Seminar Nasional Sistem Informasi dan Teknologi Informasi 2018
SENSITEK 2018
STMIK Pontianak, 12 Juli 2018

Penentuan *Attribute Value* Untuk Menentukan Bobot *Fraud* Dalam Transaksi *Online*

Solichul Huda

Universitas Dian Nuswantoro
Jl. Imam Bonjol No. 207 Semarang
e-mail: solichul.huda@dsn.dinus.ac.id

Abstrak

Fraud atau penipuan sering terjadi dalam transaksi online. Beberapa penelitian sebelumnya telah mengusulkan metode deteksi fraud dalam transaksi online. Namun dalam penentuan beberapa attribute value ditentukan oleh pakar secara subyektif; paper ini mengusulkan metode untuk menentukan attribute value tersebut. Atribut fraud dalam transaksi online terdiri enam atribut yaitu throughput time, wrong pattern, skip, same location, relationship dan quantity. Tiga atribut ditentukan menggunakan metode yang diusulkan penelitian sebelumnya, sedangkan tiga atribut berikutnya ditentukan secara subyektif oleh pakar. Paper ini mengusulkan metode pembobotan attribute value, sehingga semua atribut fraud ditentukan secara komputasi. Dalam pembobotan attribute value, pertama, menganalisis pelanggaran transaksi data training terhadap Standard Operating Procedure (SOP). Selanjutnya pakar menentukan pelanggaran yang terjadi merupakan fraud atau tidak. Kemudian dihitung probabilitas masing-masing atribut tersebut terhadap fraud yang terjadi. Lalu, menentukan fungsi keanggotaan masing-masing atribut berdasarkan nilai probabilitas. Terakhir, menentukan attribute value dari atribut quantity, relationship dan same location pada data testing menggunakan fungsi keanggotaan masing-masing atribut. Dalam penentuan bobot fraud, ditentukan juga bobot penting atribut dan bobot perilaku berdasarkan atribut yang teridentifikasi. Berdasarkan nilai threshold fraud, pelanggaran SOP yang terjadi ditentukan sebagai fraud atau tidak.

Kata kunci: *Fraud, transaksi, online, attribute value, SOP, fuzzy,*

1. Pendahuluan

Smart city saat ini menjadi acuan dalammembangun pemerintah di Kabupaten atau kota se Indonesia. Pembangunan tersebut salah satunya dilakukan dengan mengimplementasikan teknologi informasi dalam memberikan layanan kepada masyarakat. Selain itu *smart city*diimplementasikan dalam berbagai bidang, salah satunya dalam bidang ekonomi dimana sebagian dilakukan dengan meningkatan transaksi *online*.

Transaksi *online* dapat dilakukan menggunakan perangkat seluler maupun komputer PC atau laptop. Sedangkan untuk berkomunikasi, media transmisi seperti jaringan internet lewat Wifi atau paket internet dapat digunakan dengan jaminan keamanan yang disediakan oleh penyedia jaringan. Dengan teknologi informasi ini, transaksi dapat dilakukan tanpa diharuskan terjadinya pertemuan penjuan dan pembeli.

Meningkatnya jumlah transaksi *online* biasanya diikuti meningkatnya jumlah kejadian penipuan yang dikenal dengan istilah *fraud*. *Fraud* adalah bentuk kecurangan dengan cara langsung atau tidak langsung untuk mengambil keuntungan. Jumlah fraud dalam transaksi *online* akan meningkat seiring dengan meningkatnya jumlah transaksi *online*. Kondisi ini mendorong peneliti untuk mengembangkan metode deteksi fraud pada transaksi *online* [1].

Dalam transaksi *online* tidak dibatasi oleh ruang dan waktu. Pembeli dan penjual tidak saling mengetahui karakter satu dengan yang lain. Kondisi ini yang dimanfaatkan oleh pelaku fraud untuk mengambil keuntungan. Oleh karena itu, metode deteksi fraud mestinya bisa mengetahu perilaku diantara keduanya [2].

Dalam transaksi *online* tidak perlu terjadinya pertemuan antara penjual dan pembeli, sehingga penipuan/*fraud* dapat dilakukan oleh pembeli atau penjual. Metode deteksi *fraud* semestinya dapat memberikan informasi tentang perilaku atara satu dengan yang lain. Metode deteksi *fraud* ini dapat memberikan informasi tentang penjual ke pembeli, begitu juga sebaliknya. Informasi tersebut yang dapat menjadi pertimbangan transaksi yang akan dilakukan merupakan *fraud* atau bukan.

Pengembangan metode deteksi *fraud* ini bisa dilakukan berbasis data transaksi dan data proses. Penelitian berbasis data transaksi menggunakan pendekatan *data mining*, sedangkan proses transaksi menggunakan pendekatan *process mining*. Penelitian metode deteksi fraud berbasis *process mining*, akan menganalisis proses bisnis yang sedang berlangsung. Dengan demikian deteksi *fraud* yang berbasis *process mining* dapat memutuskan proses penjualan tersebut *fraud* atau tidak bisa teridentifikasi sebelum proses pembayaran dilakukan. Pendekatan ini dapat mengidentifikasi penipuan/*fraud* lebih dini.

Penelitian tentang deteksi *fraud* pada transaksi online sudah pernah diusulkan oleh penelitian sebelumnya [3],[4],[5]. Namun penelitian tersebut berbasis *data mining*, sehingga *fraud* teridentifikasi setelah kerugian terjadi. Penelitin ini mengusulkan metode deteksi fraud/penipuan menggunakan pendekatan *process mining*. Proses bisnis dianalisis sampai menjelang pembanyaran, jika teridentifikasi bahwa proses bisnis tersebut *fraud*, maka proses pembayaran dibatalkan.

Penelitian awal deteksi *fraud* berbasis *process mining* telah diusulkan dalam [2]. Penelitian tersebut mengidentifikasi atribut *fraud* dan pola *fraud* dalam transaksi *online*. Akan tetapi *attribute value* di lakukan secara subyektif oleh pakar. Paper ini mengusulkan metode penentuan *attribute value*.

Bobot *fraud* ditentukan oleh 3 variable yaitu *attribute valu*e, bobot penting atribut dan bobot perilaku originator. Originator adalah penjual atau pembeli yang melakukan transaksi. *Attribute value* menunjukkan bobot pelanggaran SOP [6]. Bobot penting atribut merupakan tingkat pentingnya atribut dibanding atribut lain [7]. Dan bobot perilaku menunjukkan perilaku penjual atau pembeli.

Process mining merupakan salah satu pendekatan yang mengambil *knowledge* dari proses transaksi yang dilakukan. Proses yang dijalankan disimpan didalam event logs. Dalam sebuah *event logs* minimal tersimpan kode event, nama event, waktu dimulainya event, waktu selesainya *event* dan nama originator [8],[9]. Originator adalah nama user yang menjalankan proses. Dengan demikian dalam sebuat event logs minimal ada event_code, time stamp start, time stamp end dan originator.

Standard Operating Procedure dalam process mining tersebut dikembangkan dari model proses bisnis. Process mining menggunakan beberapa algoritma dapat membuat model proses bisnis. Ada beberapa algoritma untuk membuat model proses, diantarnya menggunakan algoritma alpha, alpha plus dan algoritma heuristik. Dengan menggunakan algoritma tersebut dapat dibentuk model proses berdasarkan algoritma.

SOP dibentuk berdasarkan model proses binis ditambah dengan beberapa atribut tambahan. Penambahan atribut tersebut tergantung dengan kebutuhan sesuai dengan jenis bisnisnya. Model proses bisnis dan atribut tambahan ini yang menjadi SOP dalam process mining.

Dalam penggalian knowledge dari event logs dapat dilakukan dengan berbagai tehnik. Metode tersebut conformance, discovery dan enhacement. Penelitian [9] merupakan conformance dengan membandingkan proses binis dengan SOP.

Dalam [7] menganalisis proses bisnis menggunakan beberapa metode analisis, yaitu analisis skip, analisis throughput time, analisis decision, analisis resource dan analisis parallel. Analisis skip digunakan untuk menganalisis adanya urutan event yang lompat dibanding dengan SOP. Analisis thorughput time digunakan untuk menganalisis waktu yang dibutuhkan menjalankan proses dibanding waktu standard. Bentuk pelanggaran terhadap SOP dikenal dengan istilah atribut. Dalam [2] mengusulkan enam atribut fraud pada transaksi online. Enam atribut fraud tersebut ditunjukkan dalam Tabel 1.

Tabel 1. Atribut fraud pada transaksi online

No.	Nama atribut	Keterangan
1	*Throughput*	Waktu menjalankan *event* yang lebih kecil dibanding dengan waktu standar *event* Misalkan*event* masukkan_pesanan memerlukan waktu 25 menit, padahal waktu standard masukkan_pesanan 15 menit, maka *event* ini terindikasi *throughput time* karena menjalankan lebih besar waktu standard event
2	*Quantity*	Jumlah pembelian yang terlalu besar. Contoh dari data *trining* bahwa rata-rata pembelian 6 item. Ada case yang melakukan pemesanan sejumlah 15 item, maka terindikasi *quantity*karena jumlah pemesanannya melebihi jumlah rata-rata
3	*Same location*	Tempat pembeli dengan lokasi penjual satu lokasi Contoh alamat pembeli jl. muwardi no. 13salatiga, sedangkan alamat penjual online juga berada di Jl. Muwardi no. 54 Salatiga. Disebabkan lokasi pembeli dan penjual dalam nama jalan dan kota yang sama maka case terindikasi *same*
4	*Wrong pattern*	Urutan proses bisnis berbeda dengan urutan SOP. Urutan proses dalam SOP seharusnya *event* A1, *event* B1 kemudian *event* C1. C*ase* ini terindikasi *wrong pattern* jika case tersebut urutannya *event* A1, *event* C1 selanjutnya *event* B1.
5	*Skip*	Misalnya urutan proses nya seharusnya *event* A, *event* B kemudian *event* C. Dalam

		proses bisnis sebuah case *event* A, *event* C kemudian *event* D, karena melompati event B, case ini melompati 1 *event* dibanding dengan SOP
6	*Relationship*	Seandainya ada pelanggan tetap dan kustomer sudah membeli tiga kali atau lebih, maka *relationship*

Sumber utama *process mining* adalah *event logs*. *Event logs* adalah kumpulan rekaman aktivitas dari sebuah sistem informasi. Sebuah *event logs* adalah satu set dari *case-caseL* $\subseteq \mathscr{C}$, dimana c_1 dan $c_2 \in L$. Dari *event logs* tersebut akan diperoleh informasi tentang *case ID*, nama *activity*, *resource*, *start time stamp* dan *complete time stamp*. Informasi tersebut merupakan informasi minimum yang harus tersedia di dalam event logs [9].

Case adalah satu rangkaian *event-event* dalam sebuah proses bisnis. Dalam aplikasi kredit ini, sebuah *case* dimulai dari proses pengajuan aplikasi kredit dan diakhiri dengan proses penerimaan atau penolakan kredit. *Event* merupakan aktifitas proses yang dijalankan, contohnya adalah *event* pengajuan kredit. *Resource* atau originator yaitu nama pelaksana yang menjalankan *event*. Sedangkan *time stamp start* dan *complete* menunjukkan waktu mulai dan berakhirnya sebuah *event* dijalankan.

Trace adalah set urutan eksekusi dari *event-event* $\sigma \in \mathscr{C}$ dimana setiap *event* hanya satu dalam *trace* untuk $1 \leq i \leq j \leq |\sigma| \;:\; \sigma(i) \neq \sigma(j)$. Dalam *event logs* pengaturan tentang penulisan *trace* dan *event* sudah dilakukan. Dalam format xes, setiap *trace* diawali dengan tag <trace> dan diakhiri dengan tag </trace>.

Informasi proses dalam *event logs* tersimpan di dalam *event*. Misal $\mathscr{C}$ adalah semua *event*, maka setiap event e $\in \mathscr{E}$. Setiap *event* minimal ada informasi tentang nama*event*, nama originator yang menjalankan, dan waktu menjalan *event* tersebut.

Setiap *event logs* diawali dengan tag <?xml>, yang menunjukkan tipe file xml yang dipakai. Kemudian awal dari *event logs* ditunjukkan dengan tag <log> dan diakhiri dengan </log>. Pada awal *event logs* didefinisikan *trace* dan *event*. Dalam *trace* biasanya didefinisikan kode *case*, yang berupa *concept* dan *value*. Kemudian dalam *event* minimal didefinisikan *concept*, lifecycle, timestamp, activity dan *resource*. Variabel *concept* digunakan untuk mendefinisikan nama*event*, *lifecycle* untuk menunjukkan *transition*, *timestamp* menunjukkan tanggal dan waktu eksekusi, *activity* untuk nama *event* dan originator menunjukkan nama pelaksana proses [9].

Process Mining dan Deteksi Fraud

Process-based Fraud (PBF) yaitu fraud yang diidentifikasi dari proses yang melanggar SOP . Dalam *process mining* dapat dilakukan dengan l*og inspection*, *control flow analysis*, *performance analysis* dan *role analysis*. Analisis tersebut digunakan untuk mengidentifikasi proses yang dicurigai sebagai PBF [8]. Namun penggunaan metode tersebut masih memerlukan analisis kembali secara manual untuk mengidentifikasi *suspicious* fraud.

Sebuah proses bisnis semestinya berjalan sesuai dengan petunjuk operasional standard yang dikenal dengan *Standard Operating Procedure* (SOP). Pelaksanaan proses bisnis yang sesuai SOP akan menghasilkan *output* dengan kualitas yang diharapkan. Sebaliknya, pelaksanaan proses yang melanggar SOP, akan merugikan perusahaan. Contoh PBF dalam transaksi online, berupa pembelian fiktif yang akan merugikan penjul atau pembeli.

Sistem bilangan fuzzy tepat untuk mengidentifikasi data yang kurang tegas [10]. Penggunaan sistem fuzzy untuk proses pengambilan keputusan sudah banyak dilakukan, diantaranya [11]. Dalam pengambilan keputusan, pendapat pakar yang berupa kualitatif dikonversi ke dalam sistem fuzzy. Keputusan untuk menentukan salah satu dari beberapa pilihan dilakukan menggunakan *Multi-Attribute Decision Making*. Dalam [11] pendapat pakar dikonversi ke fuzzy, dan proses inferensi dilakukan menggunakan MADM. Proses defuzzifikasi dilakukan menggunakan rumus yang merupakan pengembangan dari rumus defuzzifikasi.

Sebuah sistem fuzzy secara umum meliputi empat tahapan utama, yaitu fuzzifikasi, *rule base*, fuzzy inferensi dan fuzzifikasi. Terdapat beberapa model fuzzy, yaitu fuzzy sugeno, tsukamoto, dan mamdani. Namun sebagian penelitian fuzzy menggunakan fuzzy mamdani termasuk paper ini.

Pada penelitian ini, *attribut value*, bobot penting atribut dan model kepatuhan dikonversi ke dalam sistem fuzzy. Ada tiga bentuk keanggotaan fuzzy yaitu keanggotaan linier, segitiga dan trapesium. Namun bentuk trapezium merupakan bentuk fuzzy yang banyak dipakai untuk banyak dipakai untuk keanggotaan fuzzy [11].

$$\mu_A(X) = \max\left[\min\left[\frac{Y-A}{B-A}, 1, \frac{D-Y}{D-C}\right], 0\right] \quad (1)$$

dimana nila A, B, C dan D adalah empat titik dalam keanggotaan fuzzy trapezium.

Proposisi fuzzy dapat digambarkan dengan fungsi implikasi yang disebut dengan fuzzy *rule if-then*[10]. Sebuah *rule* kondisi fuzzy secara umum terbuat dari

sebuah *premise* dan *consequent*, sebagai contoh " if pelanggaran = *low* and kepatuhan =*good* (*premise*) then *attribute value =very low*", dimana *low* dan *good* dapat digambarkan dengan fungsi keanggotaan. Dalam model fuzzy, masing-masing *rule* ditunjukkan sebagai sebuah relasi, dimana dapat dihitung dengan rumus (2).

$$\mu_{ri}(X,Y) = I(\mu_{ai}(X), \mu_{bi}(Y)),\ ui=1,2,.....n \quad (2)$$

dimana $\mu_{ri}(X,Y)$ relasi dari bobot keanggotaan rule i merujuk pada input X dan Y; $\mu_{ai}(X)$ dan $\mu_{bi}(Y)$adalah bobot keanggotaan dari input X dan Y; i menunjukkan operator "and" atau "or", dan n adalah jumlah dari rule.

Proses *mapping* dari masukan menjadi keluaran dapat menggunakan mekanisme inferensi fuzzy. Dalam agregasi tersebut akan diterapkan dengan agregasi atau mekanisme logika dari *rule*. Agregasi tersebut menggunakan sistem *disjuctive* dan *conjuctive*. Dalam sistem *conjunctive*, *rule* dikoneksikan dengan koneksi "*and*", sedangkan dalam *disjunctionrule* dikoneksikan dengan "*or*" koneksi [10].

$$\mu_{Ck}(Z) = \max[\min[\mu_{Ak}(\text{input}(x)), \mu_{Bk}(\text{input}(y))]]\ k=1,2,...r \quad (3)$$

dimana μ_{Ck}, μ_{Ak} dan μ_{Ck}adalah fungsi keanggotaan dari keluaran "Z" untuk masing-masing rule "k", input "x" dan input "y".

Defuzzifikasi

Output dari sistem inferensi pada keanggotaan fuzzy adalah bilangan fuzzy.Jika bilangan krisp diperlukan untuk agregasi luaran, teknik defuzzifikasi digunakan untuk mengubah bentuk fuzzy ke krisp.Dalam metode ini, bilangan krisp dapat diperoleh dengan menggunakan rumus (4) [11].

$$S = \frac{-x_1x_2 + x_3x_4 + (\frac{1}{3})(x_4 - x_3)^2 + (\frac{1}{3})(x_2 - x_1)^2}{-x_1 - x_2 + x_3 + x_4} \quad (4)$$

dimana x_1, x_2, x_3, x_4 adalah nilai pertama, kedua, ketiga dan keempat dari fuzzy trapezium.

Modified digital logic (MDL) merupakan salah satu metode yang digunakan untuk memberikan bobot sebuah atribut dengan membandingkan antara atribut satu dengan atribut lainnya. Dalam penelitian ini, metode MDL digunakan untuk memberikan tingkat penting sebuah atribut dibanding atribut lainnya. Beberapa pakar berdiskusi tentang bobot pentingnya sebuah atribut, hasilnya disajikan dalam metode MDL. Dalam [11] metode MDL juga digunakan oleh pakar untuk memberikan bobot penting sebuah atribut dibanding atribut lainnya. Bobot penting atribut dihitung dengan rumus (5)

$$W = \frac{P_j}{\sum_{j=1}^{n} P_j} \quad (5)$$

Dimana *p* adalah *positive decision* dan *j* nilai dari atribut-atribut.

2. Pembahasan

Dalam uji coba ini peneliti mengumpulkan data *event logs* dari tiga Usaha Kecil Menengah (UKM) di Jawa Tengah dalam periode 2014-2016. Untuk pengujian dan pengukuran akurasi, data tersebut dikelompokkan dalam data *training* dan data *testing*, dengan jumlah masing-masing 2.415 *case* (7.200 *event/record*) dan 1.610 *case* (4.800 *event/record*).

Proses analisis *event logs* pada *data training* dilakukan untuk memperoleh case yang melangar SOP. Kemudian penelitian ini menkonversi jumlah pelanggaran yang terjadi dalam bentuk fuzzy dengan tiga kreteria yaitu low, middle dan high. Atribut yang di fuzzifikasi adalah atribut *throughput*, *skip* dan *wrong pattern*. Sedangkan atribut quantity, same location dan relationship berisi nlai true atau false.

Dalam penelitian sebelumnya terdapat 6 atribut Fraud yaitu *throughput time*, *quantity*, *same location*, *wrong pattern*, *skip* dan *relationship*. Untuk penentuan *attribute value* dari *throughput*, *wrong pattern* dan *skip* menggunakan metode dalam [9]. Sedangkan untuk tiga lainnya yaitu *quantity*, *same location* dan *relationship* dalam pembobotan *attribute value* menggunakan metode yang diusulkan dalam paper ini.

Dari data training, diperoleh probabilitas masing-masing atribut terhadap bobot fraud. Nilai tersebut menjadi dasar penentuan keanggotaan fuzzy masing-masing atribut. Metode ini yang digunakan untuk mengkoversi atribut *quantity*, *same location* dan *relationship* menjadi *attribute value* dengan *low*, *middle* dan *high*.

Analisis yang dilakukan terhadap data *test* menunjukkan hasil bahwa 243 *case* melanggar SOP. Sebagai contoh dalam *case* 1021 teridentifikasi tiga pelanggaran/atribut yaitu *throughput time*, *wrong pattern* dan *quantity*, masing-masing 1,1, dan 't'. Kemudian case ID 8700 memiliki 2 atribut, yaitu *throughput time* dan *wrong pattern*, masing-masing 2 dan 1. Metode yang digunakan untuk menganalisis proses bisnis seperti metode yang dalam [8]. Setelah proses fuzzifikasi menggunakan metode yang diusulkan dalam paper ini, maka *case* 1021 attribute value atribute quantity menjadi *low.*

Metode deteksi *fraud* dilakukan untuk memperoleh metode deteksi *fraud* dalam transaksi *online* dengan metode penentuan *attribute value*. Evaluasi ini dilakukan dengan menganalisis dan membobot *attribute value* case

dalam data *testing*. Kemudian melakukan dan uji *similarity* dengan pola *fraud*. Disisi lain, pakar menganalisis data *testing* menggunakan metode mereka. Evaluasi metode yang diusulkan dilakukan dengan mengukur akurasi, sensitivitas dan spesifisitas. Dalam penelitian ini uji sensitivitas dan spesifisitas dilakukan karena jumlah *fraud* dan bukan *fraud* tidak seimbang. Untuk untuk menghitung akurasi, sensitivitas dan spesifisitas masing-masing menggunakan Rumus (6), Rumus(7) dan Rumus (8).

Metode *receiver operating characteristic* (ROC) digunakan untuk mengukur akurasi metode deteksi *fraud*dalam transaksi *online*. *Framework* ini mengukur akurasi dengan mempertimbangkan *true positive* (TP), *true negative* (TN), *false positive* (FP), dan *false negative* (FN). TP berarti pakar dan metode ini sama menentukan bahwa *case* tersebut *fraud* atau penipuan. TN juga mengangap bahwa pakar dan metode menentukan bahwa *case* tersebut bukan *fraud*. Jika pakar menentukan *fraud*sedangkan metode bukan fraud, berarti FN. Jika pakar memutuskan bukan *fraud* sedangkan metode menentukan *fraud*, berarti FP.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}. \quad (6)$$

$$Sensitivitas = \frac{TP}{TP+FN} \quad (7)$$

$$Spesifisitas = \frac{TN}{TN+FP} \quad (8)$$

Evaluasi yang peneliti lakukan menghasilkan 243 *case* yang melanggar SOP. Metode ini mengidentifikasi 243 *case* tersebut merupakan *fraud*. Pakar juga menganalisis proses bisnis pada data *testing* menggunakan metode mereka. Pakar mengidentifikasi hanya 201 *case* yang dianggap *fraud* atau penipuan. Dengan demikian ada perbedaan antara hasil analisis metode yang diusulkan dengan hasil analisis oleh pakar. Hasil diskusi dengan pakar tersebut menunjukkan bahwa menggunakan metode yang diusulkan 201 *case* diidentifikasi sebagai *true positive*, artinya bahwa pakar dan metode ini sama mengidentifikasi bahwa 201 case tersebut *fraud*. Kemudian, 42 *case* sebagai *false positive*, berarti ada 42 *case* yang menurut metode ini terindikasi fraud, sedangkan menurut pakar bukan fraud. Dan 1.367 case sebagai *true negative*, dimana pakar dan metode ini sama menentukan 1.367 case bukan *fraud*. Menggunakan Rumus (6), Rumus (7) dan Rumus (8), metode ini memperoleh akurasi 0,97, sensitivitas 1dan spesifisitas 0,97. Hasil ini sama akurasinya dengan pembobotan attribute value yang dilakukan oleh pakar. Hasil evaluasi metode yang diusulkan ditunjukkan dalam Tabel 2.

Tabel 2. Hasil Evaluasi Metode

Variabel ROC				Akurasi	Sensitivitas	Spesifisitas
True Positive	*False Positive*	*False negative*	*True negative*			
201	42	0	1.367	0,97	1	0,97

3. Kesimpulan

Metode penentuan *attribute value* pada atribut *quantity*, *same location* dan *relationship* dapat dilakukan menggunakan metode fuzzy yang diusulkan dalam paper ini. Fungsi keanggotaan fuzzy masing-masing atribut ditentukan dalam tiga kretaria yaitu *low*, *middle* dan *high*. Dalam paper ini, bobot *attribute value* semua atribut fraud dalam transaksi *online* yaitu *throughputtime*, *skip*, *wrong pattern*, *quantity*, *same location* dan *relationship* dapat dilakukan secara komputasi. Hasil evaluasi menunjukkan bahwa metode yang diusulkan ini memiliki akurasi yang sama dengan penentuan *attribute value* yang dilakukan oleh pakar. Metode penentuan *attribute value* yang diusulkan ini dapat mengurangi peran pakar dalam menentukan *fraud*.

Daftar Pustaka

[1]. I.Amara, A. B. Amar dan A. Jarboui. Detection of Fraud in Financial Statements: French Companies as a Case Study. "International Journal of Academic Research in Accounting, Finance and Management Sciences". 2013: 3(3), 44-55.
[2]. S.Huda, H.A. Santoso,"Identifikasi Pola Fraud dalam ransaksi Online", Konferensi Nasional Sistem Informasi 2018, Pangkal Pinang, 2018, 19.
[3]. C. Khyati dan M. Bhawna, Credit Card Fraud: Bang in E-Commerce. "International Journal Of Computational Engineering Research " . 2012: 3(2), 935-941.
[4]. C.Evandro , B. Gabriel dan P. Adriano C. M. "Fraud Analysis and Prevention in e-Commerce Transactions". IEEE. 2014;42-49.
[5]. M. Jans, M. J. van der Werf, N. Lybaert dan K. Vanhoof. "A Business Process Mining Application for Internal Transaction Fraud Mitigation". Expert Systems with Applications. 2011. 38(10). 13351-13359.
[6]. S. Huda, R. Sarno dan T. Ahmad. "Fuzzy MADM approach for Rating of Process-based Fraud". Journal ICT. Research Application. 2015: 9(2). 111-128.
[7]. R. Sarno, D. R. Dewandono, T. Ahmad, M. F. Naufal dan F. Sinaga. "Hybrid Association Rule Learning and Process Mining for Fraud Detection". IAENG International Journal of Computer Science. 2015:42(2).59-72.
[8]. S. Huda, R. Sarno dan T. Ahmad. "Increasing accuracy of Process-based Fraud Using Behavior Models", International Journal of Software Engineering and Its Applications.2016. 10(5). 175-188.
[9]. W. M. P. van der Aalst. "Discovery, Conformance dan Enhancement of Business Processes". Springer. 2010: 7-8.
[10]. Zadeh, L.A., (1965), "Fuzzy Sets", *Information and Control*, vol. 8, No. 3,hal. 338-353.
[11]. Vats, S., Vats, G., Vaish, R. dan Kumar, V., (2014), "Selection of Optimal Toll Collection System for India : A Subjective-Fuzzy Decision Making Approach",Applied Soft Computing, vol.21, hal. 444-452.