnya tertutup terhadap w,s ehingga dimugkinkan untuk menghitung jarak antara w dan w'. Dengan kata lain dimungkinkan untuk menentukan tingkat variasi yang dapat diterima diantara dua nilai yang merupakan atribut yang dimiliki oleh M. Penurunan w akan gagal jika vl > w-w', dimana vl adalah variasi yang diperbolehkan sedangkan w-w' adalah jarak antara w dan w' yang diukur berdasarkan metric Hamming dimana perbedaan jarak dapat memberikan pemahaman rinci mengenai metric ini. Dalam istilah yang sederhana, metric ini digunakan untuk mengevaluasi variasi dalam jumlah posisi bit dari dua masukan yang diberikan.

Sebuah sketsa yang aman dapat diperluas untuk membuat ekstraktor fuzzy. Ekstraktor fuzzy pada ruang metric M didefinisikan sebagai dua prosedur Gen (generator probabilistic), Rep (prosedur reproduksi). Fungsi generator menerima sebuah w input dan mengelurakan output berupa string R yang sudah terekstarksi dan juga string publik P. Prosedur reproduksi menggunakan variable output P dan input w' untuk mengekstraksi R. Variabel input w yang disebutkan disini merupakan atribut biometric yang dipresentasikan selama proses pendaftaran. Genereasi R dan P sangat bergantung pada logika yang dibangunke dalam fungsi Gen.

Karena skema diatas menghasilkan R yang definitive untuk input yang diberikan, maka metode ini dapat dimanfaatkan untuk menghasilkan identifier untuk menciptakan biometric yang disimpan sebagai template. Identifier ini kemudian dapat diambil dan diproses untuk membentuk kunci. Mari kita perhatikan langkah proses pendaftaran pada gambar 1. (langkah 1 pada gambar 1). Ini adalah fase dimana user melakukan pendaftaran dengan mendaftarkan data biometric yang akan disimpan oleh system. Skenario yang sebenarnya seharusnya dapat mencakup banyak biometric tetapi untuk menyederhanakannya, pada tahap ini kami menggunakan atribut biometric tunggla. Sebagai contoh data biometric yang didaftarkan oleh user adalah suara. Ketika pertama kali mendaftar, user akan membacakan sebuah kata sandi ke microfon. Suara ini akan menjadi inputan beberapa w yang merupakan metric dari ruang M dan dapat diwakilkan dengan menggunakan bit n. Ekstraktor fuzzy akan memanggil fungsi Gen dengan input w. Gen(w) akan menghasilkan beberapa R dan string public P. R yang diperoleh disini dapat digunakan sebagai template parsial atau dapat diubah berdasarkan beberapa fungsi yang telah ditetapkan. Seperti yang telah dijelaskan sebelumnya, hal ini dapat digunakan sebagai kunci utama. Pada kasus ini kami mengasumsikan hanya satu suara yang dikumpulkan dan rata-rata sampel ini didapatkan berdasarkan variasi antara satu sama lain yang dapat digunakan untuk menentukan w.

Untuk tahap representasi atribut (langkah 2 dalam gambar 1) nilai R setiap atribut diangap sebagai blok bangunan kunci utama. Dimisalkan atribut a1 diwakili oleh R1.

Fungsi konsolidasi dieksekusi baik selama pendaftaran maupun pada setiap sesi autentikasi. Fungsi konsolidasi terdiri dari beberapa fungsi hash. Sesi pendaftaran menggunakan fungsi ini untuk membangkitkan kunci. Sesi autentikasi akan berhasil jika pembanding kecocokan kunci disimpan oleh kunci yang lengkap. Oleh karena itu, setiap atribut biometric dengan range input {w'1, w'2, w'3…, w'n} yang semuanya tertutup terhadap w harus menggunakan fungsi recovery (Rec) dan public string untuk membangkitkan R. Ketika fungsi recovery menghasilkan hasil yang sukses untuk setiap atribut biometric, maka kita sangat yakin jika kunci ini sesuai. Hal ini dikarenakan input yang masuk ke fungsi konsolidasi selama proses pendaftaran dan autentikasi telah sesuai dan kunci pembanding dan kunci yang disimpan nilainya sama.

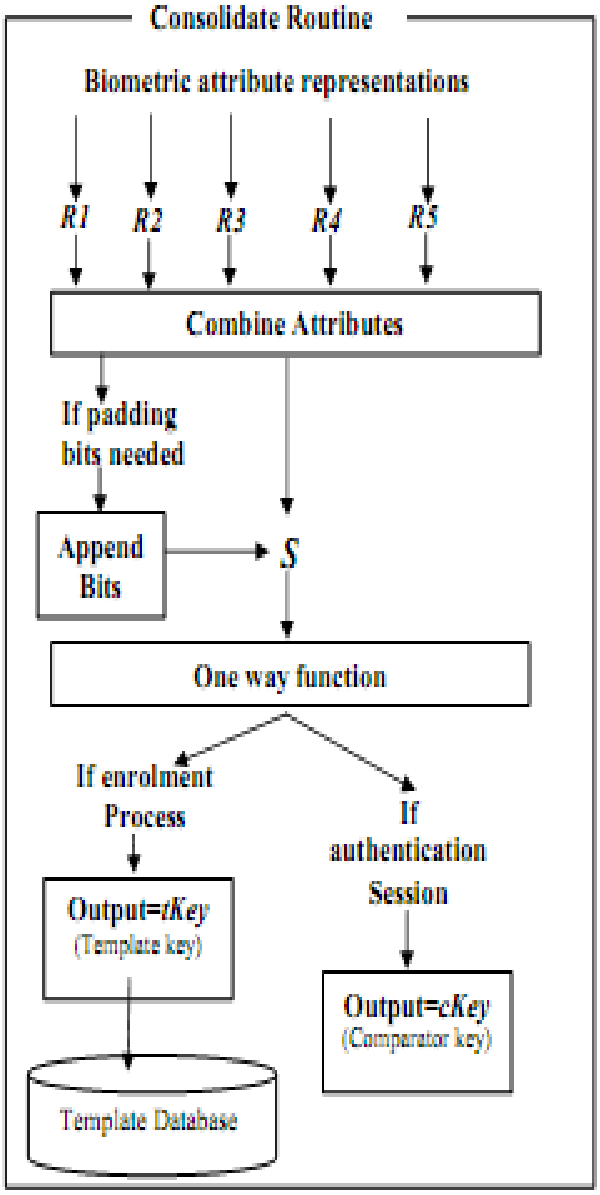
Selama fungsi konsolidasi dapat menentukan constraint untuk membuat kunci yang kompleks, level toleransi untuk setiap atribut biometric dapat didefinisikan di level end user. Level-level toleransi dapat secara bebas ditentukan dari himpunan ruang metrika dari semua variasi. Mari kita kembali pada kondisi w-w' < vl. Mendefinisikan range dari vl dapat menentukan level toleransi, Jika vl berasal dari range yang sangat kecil maka system akan lebih presisi dan lebih toleran. Sedangkan untuk range vl yang besar akan membuat system lebih rentan dalam menerima data-data yang error.

V. KONSOLIDASI

Fungsi konsolidasi akan melibatkan beberapa fungsi untuk melakukan proses terhadap atribut-atribut biometric. Fungsi ini akan menerima parameter berupa representasi biometric untuk n atribut fisik untuk menghasilkan kunci. Selama proses pendaftaran, proses konsolidasi menghasilkan template yang secara permanen disimpan. Fungsi konsolidasi juga mengeksekusi untuk setiap sesi autentikasi dan setiap sesi akan menghasikan kunci pembanding (cKey). Kunci ini akan digunakan untuk mengekripsi komunikasi secara real-time jika dan hanya jika kunci ini cocok dengan kunci template yang disimpan (cKey = tKey).

Fungsi konsolidasi akan menerima inputan berupa urutan bit awal dari nilai representasi R dari atribut-atribut biometric. Dari n atribut biometric kita akan memiliki satu himpunan Ri dimana i = {1…n}. Setiap

Ri mungkin dikenakan sedikit padding awal untuk mencapai urutan size yang tetap. Padding akan sesuai dengan aproksimasi dari panjang kunci output. Sekarang kita telah memiliki panjang bit string yang terbatas misalkan dengan variable S. S akan menjadi input dari fungsi untuk menghasilkan fungsi key. String ini akan dibagi ke dalam blok-blok. Fungsi ini akan melakukan serangkaian himpunan iterasi dan proses bit-wise untuk setiap blok S.



Gambar 2. Diagram alir fungsi konsolidasi

Pada sesi pendaftaran dengan fungsi konsolidasi user akan membuat dan menyimpan kunci ke dalam database template yang akan digunakan oleh fungsi konsolidasi yang sama untuk membandingkan string cKey dengan kunci yang disimpan di database tadi (template).

Biometrik merupakan suatu masalah yang presentasinya tidak konsisten yang bergantung pada bagaimana atribut disajikan dan diwakilkan. Sering kali, user yang valid tidak dapat menyajikan semua atribut-atribut yang akurat untuk mengasilkan perbedaan besar data biometric disajikan selama pendaftaran dan beberapa instance autentikasi. Misalkan terdapat kasus user menderita demam dan suaranya terganggu sehingga impikasinya terdapat variasi yang besar dari data voice user yang disimpan di database dengan voice user ketika akan melakukan autentikasi. Jika variable wvoice merupakan suara user pada kondisi sehat yang disimpan di database dan w'voice adalah suara user ketika menderita demam maka akan terdapat kemungkinan wvoice – w'voice > vlvoice. Jika kasus ini benar-benar terjadi maka hasil dari fungsi recovery dimisalkan saja dengan variable Rvoice ketika digunakan pada sketsa keamanan menjadi tidak dimungkinkan yang menyebabkan autentikasi akan gagal.

Metode sebelumnya dijelaskan bagaimana cara membuat template yang disimpan secara permanen dan kemudian digunakan untuk melakukan perbandingan. Tetapi apakah mungkin untuk membangkitkan kunci-kunci berdasarkan pada aturan atribut parsial dimana tantangan aturan atribut parsial adalah untuk memungkinkan akses ke orang dan mengeluarkan kunci yang tepat untuk transaksi-transaksi dalam kondisi user valid yang akan melakukan transaksi memiliki atribut biometric yang sesuai tetapi jumlahnya sedikit.

Untuk solusinya system ini akan menggunakan konsolidasi parsial yang berarti jika atribut n disajikan pada sesi autentikasi dan jika hanya ada beberapa n atribut yang deketahui cocok maka system akan mengabaikan atribut yang keliru dan hanya akan melakukan konsolidasi terhadap atribut yang benar. Oleh karena itu, kunci pembanding perantara tidak dapat cocok dengan beberapa template yang disimpan. Kunci template dibuat pada skema ini tidak digunakan untuk perbandingan tetapi langsung dibebaskan jika sebagian atribut cocok ketika dilakukan perbandingan.

Jika diasumsikan bahwa selama pendaftaran user mampu menyediakan semua atribut biometric yang ditentukan. Contoh, ketika proses pendaftaran, system akan melakukan prosedur pengecekan sidik jari, iris, suara, fitur wajah dan sandi. Pada saat pendaftaran, representasi untuk semua atribut akan dihasilkan yaitu Rvoice, Riris, Rfingerprints, Rfacial dan password. Representasi ini digunakan untuk membuat kunci dengan menggunakaan fungsi satu arah seperti yang sudah dijelaskan pada bagian sebelumya.

Ada beberapa constrait/kendala ketika kita berbicara masalah keamanan yang terkait dengan system ini mengingat bahwa seseorang dapat masuk ke dalam system melalui proses autentikasi dengan atribut yang hanya sedikit. Misalkan administrator system menetapkan

bawah setidaknya terdapat tiga dari lima atribut yang wajib agar dapat lolos dari autentikasi system. Administrator juga dapat menetapkan bobot untuk masing-masing atribut dan menetapkan untuk lolos proses autentikasi penjumlahan atribut-atribut yang benar harus lebih besar dari nilai tertentu. Misalkan untuk kasus 5 atribut kita menetapkan bobotnya seperti berikut :

Voice = 7, Iris = 4, Struktur Muka = 10, Sidik jari = 3, Password = 16

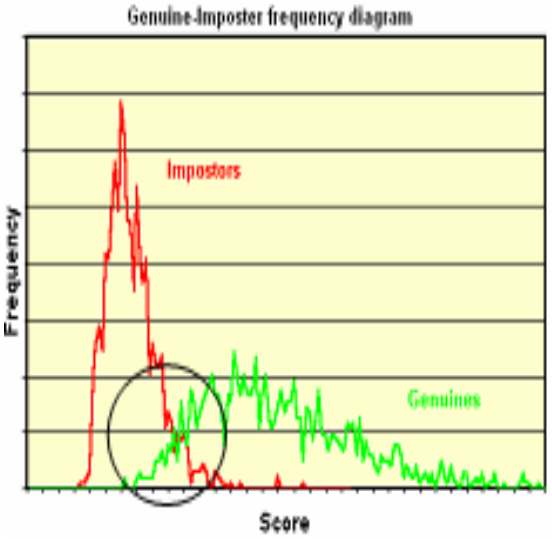
Mari kita misalkan constraint proses autentikasi sukses yaitu penjumlahan minimal dari bobot bernilai lebih dari/sama dengan 15 dan jumlah atribut yang wajib benar bernilai 3. Misalkan selama proses autentikasi, hanya 3 dari 5 atribut yang dinyatakan benar yaitu suara, iris dan sidik jari. Penjumlahan ketiga bobot ini bernilai 14 sehingga proses autentikasi akan gagal karena tidak memenuhi constraint pertama yaitu penjumlahan minimal dari bobot bernilai lebih dari/sama dengan 15 walaupun user memenuhi constraint kedua. Begitu juga untuk kasus proses autentikasi menemukan terdapat 2 atribut yang dinyatakan benar yaitu password dan suara. Penjumlahan kedua atribut ini bernilai 23 yang tentu saja memenuhi constraint pertama tetapi proses autentikasi tetap akan dinyatakan gagal karena jumlah atribut tidak memenuhi constraint kedua.

Setiap atribut-atribut yang diajukan selama autentikasi akan diperiksa agar memenuhi constraint Rn-vln < R'n dan atribut apapun yang melanggar constaraint ini akan dibuang. Fungsi konsolidasi parsial akan menerima parameter input berupa penjumlahan bobot dan fungsi ini akan menunjukkan atribut mana yang memiliki kecocokan yang benar-benar sempurna. Misalkan atribut-atribut yang dideteksi ketika proses autentikasi adalah struktur muka, sidik jari dan password yang berarti penjumlahan bobot dari ketiga atribut tersebut bernilai 29. Bobot yang melekat pada atribut tersebut dimanipulasi sedemikian rupa sehingga penjumlahan kombinasi yang unik membuatnya semakin mudah untuk mengidentifikasi atribut-atribut yang cocok.

Pada saat ini, fungsi konsolidasi dapat menggunakan fungsi satu arah untuk membangkitkan kunci dinamis hanya menggunakan atribut-atribut yang cocok. Secara alternative, hal ini dapat dilakukan dengan merilis kunci static yang disimpan yang dibuat dengan menggunakan semua n atribut ketika proses pendaftaran dilakukan. Ketika atribut-atribut yang ada lebih sedikit dari yang seharusnya maka metode ini memerlukan padding bit untuk membuat panjang kunci yang aman.

V. TEST EFISIENSI

Sebuah metode untuk mengevaluasi kinerja system verifikasi biometric adalah dengan menyajikan user yang banyak baik itu user yang benar benar memiliki hak akses dan user yang tidak memiliki hak akses dan menghitung kesamaan rating dengan referensi yang tersimpan.



Gambar 3. Digaram Frekuensi User Asli-User Penipu pada Sistem Autentikasi Single Biometrik

Dalam kasus ini, acuan yang disimpan adalah himpunan representasi digital untuk beberapa atribut biometric yang disimpan selama pendaftaran.

Gambar diatas merupakan grafik yang berasal dari Biometrics FAQ dan menunjukkan diagram frekuensi penipu yang berlaku pada system atribut single biometric. Seperti yang terlihat di bagian yang dilingkari, terdapat dua kurva yang saling berpotongan yang menunjukkan disanalah ancaman penipu untuk mendapatkan akses. Untuk kasus terbaik, kedua kurva tersebut seharusnya tidak berpotongan. Di system autentikasi single biometric, hal ini tidak dimungkinkan.

Namun, system yang ditawarkan disini dapat melakukan penyelidikan dengan cara mencoba untuk menghilangkan tumpang tindih yang dialami oleh kedua kurva. Karena serangan yang sempurna didasarkan pada atribut yang multiple, maka hal ini dapat menjadi dasar untuk mengevaluasi system ini.

Autentikasi single biometrik dapat diserang dengan menggunakan metode hill-climbing. Solusinya ialah dengan menambah atribut-atribut untuk autentikasi dan menggunakannya dalam konjungsi dengan fungsi hash dapat mengurangi atau menghilangkan ruang gerak dari serangan.

V. KESIMPULAN

Skema untuk menggunakan banyak atribut fisik manusia untuk membuat kunci telah dapat diimplementasikan. Menggabungkan biometric dan krptografi merupakan sesuatu yang sifatnya baru dan mengambil pengaruh pada kemanan komunikasi yang sifatnya sudah sangat canggih. Metode-metode yang

disajikan masih tergolong kedalam fase penelitian dan sedang diteliti lebih lanjut dari segi perspektif matematika. Pada saat kita berkonsentrasi pada masalah implementasi kita akan berusaha untuk mengurangi overhead-overhead yang kompleks dalam mengatur operasi pembangkitan kunci menggunakan biometric. Metode-metode yang digunakan untuk menangani data biometric hybrid sepertinya bersifat straightforward tetapi kerumitan perhitungan untuk meng-embed keamanan yang benar-benar aman pada system sangatlah rumit. Fokus pada makalah ini ialah bagaimana kita mengatur representasi data biometric yang besar dan kompleksitas waktu dari proses konsolidasi untuk membangkitkan kunci, dan mengatur constraint pada sesi autentikasi

REFERENSI

- http://www.m2sys.com/hybrid-biometric-platform.htm
- http://spie.org/documents/Newsroom/Imported/001590/001590_10.pdf
- Federal Financial Institutions Examination Council "Authentication in an electronic banking environment". Available www.ffiec.gov/pdf/pr080801.pdf
- A. Jain, R. Bolle, and S. Pankanti, Biometrics : Personal identification in networked society Kulwer Academic publishers, 1999
- A. Burnett, A. Duffy, T. Dowling, "A biometric identity based signature scheme" Cryptology ePrint Archive, available at http://eprint.iacr.org/2004/176

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

Nur Adi Susliawan D C
13508081