konferen1

by Solichul Huda

Submission date: 19-Dec-2018 01:39PM (UTC+0700)
Submission ID: 1059122336
File name: KNSI_2018_paper_64.pdf (309.88K)
Word count: 2394
Character count: 14881

Identifikasi Pola *Fraud* dalam Transaksi *Online*

Solichul Huda[1)], Heru Agus Santoso[2)]
Universitas Dian Nuswantoro
Jl. Imam Bonjol 155 Semarang
e-mail: solichul.huda@dinus.ac.id

Abstrak

Kuantitas fraud (penipuan) pada transaksi online meningkat dari waktu ke waktu. Beberapa penelitian sebelumnya telah mengusulkan metode deteksi fraud; namun metode tersebut tidak dapat mendeteksi fraud dalam transaksi online dengan baik. Hal itu disebabkan oleh indikator fraud tidak dapat menangkap dengan tepat pelanggaran Standard Operating Sistem (SOP) pada transaksi online. Penelitian ini mengusulkan atribut/indikator fraud dan pola fraud untuk menganalisis proses bisnis pada transaksi online. Penentuan fraud atau penipuan dilakukan dengan, pertama menganalisis bisnis proses transaksi online. Selanjutnya, transaksi online yang terindikasi fraud diidentifikasi sebagai suspicious fraud. Terakhir, melakukan uji similarity untuk menentukan pelanggaran SOP tersebut merupakan fraud atau bukan. Dari eksperimen yang dilakukan menunjukkan bahwa metode yang diusulkan ini mampu mendeteksi fraud pada transaksi online dengan akurasi dan FDR masing-masing 0.97dan 0.17.

Kata kunci: *identifikasi, fraud, penipuan, transaksi, online, pola.*

1. Pendahuluan

Dewasa ini pemerintah daerah atau pemerintah kota berlomba meningkatkan pelayanan mereka kepada masyarakat dengan memujudkan *smart city*. Layanan tersebut meliputi bidang kesehatan, bidang pembangunan fisik infrastruktur jaringan komunikasi, termasuk bidang ekonomi. Dalam bidang ekonomi misalnya, pemerintah mendorong pemanfaatan teknologi informasi oleh Usaha Kecil Menengah (UKM) sehingga mendukung terwujudnya *smart city*. Pemanfaatan teknologi informasi dapat diwujudkan dalam bentuk sistem informasi transaksi *online*.

Transaksi *online* merupakan implementasi teknologi informasi untuk transaksi jual beli. Teknologi tersebut meliputi teknologi perangkat keras komputer, telepon seluler, dan teknologi perangkat lunak. Perkembangan teknologi informasi ini membuat transaksi jual beli tidak dibatasi oleh ruang dan waktu. Penjualan *online* ini sejalan dengan program pemerintah dalam menggerakkan masyarakat untuk melakukan transaksi lewat transaksi *online*. Namun disisi lain, pelaku penipuan (*fraud*) memandang transaksi *online* merupakan area baru memperoleh keuntungan [1].

Dalam dua tahun terakhir ini penipuan *online* (*cyber crime*) dalam bentuk penipuan transaksi *online* jumlahnya semakin meningkat. Modus penipuan/fraud tersebut berubah-ubah dan selalu berkembang metode atau teknik yang digunakan. Oleh karena itu pemerintah dan peneliti perlu kerja keras untuk mengembangkan metode deteksi fraud / penipuan agar transaksi *online* aman.

Penelitian-penelitian sebelumnya sudah pernah mengusulkan metode deteksi fraud/penipuan. Namun, metode tersebut hanya dapat mendeteksi fraud setelah fraud terjadi [2],[3],[4],[5],[6]. Selain itu, sejauh yang peneliti ketahui, belum ada penelitian yang fokus mengembangkan metode mendeteksi fraud/penipuan pada transaksi *online*. Penelitian ini akan mengembangkan metode deteksi fraud pada transaksi *online* berbasis proses transaksi yang sedang dilakukan. Analisis proses bisnis tersebut diharapkan dapat menunjukkan indikasi terjadinya fraud/penipuan, sehingga fraud terdeteksi lebih dini sebelum kerugian terjadi.

Dalam penjualan *online*, penjual dan pembeli dapat mengaktualisasikan bentuk bisninya dengan berbagai media mulai dari desain tampilan sampai umpan balik pembeli, yang umumnya berupa testimoni. Selain itu mereka dapat memilih barang yang akan diperjualbelikan dengan mudah, cepat tanpa dibatasi tempat dan waktu. Model ini yang membuat masyarakat tertarik melakukan transaksi *online*.

Fraud/penipuan yang terjadi dalam transaksi *online* dapat dilakukan oleh penjual atau pembeli. Penipuan terhadap penjual, umumnya berupa tidak diterimanya uang dari pembeli sesuai dengan aturan yang mereka disepakati. Sedangkan penipuan terhadap pembeli, umumnya berujud ketidaksesuaian antara barang pesanan dengan barang yang dikirim, atau barang sama sekali tidak diterima.

Penipuan *online* mudah dilakukan karena ada celah keamanan yang berupa tidak adanya pertemuan antara penjual dengan pembeli. Saat transaksi, penjual maupun pembeli kesulitan untuk melakukan validasi dan verifikasi pisik tentang identitas penjual atau pembeli, seperti alamat usaha atau kondisi barang yang perjualbelikan. Selain itu, pembeli atau penjual tidak mengetahui perilaku diantara mereka.

Teknologi informasi dalam transaksi *online*, sebetulnya dapat menunjukkan lokasi pelaku transaksi. Kemudian, pola penjual dan pembeli dalam transaksi juga dapat dipelajari dari *event logs* atau data transaksi yang ada. *Event logs* berfungsi untuk menyimpan proses transaksi yang dilakukan [7]. Dalam *event logs* ini minimal tersimpan informasi mengenahi nama *event*, lama melalukan *event*, dan *user* (originator) yang menjalankan *event* [9]. Contoh *event* dalam transaksi *online* adalah pesan_barang. Selama ini, *event logs* hanya dipakai untuk menganalisis proses setelah terjadi fraud. Penelitian ini akan mengunakan *event logs* untuk menganalisis proses transaksi yang sedang berlangsung sehingga indikasi *fraud*/penipuan teridentifikasi lebih dini. Penelitian ini akan mengidentifikasi fraud/penipuan berdasarkan proses transaksi yang terjadi. Untuk menganalisis data transaksi menggunakan teknik *data mining*, sedangkan untuk menganalisis proses transaksi menggunakan teknik *process mining* [10]. Studi ini akan menggunakan pendekatan *process mining* dan *data mining* untuk mengembangkan metode deteksi fraud/penipuan berdasarkan data transaksi dan *event logs*.

Fraud dalam aplikasi kredit kemungkinan sedikit berbeda dengan *fraud* dalam transaksi *online*, sehingga kemungkinan indikator atau atributnya juga berbeda. Oleh karena itu, penelitian ini akan mengidentifikasi indikasi / atribut *fraud* pada transaksi *online*. Begitupun pola penipuannya kemungkinan berbeda dengan *fraud* pada aplikasi kredit; penelitian ini akan mengidentifikasi pola *fraud* dalam transaksi *online*. Hipotesis penelitian ini, metode yang diusulkan mampu mendeteksi penipuan pada transaksi *online* dengan akurat.

2. Metode Penelitian

2.1 Data Penelitian

Dalam melakukan penelitian ini, data sumber utama berupa data primer dan data sekunder. Data primer berupa *event logs* transaksi *online* yang diambil dari tiga Usaha Kecil Menengah (UKM) yang melakukan transaksi *online* dalam tiga tahun terakhir ini. Sedangkan data sekunder berupa data tambahan yang diperoleh dari buku panduan atau *standard operating system* (SOP).

Event logs transaksi ini berjumlah 4.025 case atau *process instance* dengan 12.000 *event*/*record*. Data tersebut dibagi menjadi data *trining* dan data *testing* masing-masing 2.415 *case* dengan 7.200 *record* dan 1.610 case dengan 4.800 *record*.

2.2. Penentuan Indikator

Indikasi penipuan yang terjadi diidentifikasi menggunakan metode analisis proses dan analisis data. Penelitian ini menggabungkan pendekatan *process mining* dengan *data mining*. Pertama, analisis menggunakan aplikasi ProM. Dan selanjutnya, menganalisis data untuk memperoleh pembedaan dengan data lainnya.

2.2.1. Klasifikasi pelanggaran

Penelitian ini akan menganalisis proses bisnis semua *case* dalam data *training*. Selanjutnya, hasil analisis tersebut dicluster sesuai dengan urutan proses bisnis dan data masing-masing *case*. Analisis ini menghasilkan delapan *cluster*, dimana satu *cluster* berisi *case* yang tidak melanggar SOP, sedangkan tujuh *cluster* lainnya melanggar SOP. Kami menganalisis tujuh *cluster* tersebut dan menunjukkan ada tujuh jenis pelanggaran SOP, yaitu *throughput time, quantity, same location, wrong pattern, skip, map* dan *relationship*. Indikator *throughput time, wrong pattern,*dan *skip* sudah pernah diidentifikasi dalam [4],[5],[6]. Selanjutnya, tujuh jenis pelanggaran SOP tersebut dikenal dengan istilah atribut atau indikator.

2.2.2. Penentuan indikator *fraud*.

Penelitian ini mengidentifikasi tujuh pelanggaran SOP. Penelitian ini menguji bobot korelasi antara tujuh atribut/indikator *fraud* tersebut dengan bobot *fraud*. Dari uji korelasi menunjukkan bahwa enam indikator/atribut memiliki korelasi yang signifikan dengan *fraud*/penipuan. Dengan demikian, enam atribut tersebut ditentukan sebagai atribut/indikator *fraud*. Enam indikator atau atribut tersebut adalah *throughput time, quantity, same location, wrong pattern, skip* dan *relationship*. Indikator/atribut *fraud* tersebut ditunjukkan dalam Tabel 1.

2.3 Penentuan Pola *Fraud*

Pola *fraud* digunakan untuk merekam berbagai pola dari *fraud*/penipuan yang sudah terjadi. Pola ini menggambarkan urutan dan kelengkapan data dari *case* tersebut. Pola ini digunakan sebagai rujukan penentuan sebuah *case* yang melanggar SOP merupakan penipuan/*fraud* atau bukan. Pola penipuan tersebut disusun berdasarkan data *training*.

2.3.1. Identifikasi Penipuan

Indikator penipuan yang telah teridentifikasi digunakan sebagai dasar identifikasi penipuan dari sebuah *case* transaksi dari data *training*. Langkah ini akan menghasilkan *case* yang terindikasi penipuan. Selanjutnya verifikasi penipuan tersebut dilakukan dengan membandingkan *case* data *training* dengan *case* penipuan. Hasilnya berupa *case* yang terindikasi *fraud* atau bukan.

Tabel 1. Indikator/atribut *Fraud* Dalam Transaksi *Online*

No.	Nama indikator	Keterangan	Penjelasan
1	*Throughput time*	Waktu menjalankan *event* yang lebih kecil dibanding dengan waktu standar menjalankan *event*	*Event* masukkan_pesanan memerlukan waktu 30 menit, padahal waktu standard masukkan_pesanan 15 menit, maka *event* ini terindikasi *throughput time*
2	*Quantity*	Jumlah pembelian yang terlalu besar	Misalnya dari data *trining* bahwa rata-rata pembelian 5 item. Ada pemesanan sejumlah 15 item, maka terindikasi *quantity*
3	*Same location*	Tempat pembeli dengan lokasi penjual satu lokasi	Lokasi pembeli dan penjual dalam nama jalan dan kota yang sama terindikasi *same location*
4	*Wrong pattern*	Urutan proses bisnis berbeda dengan pola SOP	Urutan proses nya seharusnya *event* A, *event* B kemudian *event* C. Dalam sebuah proses bisnis urutannya *event* A, *event* C selanjutnya *event* B, maka *case* ini terindikasi *wrong pattern*
5	Skip	Melompati *event* dibanding dengan SOP	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 terindikasi *Skip*
6	*Relationship*	Pelanggan tetap	Jika kustomer sudah membeli tiga kali atau lebih, maka *relationship* .t.

2.3.2. Penentuan Pola *Fraud*

Penelitian ini akan menganalisis pola dari case penipuan. Pola tersebut menggambarkan urutan, dan data yang ada dalam case. Pola dari semua case penipuan tersebut, menjadi rujukan dalam menganalisis case pada proses yang sedang berjalan. Contoh pola penipuan atau *fraud* ditunjukkan dalam Tabel 2.

Tabel 2. Contoh Pola *Fraud* Pada Transaksi *Online*

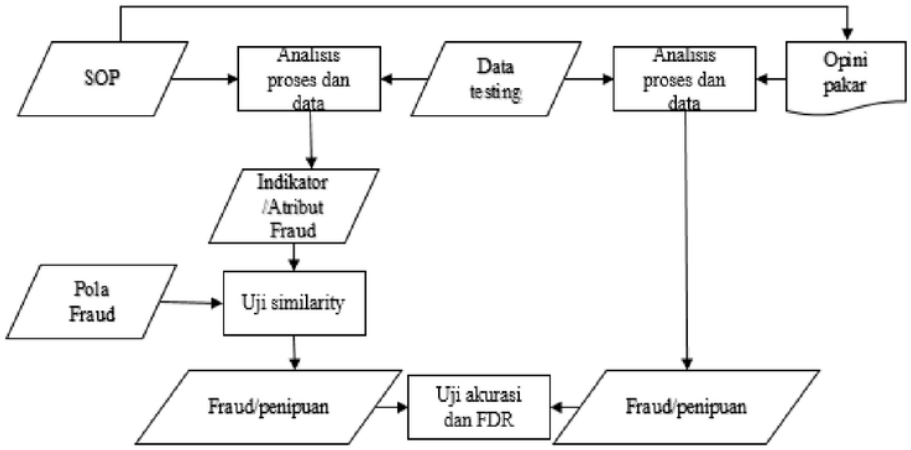
Pola Fraud	Throughput Time	Wrong pattern	Skip	Same location	Quantity	Relationship
1	Low	Low	Low	f	f	f
2	Middle	Low	Low	f	f	f
3	High	Low	Low	f	f	f
4	Low	Middle	Low	t	t	t
5	Middle	Middle	Low	t	t	t
6	High	Middle	Low	t	t	t
7	Low	High	Low	f	t	t
8	Middle	High	Low	f	t	t
9	High	High	Low	f	f	f

2.4. Penentuan *Fraud*

Indikasi penipuan yang teridentifikasi dalam sebuah *case* menjadi kunci untuk menentukan *fraud*. Berdasarkan indikasi yang teridentifikasi, penelitian ini akan melakukan cek *similarity* dibanding dengan pola yang ada dalam database pola penipuan. *Case* yang memperoleh nilai diatas nilai *threshold* ditentukan sebagai *fraud*.

3. Hasil dan Pembahasan

Uji akurasi dilakukan untuk mengukur kemampuan metode yang diusulkan dalam mendeteksi *fraud* dalam transaksi *online*. Proses evaluasi ditunjukkan dalam Gambar 1.



Gambar 1. Proses Evaluasi

Dalam eksperimen ini, peneliti mengumpulkan data *event logs* dari tiga Usaha Kecil Menengah (UKM) dalam periode 2014-2016. Data tersebut dikelompokkan dalam data *training* dan data *testing*, masing-masing 2.415 *case* (7.200 *event/record*) dan 1.610 *case* (4.800 *event/record*). Kami menganalisis data dan proses dalam data *training* untuk memperoleh *case* yang melanggar SOP. Pelanggaran tersebut diidentifikasi sebagai atribut/indikator *fraud*.

Analisis terhadap data *test* menghasilkan 243 *case* melanggar SOP. *Case* 1021 memiliki tiga atribut yaitu *throughput time, wrong pattern* dan *quantity*, masing-masing 1,1, dan 't'. Sedangkan dalam case ID 8772 memiliki 2 atribut, yaitu *throughput time* dan *wrong pattern*, masing-masing 1. Contoh *case* yang teridentifikasi *fraud* ditunjukkan dalam Tabel 3.

Metode deteksi *fraud* yang diusulkan penelitian ini, diimplementasikan untuk mengidentifikasi *fraud* yang lebih akurat dibanding metode sebelumnya [5],[6]. Evaluasi ini dilakukan dengan menganlisis data *testing* menggunakan atribut/indikator *fraud* dan pola *fraud*. Disisi lain, pakar menganalisis data *testing* menggunakan metode mereka. Evaluasi akurasi dan *false discovery rating* (FDR) terhadap metode ini dilakukan untuk melihat kelebihan metode yang diusulkan ini. Rumus (1) digunakan untuk menghitung akurasi, sedangan Rumus (2) digunakan untuk menghitung FDR.

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.

Tabel 3. Contoh *Case* Yang Terindikasi *Fraud*

ID Case	Throughput Time	Wrong pattern	Skip	Same location	Quantity	Relationship
1021	1	1	-	f	t	t
3324	1	1	-	f	f	t
3581	1	-	1	f	f	t
6567	2	-	-	f	f	t
8521	2	-	-	f	f	t
8533	2	-	-	f	t	f
8645	1	-	-	f	f	t
8700	2	1	-	t	f	t
8772	1	1	-	f	f	f
8905	1	-	1	f	f	f

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$FDR = \frac{FP}{TP+FP} \quad (2)$$

Evaluasi terhadap data *testing* menghasilkan 243 *case* yang melanggar SOP. Metode ini menentukan 243 *case* yang merupakan *fraud*. Namun dari pakar menentukan hanya 201 *case* yang dianggap *fraud* atau penipuan. Hasil diskusi pakar tersebut membuktikan bahwa menggunakan metode yang diusulkan 201 *case* diidentifikasi sebagai *true positive*, 42 case sebagai *false positive*, dan 1.367 case sebagai *true negative*. Menggunakan Rumus (1) dan Rumus (2), metode ini memperoleh akurasi 0,97 dan FDR 0,17. Hasil evaluasi metode yang diusulkan ditunjukkan dalam Tabel 4.

Tabel 4. Hasil Evaluasi Metode

Variabel ROC				Akurasi	FDR
True Positive	*False Positive*	*False negative*	*True negative*		
201	42	0	1.367	0,97	0,17

4. Simpulan

Fraud dalam transaksi *online* dapat diidentifikasi dengan akurat dengan mengembangkan atribut/indikator *fraud* dan pola *fraud*. Ada enam atribut/indikator *fraud* dalam transaksi *online* yang teridentifikasi dalam penelitian ini yaitu *same location, relationship,quantity, througput time, skip* dan *wrong pattern*. Tiga atribut fraud yaitu *througput time, skip* dan *wrong pattern* sudah diusulkan oleh penelitian sebelumnya [5],[6], sedangkan tiga atribut berikutnya *same location, relationship*, dan *quantity* diusulkan penelitian ini. Tiga atribut *same location, relationshi,* dan *quantity,*dapat meningkatkan akurasi metode deteksi *fraud* atau penipuan ini pada transaksi *online*. Untuk memperoleh akurasi deteksi *fraud*, polayang ada *fraud* diperbaiki sesuai dengan pola baru *fraud*. Metode deteksi *fraud* yang diusulkan ini mampu mendeteksi *fraud* pada transaksi *online* dengan akurat.

Daftar Pustaka

[1] I. Amara, A. B. Amar and 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] M. Jans, M. J. van der Werf, N. Lybaert and K. Vanhoof. A Business Process Mining Application for Internal Transaction Fraud Mitigation. *Expert Systems with Applications.* 2011. 38(10). 13351-13359.

[3] J. Stoop. Process Mining and Fraud Detection. Thesis. Netherlands:Twente University; 2012.

[4] R. Sarno, D. R. Dewandono, T. Ahmad, M. F. Naufal and F. Sinaga. Hybrid Association Rule Learning and Process Mining for Fraud Detection. *IAENG International Journal of Computer Science*. 2015:42(2).59-72.

[5] S. Huda, R. Sarno and T. Ahmad. Fuzzy MADM approach for Rating of Process-based Fraud. *Journal ICT Research Application*. 2015: 9(2). 111-128.
[6] S. Huda, R. Sarno and T. Ahmad. Increasing accuracy of Process-based Fraud Using Behavior Models, International Journal of Software Engineering and Its Applications.2016. 10(5). 175-188.
[7] W. M. P. van der Aalst. Discovery, Conformance and Enhancement of Business Processes. Springer. 10: 7-8.
[8] R. Sarno, P. L. I. Sari. H. Ginardi, D. Sunaryono , I. Mukhlash. Decision Mining For Multi Choice Workflow Patterns, *International conference on Computer Control, and Its Application*. 2013.19-21.
[9] R. Sarno, A.B. Sanjoyo, I. Mukhlash and M.H. Astuti. Petri Net Model of ERP Business Process Variations for Small and Medium Enterprises. *Journal of Theoretical and Applied Information Technology*. 2013. 54(1). 31-38.
[10] W. M. P. van der Aalst, H.A. Reijers and M. Song. Discovering Social Networks from Event Logs. Computer Supported Cooperative Work. 2005. 14. 549-593.

konferen1

ORIGINALITY REPORT

11%	%	%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Muhammadiyah Ponorogo Student Paper	2%
2	Submitted to Universitas Pendidikan Indonesia Student Paper	2%
3	Submitted to Universiteit van Amsterdam Student Paper	1%
4	Submitted to UIN Syarif Hidayatullah Jakarta Student Paper	1%
5	Submitted to Birla Institute of Technology and Science Pilani Student Paper	1%
6	Submitted to Laureate Higher Education Group Student Paper	1%
7	Submitted to University of Dayton Student Paper	1%
8	Submitted to Lambung Mangkurat University Student Paper	1%

9	Submitted to University of Birmingham Student Paper	1%
10	Submitted to Universitas Brawijaya Student Paper	1%
11	Submitted to Universitas Dian Nuswantoro Student Paper	<1%
12	Submitted to Associatie K.U.Leuven Student Paper	<1%

Exclude quotes	On	Exclude matches	< 1 words
Exclude bibliography	On		