Penerapan *Fuzzy Logic* untuk Penilaian Tingkat Keamanan *Online Store*

Reinhard Denis Najogie - 13509097
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13509097@std.stei.itb.ac.id

Abstrak—*Online store* adalah situs yang memfasilitasi pertemuan antara penjual dan pembeli barang dan/atau jasa melalui internet. Walaupun *online store* memberikan banyak kemudahan dan keuntungan bagi pihak pembeli dan penjual, penggunaan *online store* juga memiliki kekurangan terutama dalam tingkat keamanan. Banyak kasus kerugian yang diakibatkan adanya celah keamanan pada sistem *online store*. *Fuzzy logic* adalah konsep logika yang mendasari *Fuzzy Inference System* (FIS), yaitu sistem pengambil keputusan yang menyerupai cara manusia mengambil keputusan. Dalam makalah ini akan dijelaskan desain FIS sederhana untuk menentukan tingkat keamanan *online store*. FIS ini akan mengkategorikan sebuah *online store* ke dalam lima tingkat keamanan: rendah, agak rendah, sedang, agak tinggi, dan tinggi..

Kata Kunci—*online store, fuzzy logic, fuzzy inference system*

1. Pendahuluan

Transaksi jual-beli barang dan/atau jasa merupakan hal yang mendasari kegiatan ekonomi suatu negara. Dengan berkembangnya teknologi komputer dan internet, transaksi jual-beli inipun banyak terjadi secara *online*. Ada situs yang berbentuk *online store*, dimana pihak penjual mendaftarkan segala barang jualannya dan pembeli tinggal memilih, ada juga situs yang hanya menyediakan fasilitas komunikasi antara penjual dan pembeli, sehingga penjual dan pembeli bebas berkomunikasi dan bertransaksi, dimana situs seperti ini biasanya berbentuk *online forum*. Adanya sistem transaksi jual-beli secara *online* ini membawa berbagai keuntungan baik kepada penjual maupun kepada penjual. Seorang penjual dapat menjangkau pembeli yang jaraknya jauh dan tidak mungkin bisa membeli barangnya secara langsung. Selain itu, penjual juga dapat mengurangi biaya sewa gedung/ruko yang digunakan sebagai toko tempat pembeli mencari barang, penjual hanya perlu mencari tempat penyimpanan barang sementara atau gudang. Tidak lupa juga, kesempatan promosi gratis yang didapatkan melalui pelanggan yang senang akan layanan sang penjual. Sementara dari sudut pandang pembeli, pembeli bisa menjangkau penjual yang berada jauh jaraknya, dapat lebih mudah membandingkan spesifikasi dan harga dari barang yang diinginkan, serta lebih nyaman dalam melakukan transaksi karena tidak harus mengunjungi toko tempat barang dijual dan mengantri saat pembayaran.

Terlepas dari segala kemudahan dan keuntungan yang ditawarkannya, *online store* juga memiliki hambatan yang membuat pembeli dan penjual masih takut dan ragu-ragu untuk menggunakan sistem ini. Hambatan itu adalah masalah keamanan. Transaksi jual-beli melalui internet memiliki resiko tinggi terutama bagi pengguna yang awam dan tidak terlalu mengerti mengenai masalah keamanan bertransaksi di internet. Mulai dari pencurian ID dan password akun *online store*, pencurian nomor kartu kredit, DoS (*Denial of Service*), SQL *injection*, hingga *social engineering* atau penipuan yang cerdik.

Untuk mengurangi kerugian dan dampak negatif yang dapat diakibatkan oleh transaksi *online*, penulis memiliki solusi untuk merancang suatu sistem yang bisa menentukan tingkat keamanan suatu *online store*. Sistem ini akan berbasis *fuzzy logic*, dengan beberapa alasan. Pertama, dengan *fuzzy logic* perhitungan variabel yang mempengaruhi keamanan *online store* dapat dilakukan dengan lebih sederhana karena *fuzzy logic* tidak memerlukan nilai kuantiatif yang presisi. Kedua, sistem inferensi dengan *fuzzy logic* dapat di perbaharui dengan mudah jika ada perubahan dasar pengambilan keputusan, misalnya jika ada tipe ancaman keamanan baru yang belum ada sebelumnya, atau jika nilai suatu ancaman bertambah. Ketiga, hasil inferensi berbasis *fuzzy logic* sudah banyak dipercaya dan digunakan dalam berbagai penelitian bahkan produk dengan banyak konsumen seperti barang-barang elektronik, terutama di negara Jepang. Lebih detail mengenai statistik penggunaan *fuzzy logic* dapat dilihat di [1].

2. Dasar Teori

Pada bagian ini akan dibahas mengenai masalah yang

mengancam keamanan *online store*, serta dasar teori dari *fuzzy logic* dan *fuzzy inference system*.

2.1 Ancaman Keamanan *Online Store*

Dalam keamanan *online store* pada khususnya dan keamanan situs internet pada umumnya, ada beberapa kategori jenis ancaman serangan yang umum digunakan, disini penulis menggunakan poin yang sama dengan yang digunakan oleh M. Aburrous, dkk. dalam [2].

2.1.1 *Direct Internal Attack*

Masuk dalam kategori ini adalah *phishing attack*, *social engineering*, *brute force*, serta *insider attack*. *Phishing attack* adalah tipe serangan dengan cara mengelabui pengguna situs dengan membuat mereka mengira situs yang mereka kunjung adalah situs asli dari penjual, dengan tampilan yang sama persis dan biasanya menggunakan nama domain yang dimiripkan dengan domain aslinya. *Social engineering* adalah cara menipu yang cerdik, biasanya dengan menghimpun data tentang calon korban dan mengarang-ngarang cerita untuk mengelabui korban. *Brute force* adalah serangan dengan mencoba segala kombinasi karakter untuk mengisi username dan password. *Insider attack* adalah serangan dari pihak dalam, biasanya berupa seorang pegawai perusahaan *online store* yang ingin mengambil keuntungan sendiri.

2.1.2 *Communication Tampering Attack*

Masuk dalam kategori ini adalah *sniffing*, *spoofing*, *port scan*, serta *page hijacking*. *Sniffing* adalah aktifitas mengawasi lalu-lintas data pada jaringan. Jika data tidak dienkripsi, maka informasi dapat dengan mudah dibaca oleh pihak luar. *Spoofing* adalah penyamaran suatu pihak sehingga ia dikenal sebagai pihak lain, biasanya dengan tujuan mendapat *privilege* teretentu. *Port scan* adalah aktifitas mencari *port* yang terbuka dan dapat ditembus oleh pihak penyerang. Sementara *page hijacking* adalah jenis search engine index spamming, dilakukan dengan cara membuat situs web crawler tiruan yang berisi tautan ke situs yang berbahaya.

2.1.3 *Code Programming Attack*

Masuk dalam kategori ini adalah SQL *injection*, *buffer overflow*, *cross site scripting*, serta *Trojan horse*. SQL *injection* adalah serangan dengan kode SQL yang biasanya digunakan untuk mem-bypass form login. SQL *injection* sudah jarang ditemukan, akan tetapi webmaster yang tidak berpengalaman bisa saja lupa menangani hal ini. *Buffer overflow* terjadi ketika situs diberikan query string yang sangat panjang sehingga struktur data situs tidak mampu menampungnya. *Cross site scripting* atau biasa disebut XSS adalah tipe serangan yang biasa dilakukan dengan cara memasukkan client-side script pada halaman situs yang dilihat oleh pengguna lain. *Trojan horse* adalah program yang terlihat seperti program yang aman, padahal sebenarnya mengandung kode yang berbahaya.

2.1.4 *Denial of Service Attack*

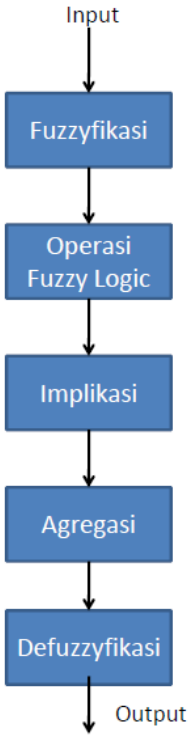
Masuk dalam kategori ini adalah *ping of* death, *ping flood*, *man in the middle*, serta *smurf attack*. *Ping of* death merupakan bentuk serangan dengan cara mengganti jenis *ping* yang biasa diterima komputer. Paket *ping* biasanya berukuran 32 byte, jika ada paket lebih besar dari ukuran itu maka komputer akan crash. Serangan ini bisa dikatakan sejarah karena komputer sekarang sudah diprogram untuk bisa mengatasi masalah *ping of* death. *Ping flood* adalah serangan DoS sederhana dimana penyerang menyerang korban dengan terus-menerus mengirimkan paket ICMP untuk membuat komputer korban sibuk dan tidak dapat melayani request lain. *Man in the middle* adalah tipe penyadapan dimana penyerang membuat koneksi sendiri diantara korban yang sedang melakukan komunikasi dan membuat mereka merasa sedang melakukan komunikasi dengan orang yang tepat. *Smurf attack* adalah tipe serangan dengan cara menghabiskan traffic dari jaringan komputer korban yang biasanya diimplementasikan dengan membanjiri sistem dengan broadcast *ping* message yang telah di-spoof.

2.2 *Fuzzy Logic*

Fuzzy logic adalah konsep logika probabilistik. Tidak seperti konsep logika konvensional yang hanya mengerti nilai benar atau salah, *fuzzy logic* mengerti nilai logika yang berupa aproksimasi. Jika pada logika konvensional nilai benar atau salah direpresentasikan dengan nilai 0 atau 1, maka pada *fuzzy logic* nilai kebenaran berupa bilangan real diantara 0 dan 1. Oleh karena itu bahasan *fuzzy logic* sering juga disebut dengan kebenaran parsial, dimana nilai kebenaran berada diantara sepenuhnya benar dan sepenuhnya salah. Hal ini dijelaskan oleh Novák, dkk. dalam [3].

Dengan dasar *fuzzy logic*, sekarang dapat dijelaskan tentang *fuzzy inference system* (FIS). FIS adalah sebuah sistem yang mampu menarik kesimpulan dari sekumpulan kaidah *fuzzy*. Kaidah *fuzzy* berarti tidak diperlukan adanya perhitungan yang eksak dalam penentuan keanggotaan sebuah variabel ke dalam himpunan *fuzzy*. Oleh karena itu FIS disebut mirip dengan cara manusia menarik kesimpulan, karena manusia biasanya tidak menghitung sampai detail segala variabel yang ada untuk mengambil suatu keputusan.

Dalam suatu FIS minimal ada dua kaidah *fuzzy*, yaitu masukan dan keluaran. FIS menerima masukan berupa nilai crisp (nilai numerik) dan juga mengeluarkan keluaran berupa nilai crisp. Tentunya dalam FIS sendiri ada pemrosesan lebih lanjut untuk mengolah nilai masukan menjadi nilai keluaran. Proses yang terjadi dalam FIS bisa dilihat pada gambar berikut:



Gambar 1 – Alur kerja FIS. Sumber : [4]

Seperti yang sudah dijelaskan sebelumnya, FIS menerima masukan dan menghasilkan keluaran. Karena nilai masukan FIS berupa nilai crisp, hal yang pertama perlu dilakukan adala fuzzifikasi, yaitu mentransformasikan nilai crisp menjadi nilai *fuzzy*. Pada tahap ini akan ditentukan membership function atau fungsi keanggotaan sebuah variabel pada suatu rentang nilai tertentu. Setelah itu akan dilakukan operasi *fuzzy logic* (biasanya berupa logika AND dan/atau OR). Dalam *fuzzy logic*, karena nilai kebenaran berupa nilai real, maka logika AND akan mengembalikan nilai minimal dari kedua nilai masukan, sementara logika OR akan mengembalikan nilai maksimal dari kedua nilai masukan. Setelah operasi *fuzzy logic*, dilakukan implikasi. Implikasi dilakukan dengan aturan-aturan (rule) yang sudah dibuat sebelumnya. Aturan dari implikasi adalah mengambil nilai maksimal dari antesenden dan konsekuen, sama seperti logika OR. Setelah itu ada agregasi atau menggabungkan semua nilai *fuzzy* dari keluaran implikasi dari seluruh aturan yang ada. Ada dua metode yang biasa digunakan pada tahap ini, yaitu metode Mamdani dan metode Sugeno. Pada metode Mamdani, akan dilakukan fungsi min pada implikasi dan max pada agregasi, atau biasa disebut metode min-max. Metode ini akan menghasilkan daerah di bawah kurva hasil agregasi. Sementara pada metode Sugeno, hasil agregasi berupa singleton-singleton, bukan daerah di bawah kurva seperti pada metode Mamdani.

3. Perancangan Sistem

Dari empat jenis ancaman keamanan *online store* yang telah dipaparkan pada bagian dasar teori, akan diambil dua untuk dijadikan variabel masukan pada FIS yang akan dibangun. Tujuan pengambilan dua ancaman dari empat ancaman yang ada adalah untuk menyederhanakan desain FIS yang dibangun tanpa menghilangkan tujuan awal untuk menentukan tingkat keamanan dari *online store*. Dua ancaman yang akan diambil adalah *direct* internal *attack* dan *code programming attack*. Dua ancaman ini akan menjadi variabel input dari FIS. Sementara variabel output FIS adalah, sesuai dengan tujuan awal, yaitu tingkat keamanan dari *online store*.

Langkah pertama dalam mendesain FIS *online store* adalah mendefinisikan fungsi keanggotaan dari setiap variabel yang ada pada sistem. Untuk FIS *online store* akan ada tiga variabel, dua input dan satu output. Variabel input yaitu tingkat *direct internal attack* (untuk selanjutnya akan disebut sebagai DIA) dan tingkat *code programming attack* (untuk selanjutnya akan disebut sebagai sebagai CPA). Sementara variabel output tingkat keamanan selanjutnya akan disebut sebagai SAFETY pada sistem.

Penulis mengimplementasi FIS dengan bantuan fitur *Fuzzy ToolBox* yang ada pada perangkat lunak MATLAB. Penulis menggunakan perangkat lunak MATLAB versi 7.12.0. Untuk memperjelas desain FIS yang akan dibuat, pada bagian berikutnya dari makalah ini akan banyak mengambil cuplikan layar (*screen shot*) dari FIS yang dirancang.

Pertama-tama desain FIS dimulai dengan memilih strategi merancang fungsi keanggotaan. Sesuai dengan definisi awal *fuzzy logic*, nilai keluaran fungsi akan berkisar dari 0 hingga 1. Dari 6 strategi perancangan fungsi keanggotaan yang ada menurut Timothy J. Ross [5], akan digunakan cara pertama, yaitu intuisi. Dengan intuisi akan digunakan pemahaman kontekstual dan semantik dari permasalahan untuk merancang fungsi keanggotaan dari suatu variabel, dalam hal ini permasalahan keamanan *online store*.

Nilai masukan untuk variabel DIA dan CPA akan berupa tingkat permasalahan yang diakibatkan oleh kedua variabel ancaman tersebut. Sementara itu bilai keluaran variabel SAFETY berupa tingkat keamanan hasil inferensi sistem. Dalam hal ini ketiga variabel di atas akan dikategorikan dalam 5 jenis tingkatan sebagai berikut:

- Rendah (R)

- Agak Rendah (AR)
- Sedang (S)
- Agak Tinggi (AT)
- Tinggi (T)

Dimana aturan inferensinya dapat dilihat dalam tabel berikut:

DIA	CPA					
		T	AT	S	AR	R
	T	R	R	AR	AR	S
	AT	R	R	AR	S	AT
	S	AR	AR	S	AT	AT
	AR	AR	S	AT	T	T
	R	S	AT	AT	T	T
SAFETY						

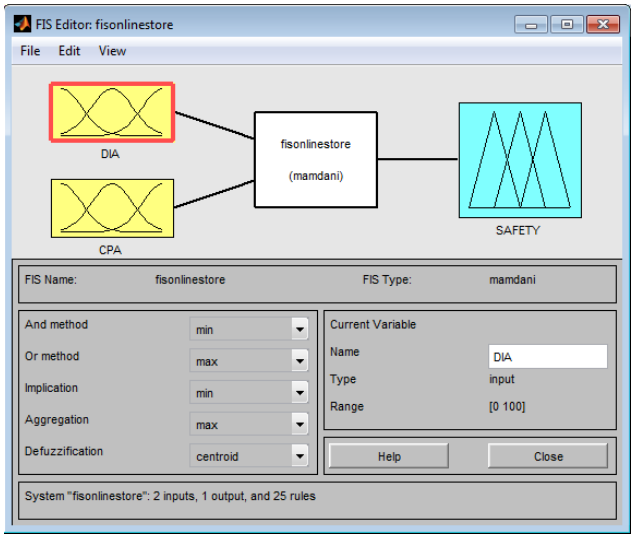
Tabel 1 – Aturan inferensi FIS *online store*

Dapat dilihat dari tabel inferensi di atas bahwa sistem akan memiliki 5 x 5 = 25 aturan inferensi yang digunakan sebagai basis pengambilan keputusan akhir dari sistem.

4. Implementasi Sistem dan Analisis

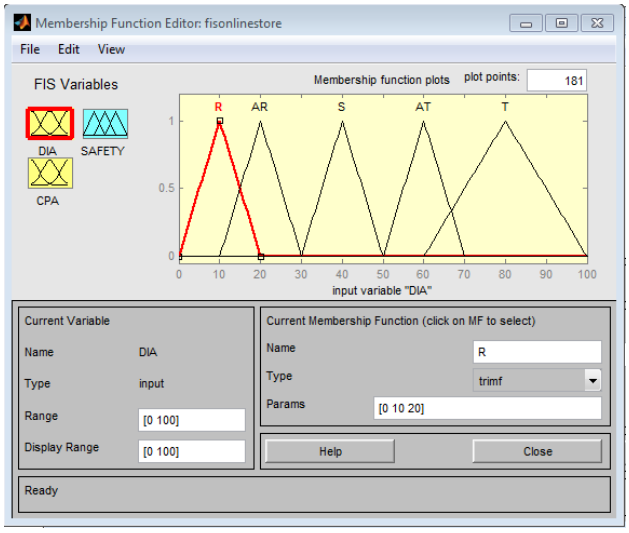
Setelah mengetahui variabel yang akan ada di FIS beserta aturan inferensinya kita bisa memulai implementasi FIS tersebut dalam *Fuzzy ToolBox* MATLAB. Dari *command line* MATLAB, kita bisa mengakses *Fuzzy ToolBox* dengan cara memasukkan command *fuzzy*. Setelah itu, *Fuzzy ToolBox* akan keluar dan kita bisa mengkonfigurasi sistem *fuzzy* yang akan kita bangun dengan menambah variabel-variabel yang diperlukan. Untuk menambahkan variabel bisa dilakukan melalui menu edit > add rule.

Berikut gambaran awal sistem:



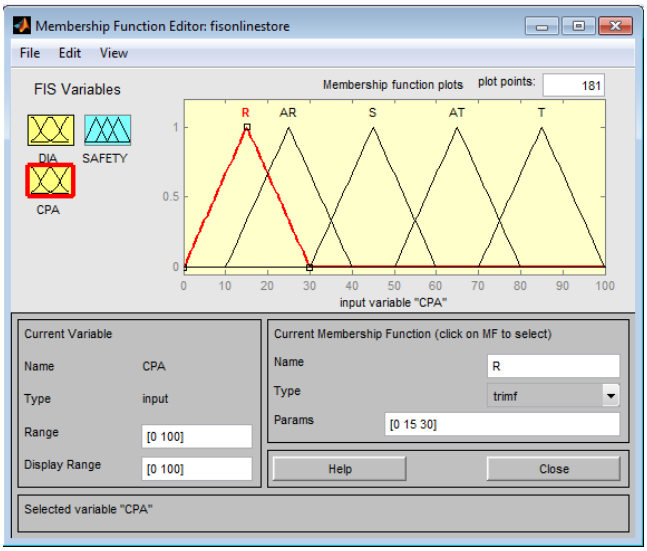
Gambar 2 – Struktur FIS *online store*

Selanjutnya fungsi keanggotaan dari variavel DIA, CPA, dan SAFETY dapat dilihat dari gambar-gambar yang diperlihatkan di bawah. Kebanyakan fungsi keanggotaan ini bertipa fungsi triangular (fungsi berbentuk segitiga). Berikut gambar fungsi keanggotaan dari variabel DIA:



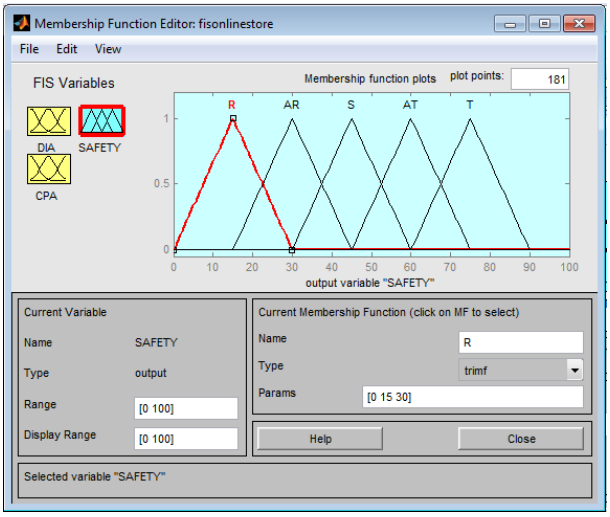
Gambar 3 – Fungsi keanggotaan variabel DIA

Fungsi keanggotaan dari variabel CPA digambarkan sebagai berikut:



Gambar 4 – Fungsi keanggotaan variabel CPA

Fungsi keanggotaan dari variabel SAFETY digambarkan sebagai berikut:

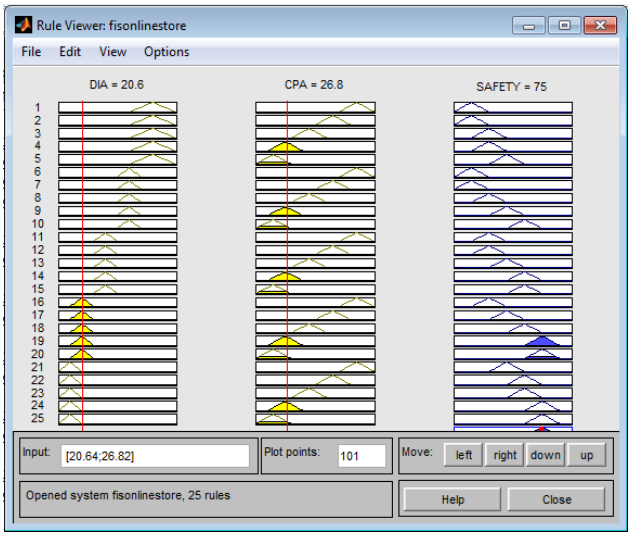


Gambar 5 – Fungsi keanggotaan variabel SAFETY

Setelah memasukkan nilai fungsi keanggotaan dari ketiga variabel dalam sistem, langkah selanjutnya adalah memasukkan aturan-aturan untuk langkah inferensi sistem. Untuk memasukkan dan menambahkan aturan pada sistem bisa dilakukan melalui menu edit > rules. Selanjutnya akan muncul antarmuka untuk menambahkan aturan. Disinilah tempat dimasukkannya aturan-aturan yang ada dalam Tabel 1 pada bagian Perancangan Sistem makalah ini. Secara detail, 25 aturan yang dimasukkan adalah sebagai berikut:

1. If (DIA is T) and (CPA is T) then (SAFETY is R)
2. If (DIA is T) and (CPA is AT) then (SAFETY is R)
3. If (DIA is T) and (CPA is S) then (SAFETY is AR)
4. If (DIA is T) and (CPA is AR) then (SAFETY is AR)
5. If (DIA is T) and (CPA is R) then (SAFETY is S)
6. If (DIA is AT) and (CPA is T) then (SAFETY is R)
7. If (DIA is AT) and (CPA is AT) then (SAFETY is R)
8. If (DIA is AT) and (CPA is S) then (SAFETY is AR)
9. If (DIA is AT) and (CPA is AR) then (SAFETY is S)
10. If (DIA is AT) and (CPA is R) then (SAFETY is AT)
11. If (DIA is S) and (CPA is T) then (SAFETY is AR)
12. If (DIA is S) and (CPA is AT) then (SAFETY is AR)
13. If (DIA is S) and (CPA is S) then (SAFETY is S)
14. If (DIA is S) and (CPA is AR) then (SAFETY is AT)
15. If (DIA is S) and (CPA is R) then (SAFETY is AT)
16. If (DIA is AR) and (CPA is T) then (SAFETY is AR)
17. If (DIA is AR) and (CPA is AT) then (SAFETY is S)
18. If (DIA is AR) and (CPA is S) then (SAFETY is AT)
19. If (DIA is AR) and (CPA is AR) then (SAFETY is T)
20. If (DIA is AR) and (CPA is R) then (SAFETY is T)
21. If (DIA is R) and (CPA is T) then (SAFETY is S)
22. If (DIA is R) and (CPA is AT) then (SAFETY is AT)
23. If (DIA is R) and (CPA is S) then (SAFETY is AT)
24. If (DIA is R) and (CPA is AR) then (SAFETY is T)
25. If (DIA is R) and (CPA is R) then (SAFETY is T)

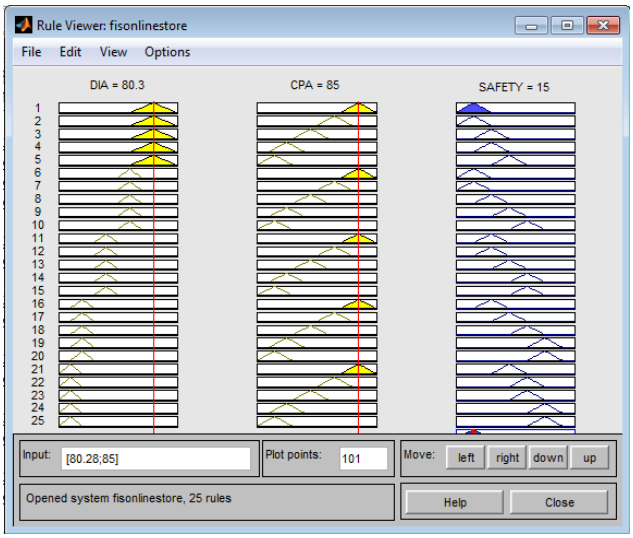
Setelah memasukkan 25 aturan di atas, kita dapat melihat hasil agregasi dari menu view > rules. Dalam menu ini tahap agregasi dan defuzzifikasi sekalian terjadi, dan untuk mengubah-ubah nilai masukan kita tinggal menggeser garis yang ada pada tiap variabel masukan. Berikut gambar hasil inferensi dengan nilai masukan DIA = 20.6 dan CPA = 26.8.



Gambar 6 – Hasil inferensi Mamdani dengan DIA = 20.6 dan CPA = 26.8

Bisa dilihat bahwa nilai SAFETY = 75, yang artinya kurang lebih dengan tingkat DIA sebesar 20.6 dan CPA sebesar 26.8, tingkat keamanan *online store* tersebut adalah 75 atau secara kualitatif terletak diantara tingkat keamanan agak tinggi (AT) dan tinggi (T).

Lalu berikut hasil inferensi dengan masukan DIA = 80.3 dan CPA = 85.

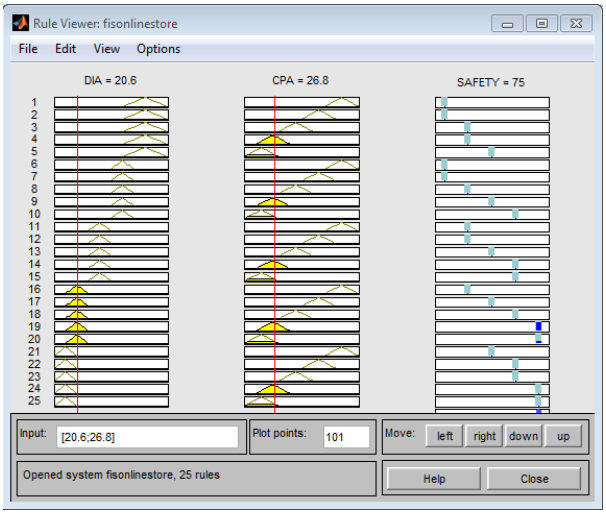


Gambar 7 – Hasil inferensi Mamdani dengan DIA = 80.3 dan CPA = 85

Dapat dilihat bahwa nilai SAFETY = 15. Hal ini sudah sesuai dengan penalaran bahwa semakin tinggi resiko DIA dan CPA pada suatu *online store*, maka semakin rendah tingkat keamanannya.

Sekarang akan dibandingkan hasil inferensi dengan metode Sugeno dengan masukan DIA = 20.6 dan CPA = 26.8, seperti contoh sebelumnya yang diagregasi dengan

metode Mamdani.



Gambar 8 – Hasil inferensi Sugeno dengan DIA = 20.6 dan CPA = 26.8

Bisa dilihat bahwa hasilnya sama yaitu SAFETY = 75. Perlu diingat metode Sugeno memiliki cara agregasi yang berebeda dengan metode Mamdani dan tidak selalu menghasilkan hasil yang sama. Dalam contoh di atas, kebetulan hasil inferensinya sama. Mengenai metode mana yang lebih baik, akan sulit untuk membandingkannya, karena kita membicarakan *fuzzy logic*, dimana nilai kebenarannya *fuzzy* atau samar-samar. Ada baiknya dalam merancang suatu FIS kita membuat versi Mamdani dan Sugeno nya sebagai bahan perbandingan.

5. Kesimpulan dan Pengembangan Lebih Lanjut

Dalam makalah ini telah dibahas rancangan sistem penilai tingkat keamanan suatu *online store* dengan *fuzzy logic* serta implementasinya dengan perangkat lunak MATLAB. Tentu untuk penggunaan secara praktisnya untuk menilai tingkat keamanan suatu *online store* tidak cukup dengan sistem yang sudah diimplentasikan di atas. Sistem yang telah dibangun di atas memiliki satu kekurangan untuk langsung digunakan untuk menilai tingkat keamanan suatu *online store*, yaitu masukan nilai DIA dan CPA harus dilakukan secara manual. Strategi dan cara mendapatkan nilai ini berada di luar cakupan makalah ini. Bagi pembaca yang ingin mempelajari cara mendapatkan nilai masukan ini dapat menggunakan perangkat lunak khusus yang dirancang untuk menemukan celah-celah teknis keamanan yang ada pada suatu situs *online store* seperti Acunetix [6].

Untuk pengembangan lebih lanjutnya sistem yang telah dibangun dapat ditingkatkan akurasinya dengan cara menambah variabel masukan. Variabel masukan tambahan ini dapat berupa dua poin lain yang ada pada bagian 2.1 yaitu CTA (Communication Tampering *Attack*) dan DoS (*Denial of Service*) maupun variabel lain yang dirasa mempengaruhi tingkat keamanan suatu *online store* seperti penyedia hosting situs, CMS (*Content Management System*), domain situs, dan sebagainya. Namun, perlu diketahui bahwa dengan menambah variabel masukan maka perancangan aturan-aturan inferensi akan bertambah kompleks karena jumlah aturan yang harus dimasukkan akan bertambah secara signifikan.

Referensi

[1] http://www.cs.berkeley.edu/~zadeh/stimfl.html - diakses pada 12 Mei 2012 pukul 10.00.

[2] M. Aburrous, M. A. Hossain, F. Thabatah, dan K. Dahal. *Intelligent Quality Performance Assessment for E-Bangking Security using Fuzzy Logic*. 5th International Conference on Information Technology: New Generations, Washington: 2008.

[3] V. Novák, I. Perfilieva, dan J. Močkoř, *Mathematical principles of fuzzy logic*. Dodrecht: Kluwer Academic, 1999.

[4] R. Munir. *Sistem Inferensi Fuzzy*. Bahan Kuliah IF4058 Topik Khusus Informatika I. Bandung, 2012.

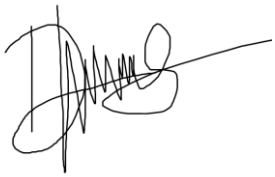
[5] Timothy J. Ross. *Fuzzy Logic with Engineering Applications, 3rd edition*. John Wiley & Sons: Singapore, 2010.

[6] http://www.acunetix.com/vulnerability-scanner/ - diakses pada 12 Mei 2012 pukul 19.03.

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, 11 Mei 2012
ttd



Reinhard Denis Najogie