ISSN : 2337-3067
E-Jurnal Ekonomi dan Bisnis Universitas Udayana 9.9 (2020):851-878

PEMETAAN BENTUK DAN PENCEGAHAN PENIPUAN *E-COMMERCE*

Ni Komang Arista Dewi[1]
Luh Putu Mahyuni[2]

Universitas Pendidikan Nasional, Bali, Indonesia[1,2]
Email: aristadewi0902@gmail.com[1] mahyuniluhputu@undiknas.ac.id[2]

ABSTRACT

The rapid growth of buying and selling transactions, makes electronic fraud also increased so that many consumers have suffered losses due to fraud occurred. The purpose of this research is to find out the types of fraud that can occur in e-commerce and the prevention that can be done. The author presents a review with an interpretive approach to the related articles, through mapping on articles collected from Google Scholar, Elsevier, Springer, Taylor & Francis, and MDPI (Multidisciplinary Digital Publishing Institute). From these sources, the author collected 105 articles, after articles selection process based on the last 10 years and the suitability of the discussion finally the author collected 55 articles. The results of this research is the authors found various types of fraud in four categories of e-commerce, fraud in the payment system, and fraud in e-commerce involving customers. Modern methods of fraud detection are also presented in this research, such as data mining, Bayesan networks, algorithms, vector support machine, genetic programming, tress decision making, Adaptive Neuro-Fuzzy Inference Systems, Protection Assistance Websites (PAW), and Models Privacy Antecedent-Privacy Concern-Outcomes (APCO). With the explanation on the results, consumers are expected to be more careful when making transactions on e-commerce to avoid fraud.

Keywords*: E-Commerce; Electronic Fraud; Fraud Detection.*

ABSTRAK

Seiring berkembangnya transaksi jual beli, penipuan elektronik juga turut meningkat sehingga mengakibatkan banyak konsumen yang telah mengalami kerugian akibat penipuan yang terjadi. Tujuan dari penelitian ini adalah untuk mengetahui jenis penipuan yang dapat terjadi dalam perdagangan elektronik dan pencegahan yang dapat dilakukan. Dalam penelitian ini disajikan review dengan metode pendekatan interpretif atas artikel terkait, dengan proses pemetaan pada artikel yang dikumpulkan melalui situs Google Cendekia, Elsevier, Springer, Taylor & Francis, dan MDPI (Multidisciplinary Digital Publishing Institute). Dari sumber tersebut, 105 artikel berhasil dikumpulkan, setelah proses seleksi artikel berdasarkan 10 tahun terahir dan kesesuaian pembahasan akhirnya diperoleh 55 artikel. Hasil penelitian ini adalah ditemukan berbagai jenis penipuan pada keempat kategori e-coomerce serta penipuan pada sistem pebayaran dan penipuan pada e-commerce yang menyangkut pelanggan. Metode modern pendeteksi penipuan juga disajikan dalam penelitian ini, seperti data mining, jaringan bayesan, algoritma, mesin pendukung vector, pemrograman genetik, pohon pengambilan keputusan, Adaptive Neuro-Fuzzy Inference System, Situs Web Bantuan Perlindungan (PAW), dan Model Privacy Antecedent-Privacy Concern-Outcomes (APCO). Dengan penjabaran pada hasil penelitian ini, konsumen diharapkan untuk lebih berhati-hati saat melakukan transaksi di situs e-commerce agar terhindar dari berbagai tindak penipuan.

Kata kunci: Perdagangan Elektronik; Penipuan Elektronik; Pendeteksi Pada Penipuan.

PENDAHULUAN

Pesatnya perkembangan internet dari tahun ke tahun telah mendorong kemajuan pertukaran informasi di dunia ini. Hal ini juga sangat mempengaruhi peningkatan penggunaan internet untuk transaksi bisnis komersial yang biasa disebut dengan perdagangan elektronik (*e-commerce*) (Makarti, 2011). *E-commerce* merupakan aktivitas pembelian atau penjualan produk secara elektronik pada layanan *online* atau melalui internet, misalnya dapat memanfaatkan jaringan *area* lokal (LAN) atau jaringan pribadi *virtual* (VPN) sebagai media untuk mengirim transaksi (Rofiq & Mula, 2010). Perilaku belanja *online* ini, telah memengaruhi konsumen di seluruh dunia, mereka memilih untuk menggunakan *e-commerce* karena merasa nyaman dan tidak perlu membuang banyak waktu seperti berbelanja di pasar konvensional dan cenderung praktis dalam transaksinya. Berbagai kegiatan transaksi keuangan seperti membeli barang, transaksi uang ke akun lain, membeli layanan tertentu, dan sebagainya, dapat dilakukan dimana saja dengan menggunakan memanfaatkan situ *e-commerce* (Amiruddin *et al*., 2019).

Sistem pembayaran pada *e-commerce* menggunakan sistem pembayaran elektronik atau *digital*. Sistem pembayaran elektronik adalah cara modern transaksi moneter, yang telah muncul dalam pengembangan teknologi informasi di bawah naungan teknologi Jaringan. Pengoperasian pada pembayaran elektronik harus terhubung *online* ke lembaga keuangan atau pihak ketiga lainnya untuk memvalidasi pembayaran ketika konsumen melakukan transaksi. (Akintoye & Araoye, 2011)

Perkembangan pada *e-commerce* juga dapat berdampak negatif, yaitu dengan maraknya penipuan yang terjadi. Penipuan adalah tindakan yang dilakukan secara tidak jujur untuk menyakiti seseorang, dan biasanya dilakukan untuk mendapatkan berbagai manfaat yang seringkali bersifat finansial (JRana & Baria, 2015). Namun, beberapa *e-commerce* juga melakukan penipuan guna meningkatkan citra *platform* mereka untuk menarik pembeli. Menurut Wariati & Susanti (2014) penipuan yang biasa terjadi pada *e-commerce* yaitu toko palsu, pembayaran dimanipulasi, dan kerusakan pada barang atau barang tidak dikirim. Penipuan *e-commerce* ini terjadi karena kita kurang waspada dalam bertransaksi atau dapat disebabkan oleh penjual dan pembeli yang tidak saling bertemu satu sama lain sehingga mereka sangat rentan terhadap berbagai jenis penipuan (Hwang & Lai, 2015). Oleh karena itu, mendeteksi penipuan dan melakukan pencegahan diperlukan agar merasa aman ketika melakukan transaksi pada *e-commerce* (Valentin, 2013).

Mengingat maraknya penipuan pada situs *e-commerce* yang dapat mengakibatkan kerugian finansial yang cukup besar, sebagai konsumen perlu adanya pengetahuan mengenai jenis penipuan yang umum terjadi dan metode pencegahan yang digunakan untuk mendeteksi penipuan agar terhindar dari berbagai kerugian. Beberapa penelitian sebelumnya hanya membahas tentang identifikasi dan metode pencegahan penipuan *e-commerce* (Makarti, 2011; Chang & Chang, 2012; Syed & Shabbir, 2013; Valentin, 2013; Caldeira, Brandao, & Pereira, 2014; Leung, Lai, Chen, & Wan, 2014; Massa & Valverde, 2014; Hwang & Lai, 2015; JRana & Baria, 2015; Singh & Singh, 2015; Abdallah, Maarof, &

Zainal, 2016; Beránek, Nýdl, & Remeš, 2016; Gerlach, Pavlovic, & Gerlach, 2016; Lima & Pereira, 2016; Yang *et al*., 2016; Ramadhan & Amelia, 2016; Sun *et al*., 2017; Prisha, Neo, Ong, & Teo, 2017; Raghava-Raju, 2017; Shaji & Panchal, 2017; Wiralestari, 2017; Renjith, 2018; Weng *et al*., 2018; Zhao *et al*., 2018; Zheng *et al*., 2018); Amasiatu & Shah, 2019; Amiruddin *et al*., 2019; Carta *et al*., 2019; Raghavan & Gayar, 2019; Shah *et al*., 2019; Soomro *et al*., 2019. Sementara penelitian lainnya lebih fokus pada penipuan sistem pembayaran dan penipuan terkait dengan pelanggan (Keraf & Hidup, 2010; Rofiq & Mula, 2010; Raj & Portia, 2011; Hu, Liu, & Sambamurthy, 2011; Akintoye & Araoye, 2011; Saputro, Hukum, & Maret, 2011; Rofiq, 2012; Chaudhary & Mallick, 2012; Tripathi & Pavaskar, 2012; Wariati & Susanti, 2014; Shivagangadhar & Sathyan, 2015; Fitrianda, 2016; Tee & Ong, 2016; Goswami *et al*., 2017; Save *et al*, 2017; Pranita & Suardana, 2018; Nurhatinah, 2018; Porwal & Mukund, 2018; Choi, Chung, & Young, 2019; Chun, 2019; Giulietti & Assumpção, 2019; Mussardo, 2019; Sun, Fang, & Hwang, 2019; Ventre & Kolbe, 2020). Penelitian ini penting dilakukan karena gambar utuh tentang identifikasi penipuan pada *e-commerce* baik penipuan pada sistem pembayaran maupun penipuan yang terkait dengan pelanggan dirangkum lengkap, melalui proses pemetaan dengan merangkum dari 55 artikel yang dikumpulkan. Sehingga setelah membaca penelitian ini, diharapkan dapat menjadi sumber referensi bagi konsumen agar lebih waspada dalam bertransaksi pada situs *e-commerce*. Maka, penelitian ini bertujuan untuk mengetahui jenis penipuan yang dapat terjadi dalam perdagangan elektronik dan metode pencegahan yang dapat dilakukan, serta pertanyaan penelitian dari kajian ini adalah apa saja jenis penipuan

yang dapat terjadi pada situs *e-commerce* dan bagaimana metode pencegahan yang dapat dilakukan?

METODE PENELITIAN

Dalam penelitian ini disajikan review dengan metode pendekatan interpretif atas artikel-artikel yang berhasil dikumpulkan. Pendekatan interpretif juga disebut sebagai fenomenologi, yang berarti suatu penelitian kualitatif untuk mengungkap kesamaan makna yang menjadi esensi dari fenomena saat ini. Pendekatan interpretif dilakukan untuk mengembangkan sesuatu dibalik peristiwa dengan latar belakang pemikiran manusia (Hughes, 2008). Menurut Hasanadi (2019), pendekatan interpretif sangat memandang realitas sosial sebagai hal yang dinamis, berproses dan bermakna subjektif. Review yang disajikan telah melalui proses pemetaan sesuai dengan tujuan dari artikel ini yaitu tujuan dari artikel ini yaitu mengetahui jenis penipuan yang dapat terjadi dalam perdagangan elektronik dan pencegahan yang dapat dilakukan.

Langkah-langkah yang dilakukan untuk mendapatkan data yaitu pertama, artikel yang relevan dikumpulkan melalui situs Google Cendekia, Elsevier, Springer, Taylor & Francis, dan MDPI (Multidisciplinary Digital Publishing Institute) dengan kata kunci *"fraud in e-commerce", "identification fraud in e-commerce*", dan "kecurangan pada e-commerce" sehingga 105 artikel dikumpulkan. Kemudian harus dipastikan tidak ada artikel yang sama, tiga artikel dihapus sehingga terkumpul 102 artikel. Selanjutnya artikel dibatasi berdasarkan 10 tahun terakhir (2010-2020) dan diperoleh 73 artikel. Kemudian, 73 artikel

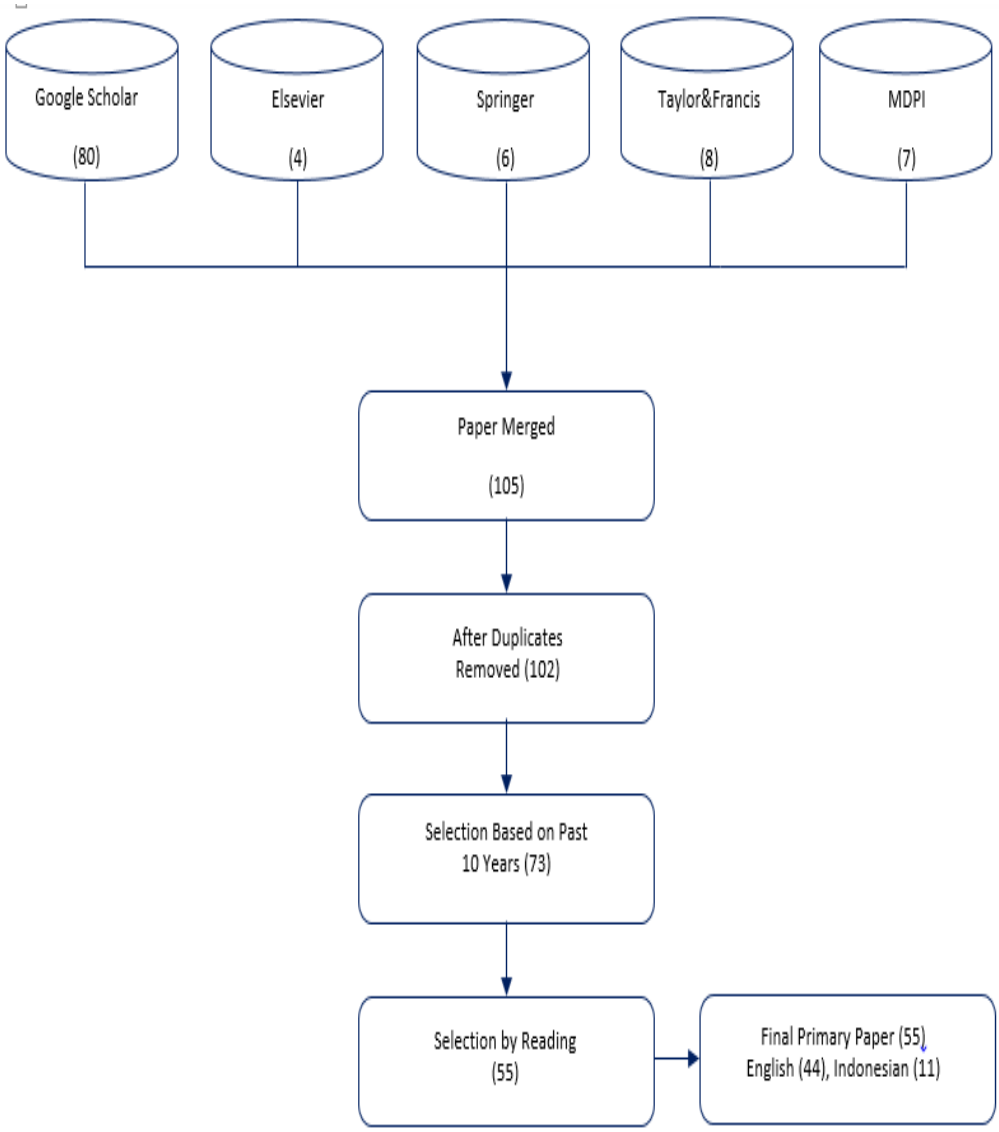
tersebut dibaca untuk mencari artikel yang paling terkait dengan pembahasan pada penelitian ini, sehingga dikumpulkan 55 artikel (Bahasa Inggris dengan 44 artikel dan Bahasa Indonesia dengan 11 artikel).

Setelah artikel terkumpul, dilakukan pemetaan terkait temuan artikel mengenai metode yang digunakan dan kesimpulan yang disajikan dalam setiap artikel, hingga akhirnya mencapai tujuan pada penelitian ini yaitu mengetahui jenis penipuan yang dapat terjadi dalam perdagangan elektronik dan pencegahan yang dapat dilakukan.

HASIL DAN PEMBAHASAN

Untuk menjawab pertanyaan penelitian ini yaitu apa saja jenis penipuan yang dapat terjadi pada situs *e-commerce* dan bagaimana metode pencegahan yang dapat dilakukan, artikel yang relevan dikumpulkan melalui situs *Google* Scholar, *Elsevier*, *Springer*, *Taylor & Francis*, dan MDPI (Multidisciplinary Digital Publishing Institute). Kata kunci yang digunakan dalam proses pencarian adalah: "*fraud in e-commerce*", "*identification of fraud in e-commerce*", dan "penipuan pada *e-commerce*". Pada tahap awal penelusuran diperoleh 105 artikel, terdapat tiga artikel yang sama, dikeluarkan, menghasilkan 103 artikel. Kemudian dilakukan seleksi lebih lanjut untuk membatasi pada artikel yang terbit 10 tahun terakhir. Proses ini menghasilkan 73 artikel. Berikutnya, 73 artikel itu dibaca secara menyeluruh untuk menentukan kesesuaian isinya dalam menjawab pertanyaan penelitian. Setelah membaca secara menyeluruh, diperoleh 55 artikel (44 artikel berbahasa Inggris dan 11 artikel berbahasa Indonesia) yang sesuai untuk menjawab

pertanyaan penelitian. Proses seleksi artikel ditampilkan pada Gambar 1.

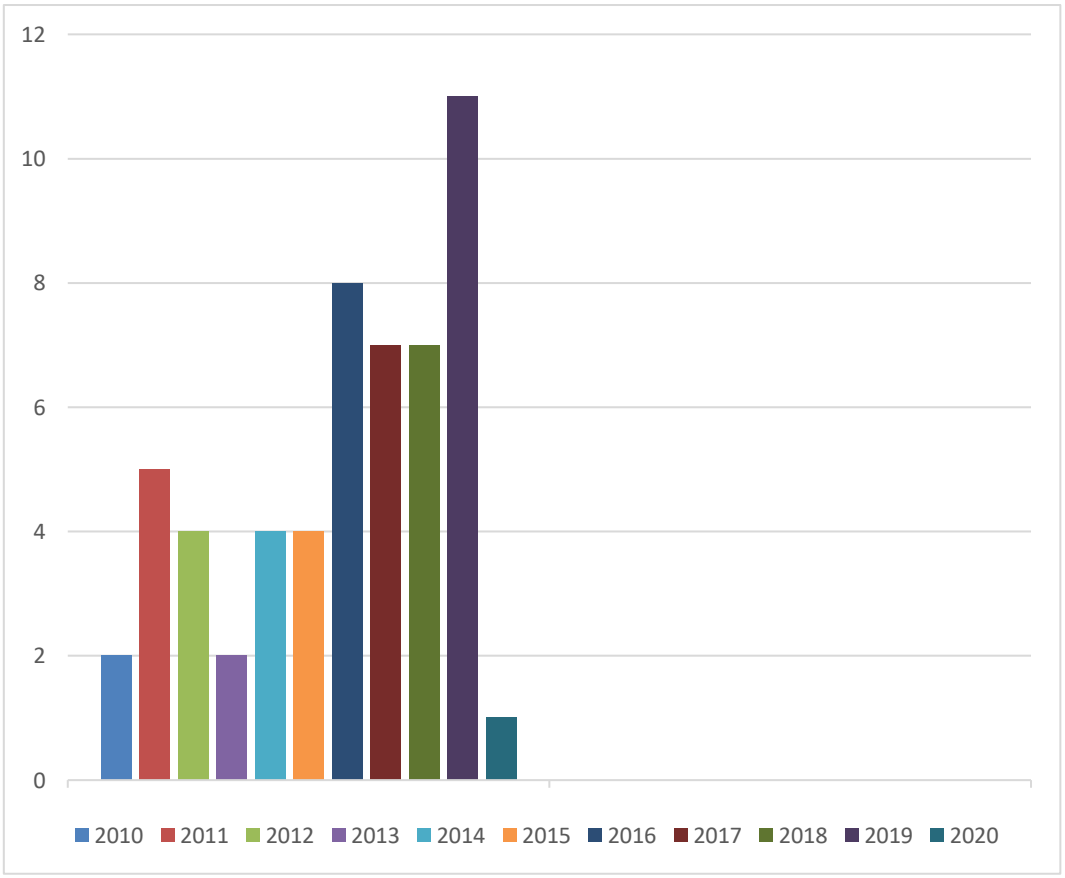


Sumber: diolah oleh penulis

Gambar 1.
Proses Seleksi Artikel

Penelitian ini membatasi penelusuran artikel pada artikel yang diterbitkan 10 tahun terakhir, yaitu tahun 2010 hingga 2020. Pembatasan ini dilakukan untuk mendapatkan perkembangan riset terkini. Hal ini penting mengingat perkembangan

e-commerce yang sangat pesat, begitupula dengan bentuk-bentuk penipuan yang terjadi. Gambar 2 menyajikan pengelompokan artikel berdasarkan tahun publikasi. Sebagaimana dapat dilihat pada Gambar 2, terdapat trend peningkatan jumlah penelitian terkait penipuan pada *e-commerce*, dengan jumlah terbesar pada tahun 2019, yaitu 11 artikel.



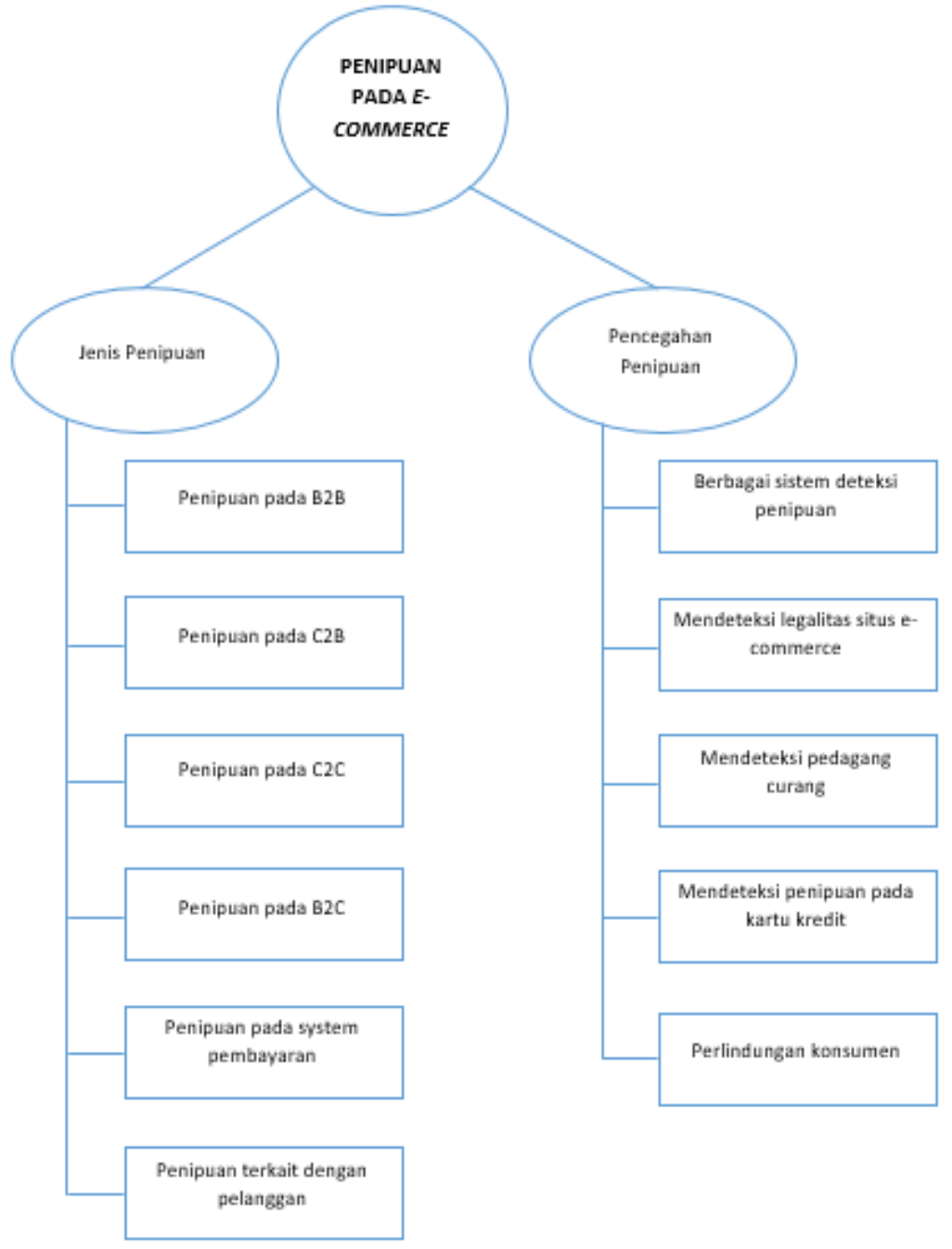
Sumber: diolah oleh penulis

Gambar 2.
Pengelompokan Artikel Berdasarkan Tahun Publikasi

Untuk menjawab pertanyaan penelitian ini, materi artikel-artikel yang digunakan dalam proses analisis interpretif dikelompokkan ke dalam tema-tema dan kode-kode. Gambar 3 menunjukkan hasil pemetaan tema dan kode dari 55

artikel yang dianalisis dalam penelitian ini.

Sumber: diolah oleh penulis



Gambar 3.
Peta Penelitian Terkait Penipuan Pada *E-commerce*

PEMBAHASAN

Mengidentifikasi penipuan dalam *E-commerce*. Kemajuan teknologi dalam bidang perdagangan memudahkan konsumen dalam memenuhi kebutuhan sehari-harinya dengan membeli barang atau jasa melalui internet (Fitrianda, 2016). Dengan banyaknya *platform-platform* yang tersedia dari berbagai negara, membuat konsumen dapat membandingkan harga dan kualitas produk dari masing-masing pedagang (Choi *et al*., 2019). Penyebab terjadinya penipuan *online* adalah adanya peretas, pelanggan jahat, pelanggan tidak puas, dan penjual yang saling bersaing (Leung *et al*., 2014). Raghava-Raju (2017) Transaksi bisnis *e-commerce* dapat dibagi menjadi empat kategori: Bisnis ke Bisnis (B2B) melibatkan satu perusahaan dengan perusahaan lainnya, Bisnis ke Konsumen (B2C) melibatkan penjual dan pembeli perorangan, Konsumen ke Bisnis (C2B) melibatkan pelaku bisnis perorangan dan bertransaksi dengan perusahaan, dan Konsumen ke Konsumen (C2C) melibatkan perorangan sebagai penjual dan pembeli individu (Giulietti & Assumpção, 2019).

Penipuan pada *e-commerce* bisa terjadi pada keempat kategori diatas, sesuai dengan artikel yang berhasil dikumpulkan, ditemukan contoh penipuan yang terjadi pada bisnis ke bisnis (B2B) yaitu penipuan pihak pertama di mana perusahaan ritel melakukan penipuan terhadap pengecer. Masalah ini umum terjadi di dunia B2B, dimana berbagai tindakan tidak bertanggung jawab yang dilakukan oleh perusahaan ritel maupun pengecer untuk meningkatkan keuntungan dalam bertransaksi (Amasiatu & Shah, 2019). Contoh adanya penipuan yang ddialami oleh pengecer, dalam penelitian Soomro *et al*., (2019) menemukan bahwa pengecer perlu

memahami manajemen penipuan agar tidak mengalami kerugian yang mengakibatkan hilangnya sejumlah pendapat mereka dan situasi penipuan yang tidak terkendali dapat menghambat perkembangan *e-commerce* dan kerugian yang signifikan di pasar modal. Penipuan lainnya yang ditemukan adalah *human clickers*, banyak perusahaan *e-commerce* menghasilkan pendapatan iklan dengan menjual klik (dikenal sebagai model Bayar-Per-Klik). Mekanismenya adalah perusahaan *e-commerce* dibayar setiap kali tautan iklan di situs web mereka diklik yang mengarah ke konten perusahaan *sponsor*. Tindak kecurangan yang dilakukan adalah perusahaan *e-commerce* yang tidak jujur dengan membayar orang (human clickers) untuk mengklik iklan ini sehingga perusahaan mendapatkan lebih banyak keuntungan (Beránek *et al*., 2016).

Salah satu contoh dari transasksi C2B adalah pembuatan desain logo yang dibuat oleh individu untuk suatu perusahaan *platform*. Penipuan yang mungkin terjadi misalnya individu yang membuat logo membawa kabur sejumlah uang dari perusahaan *platform* tersebut, maka dari itu perusahaan platform harus memilih individu yang berkompeten dan telah terpecaya dalam mendesain logo. Namun pada penelitian ini, tidak ditemukan artikel yang menjelaskan penipuan pada konsumen ke bisnis.

Penipuan berikutnya yang dapat terjadi pada *e-commerce* adalah penipuan situs lelang elektronik yang termasuk dalam kategori konsumen ke konsumen (C2C). Situs lelang elektronik telah berkembang dan menciptakan pasar *virtual* besar, di mana berbagai jenis barang tersedia yang mudah dibeli. Salah satu penipuan yang dapat terjadi yaitu penipu dapat menggunakan banyak akun untuk

menjalankan skema canggih sambil menyamarkan niat jahat mereka dan menghindari metode deteksi tradisional yang hanya memeriksa identitas individu (Chang & Chang, 2012). Mekanisme dalam lelang tersebut adalah menjual barang kepada penawar harga tertinggi, jadi untuk penipu yang memiliki banyak akun dan ingin membeli suatu barang, dia bisa saja menyamar menjadi orang-orang yang berbeda untuk memperebutkan barang tersebut. Beberapa penipuan sering diabaikan karena teknologi terselubung yang digunakan oleh penipu, membuat kerusakan signifikan hingga kerugian finansial yang tidak terdeteksi untuk waktu yang lama (Leung *et al*., 2014).

Implementasi jual beli *online* sebenarnya sering menimbulkan berbagai macam masalah, misalnya yang terjadi pada bisnis kepada konsumen (B2C) yang dapat disebabkan oleh ketidakjujuran, kesalahan manusia, atau kesalahan yang disebabkan oleh sistem elektronik, sehingga banyak konsumen mengalami kerugian yang menyebabkan konsumen takut untuk berbelanja *online* (Pranita & Suardana, 2018). Masalah lain yang dapat terjadi dalam transaksi *online* antara lain kualitas barang yang dipesan tidak sesuai dengan yang dijanjikan oleh pedagang, waktu pengiriman yang terlambat, dan kerusakan barang dalam proses pengiriman. Diantara kategori *e-commerce* tersebut, B2C merupakan kegiatan yang paling sering terjadi dalam ekonomi digital (Rofiq, 2012). Oleh karena itu, penelitian ini berfokus pada transaksi penipuan B2C yang dilakukan oleh suatu perusahaan bisnis dan konsumen sebagai pengguna akhir, secara umum posisi konsumen tidak sekuat perusahaan sehingga konsumen berpotensi mengalami beberapa masalah atau tindak penipuan, terutama pada transaksi pembayaran online (Saputro *et al*., 2011).

Kemajuan teknologi informasi telah memfasilitasi inovasi dalam pembayaran elektronik yang dapat digunakan saat bertransaksi dalam *e-commerce*, membayar barang dan jasa yang diperdagangkan tanpa menggunakan uang tunai fisik (Tee & Ong, 2016). Pembayaran tanpa uang tunai adalah pembayaran dalam bentuk *digital* sebagai media untuk bertukar barang dan jasa, misalnya pembayaran secara *transfer* atau menggunakan kartu kredit dengan hanya mencantumkan nomor kartu kredit pada platform e-*commerce*.

Penipuan kartu kredit adalah salah satu jenis penipuan yang sering terjadi dalam proses pembayaran pada *e-commerce*, banyak orang jahat mencoba mencuri informasi sensitif dari transaksi tanpa uang tunai ini yang menciptakan 535 risiko besar bagi seluruh ekosistem (Carta *et al*., 2019). Inilah sebabnya, sistem deteksi penipuan yang perlu berorientasi dalam menemukan penipuan kartu kredit, menjadi semakin penting. Sayangnya, para penipu memiliki pola tindakan yang berbeda setiap menjalankan aksinya, ini karena penipu terus berinovasi tentang cara-cara baru untuk mengelabui seseorang dan sistem *online*. Deteksi penipuan kartu kredit adalah salah satu masalah yang sering disebut sebagai masalah deteksi *outlier* (Porwal & Mukund, 2018).

Penipuan kartu kredit telah dibagi menjadi dua jenis (Tripathi & Pavaskar, 2012): Penipuan *offline* dan Penipuan *online*. Penipuan *offline* dilakukan dengan mencuri kartu secara fisik dan menggunakan kartu kredit tersebut untuk melakukan transaksi seperti biasa. Penipuan *online* dilakukan melalui internet, telepon, belanja, *web*, atau tanpa pemegang kartu. Penjahat mencuri informasi dari kartu kredit dan debit, yang dikenal sebagai *skimming* (Gerlach *et al*., 2016). *Skimming* dapat

diartikan menjadi dua hal yaitu kebocoran *database* perbankan dan *skimming* dapat terjadi pada mesin ATM atau mesin *skimming* EDC disertai dengan kamera *peep pin*. Menurut (Chaudhary & Mallick, 2012), tidak hanya penipuan yang dapat terjadi pada kartu kredit namun kartu kredit juga dapat mengalami permasalahan internal yaitu hubungan antara penyedia kartu dan pemegang kartu, misalnya kesalahan pada sistem atau perbankan penyedia kartu kredit yang memberi dampat buruk bagi pemegang kartu.

Menurut (Rofiq, 2012) *E-commerce* adalah sistem yang kompleks yang melibatkan teknologi dan manusia. Hubungan *e-commerce* dengan pelanggan sebagian besar terkait dengan aspek psikologis seperti persepsi, kepercayaan, dan kenyamanan. Dengan sukses besar dari *e-commerce*, banyak layanan promosi jahat juga meningkat, pedagang jahat berusaha untuk mempromosikan barang-barang yang ditargetkan dengan cara mengoptimalkan hasil pencarian menggunakan kunjungan palsu atau pembelian untuk mencapai keuntungan yang diinginkan (Weng *et al*., 2018).

Seiring dengan perkembangan *e-commerce* membuat meningkatnya rasa keingintahuan dalam memahami faktor-faktor yang memengaruhi pengambilan keputusan konsumen untuk membeli suatu produk. (Ventre & Kolbe, 2020) dalam penelitiannya mengkonfirmasi bahwa ulasan *online* pada toko tersebut memberikan efek positif terhadap niat beli, karea ketika konsumen ingin membeli suatu barang, pelanggan membaca *detail* produk dan ulasan toko sebelum memutuskan di mana akan membeli dan apakah akan membeli atau tidak. Namun, penelitian dari (Shivagangadhar & Sathyan, 2015) mengatakan bahwa terdapat ulasan palsu dalam

e-commerce. Pada dasarnya ulasan *online* juga sangat penting bagi toko itu sendiri dalam membuat keputusan mengenai pengembangan bisnisnya (Goswami *et al*., 2017). Ulasan palsu ini sengaja ditulis untuk memanipulasi produk atau toko sehingga menarik minat pembeli, dan dari sisi negatifnya ulasan online tersebut dapat mencemarkan nama baik pedagang itu sendiri, misalnya saingan pedagang tersebut dengan sengaja memberikan ulasan negatif kepada toko tersebut. Manipulasi pada ulasan *online* tersebut dapan mengurangi informasi yang dibutuhkan dari suatu barang atau servis yang ditawarkan. Perlu diketahui, tidak semua pedagang akan memanipulasi ulasan online, karena beberapa konsumen tidak hanya berfokus pada ulasan yang disampaikan, ada juga konsumen yang menggunakan harga sebagai indikator kualitas barang tersebut (Hu *et al*., 2011).

Permasalahan tidak hanya dirasakan oleh konsumen, tetapi juga dapat dirasakan oleh perusahaan atau toko yang menjual barang. Banyak konsumen masih ragu untuk mengungkapkan informasi mereka karena masalah *privasi*. Untuk membantu perusahaan mengumpulkan lebih banyak informasi pengguna, penelitian (Sun *et al*., 2019) menyelidiki bagaimana anteseden *privasi* dari pengalaman pembelian yang memengaruhi kekhawatiran *privasi* pengguna dan bagaimana cara lebih lanjut agar aman dalam pengungkapan informasi pengguna berdasarkan pada *Model Privacy Antecedent-Privacy Concern-Outcomes (APCO*) dan teori kalkulus privasi.

Mencegah penipuan dalam *e-commerce***.** Permasalahan pada dunia *e-commerce* sangat sering terjadi sehingga menjadi hal yang biasa, tetapi sulit untuk menentukan seberapa besar risiko yang akan diterima, maka perlu dilakukan

pendeteksian penipuan dengan berbagai macam metode (Chun, 2019). Banyak teknik atau metode modern seperti Kecerdasan Buatan, Penambangan data, Jaringan Saraf Tiruan, Jaringan *Bayesian*, Sistem Kekebalan Buatan, algoritma tetangga terdekat, Mesin Pendukung Vektor, Pohon Pengambilan Keputusan, Sistem Berbasis Logika *Fuzzy*, Pembelajaran Mesin, Penyelarasan Urutan, Pemrograman Genetik, *CLUE, Adaptive Neuro-Fuzzy Inference System*, Situs *Web* Bantuan Perlindungan (PAW), Mod*el Privacy Antecedent-Privacy Concern-Outcomes* (APCO), dll. , telah berevolusi dalam mendeteksi berbagai transaksi penipuan kartu kredit (Raj & Portia, 2011). Kegiatan penipuan biasanya tidak terdeteksi karena kurangnya kemampuan untuk mengidentifikasi penipuan yang terjadi. Untuk mengatasi penipuan dalam *e-commerce*, menurut Abdallah *et al*., (2016) sistem pencegahan penipuan (FPS) saja tidaklah cukup untuk menyediakan keamanan yang memadai pada sistem perdagangan elektronik perlu adanya deteksi penipuan yang dilakukan. Deteksi penipuan adalah aplikasi spesifik deteksi anomali, yang ditandai dengan ketidakseimbangan besar antara kelas, yang dapat menjadi faktor berbahaya untuk teknik pemilihan fitur (Lima & Pereira, 2016). Oleh karena itu, kolaborasi antara FDSs (*Fraud detection system*) dengan FPSs (*Fraud prevention systems*) dirasa efektif untuk mengamankan sistem perdagangan elektronik.

Bedasarkan artikel yang dikumpulkan, terdapat beberapa metode yang dapat digunakan untuk mendeteksi penipuan yaitu sebagai berikut: Pada artikel Sun *et al*., (2017) menyajikan CLUE, sistem deteksi penipuan transaksi berbasis pembelajaran yang menangkap informasi rinci tentang klik pengguna

menggunakan penanaman berbasis *neural network*, dan memodelkan urutan klik menggunakan jaringan saraf berulang. Pencegahan penipuan yang diusulkan oleh Raghavan & Gayar (2019) menggunakan pohon keputusan, *random forest*, jaringan saraf tiruan, dan *naïve Bayes* dan hasilnya menunjukkan bahwa akurasi tertinggi adalah 96% jaringan saraf, kemudian *random forest* dan *Naïve Bayes* adalah 95 %, untuk akurasi pohon keputusan adalah 91%. Artikel oleh Massa & Valverde (2014) mengusulkan sistem deteksi penipuan menggunakan teknik deteksi anomali yang berbeda untuk memprediksi serangan intrusi komputer dalam *e-commerce*, sistem menganalisis kueri yang dihasilkan ketika meminta kode sisi *server* pada situs *e-commerce* dan membuat model untuk fitur yang berbeda. Sedangkan metode lain yang tawarkan oleh Shaji & Panchal (2017) yaitu mengusulkan teknik berdasarkan ANFIS (*Adaptive Neuro-Fuzzy Inference System*) akan menjadi pilihan yang lebih baik untuk deteksi penipuan, untuk meningkatkan efisiensi proses deteksi penipuan. Metode pencegahan lain yang disediakan oleh Prisha *et al*., (2017) adalah menghadirkan kerangka kerja keamanan konseptual yang dirancang untuk membuat konsumen merasa aman dan meningkatkan pengalaman pengguna saat bertransaksi di situs *web e-commerce*. Kerangka kerja ini terdiri dari sesi *login* yang aman dengan verifikasi gambar, otentikasi sidik jari, dan agen analisis risiko untuk mengotorisasi dan menyetujui transaksi pengguna. Pada awalnya, pengguna harus mendaftar dengan ID unik yang terdiri dari kata dan angka, kemudian kata sandi yang harus diikuti secara alfanumerik dengan memilih gambar untuk keperluan verifikasi. Beberapa artikel lain juga membahas mengenai deteksi penipuan pada kurangan pedagang dan transaksi serta mendeteksi penipuan pada kartu kredit

menggunakan *data mining*, pohon keputusan dan *3D Secure*.

Berdasarkan artikel Ramadhan & Amelia (2016) untuk mengidentifikasi penipuan yakni dapat dilakukan dengan membangun Situs Web Bantuan Perlindungan (PAW) yang dapat memberikan informasi tentang legalitas situs *e-commerce*. PAW adalah aplikasi yang berisi pertanyaan yang mengarah pada pengujian situs *e-commerce* dan dibuat dengan konsep aplikasi yang cerdas, ramah pengguna, dan mudah digunakan. Selanjutnya, penipuan dapat terjadi karena pedagang yang memanfaatkan situasi untuk bertindak curang, pada artikel Renjith, (2018) mengusulkan model berdasarkan pencarian informasi dan klasifikasi SVM (*Support Vector Machine*) untuk secara proaktif mendeteksi pedagang yang curang berdasarkan kinerja masa lalu mereka, di mana model ini menggunakan kekuatan analitik media sosial untuk memahami dan mempertimbangkan apa yang dipikirkan orang tentang layanan/produk yang disediakan oleh penjual tertentu melalui pasar. Kecurangan transaksi juga dapat terjadi pada *e-commerce*, hal ini dapat dihindari dengan mendeteksi penipuan dengan mengekstraksi *profil* perilaku pengguna (BP) berdasarkan catatan transaksi historis pengguna. Zheng *et al*., (2018) mengusulkan grafik logis dari BP (LGBP) yang merupakan model berdasarkan pesanan total untuk mewakili hubungan logis dari atribut catatan transaksi. Berdasarkan LGBP dan catatan transaksi pengguna, maka dapat diverifikasi apakah transaksi yang masuk itu curang atau tidak.

Data mining sering digunakan dalam mendeteksi dan mengklasifikasikan penipuan yang terjadi *e-commerce*, alasannya adalah bahwa teknik *data mining* telah relevan dalam menyelesaikan tantangan ini karena dapat menangani sejumlah

besar data (Syed & Shabbir, 2013). Temuan Caldeira *et al*., (2014) mengatakan bahwa dalam menangani penipuan kartu kredit, teknik *data mining* yang digunakan untuk FFD (Financial Fraud Detection) adalah model logistik, jaringan saraf, jaringan kepercayaan *Bayesian*, dan pohon keputusan, semua model ini memiliki satu tujuan, yaitu deteksi dan klasifikasi data penipuan. Cara lain yang diungkapkan Yang *et al*., (2016), model yang efektif dan sistematis dapat membatasi transaksi penipuan pesanan online dalam layanan *e-commerce*, yaitu menggunakan metode *analytic mining* dan studi kasus. Kolaborari *data mining* dan *artificial intelligence* juga dirasa efekti bagi Singh & Singh (2015) untuk mencegah pelanggan dari penipuan transaksi *online*. Selain menggunakan *data mining* untuk mendeteksi penipuan pada kartu kredit, artikel Save *et al*., (2017) mengusulkan pohon keputusan dengan kombinasi algoritma *Luhn* dan algoritma *Hunt*. Algoritma *Luhn* digunakan untuk memvalidasi nomor kartu dan kemudian menggunakan *Address Mismatch*, jika kedua alamat tersebut cocok antara alamat penagihan dan alamat pengiriman, transaksi dapat diklasifikasikan sebagai otentik dengan probabilitas tinggi. Hasil penelitian dari Mussardo (2019) menunjukkan bahwa dengan menggunakan 3D Secure pada setiap transaksi kartu kredit dapat meningkatkan keamanan dalam transaksi, tetapi dalam praktiknya ini belum sepenuhnya terwujud karena bank tidak selalu memberikan tanggung jawab penuh kepada pelanggan untuk penipuan yang terjadi, bank hanya memberikan bantuan untuk mengidentifikasi penipuan yang terjadi dalam proses transaksi.

Pihak-pihak yang terlibat dalam transaksi *e-commerce* biasanya tidak sepenuhnya percaya satu sama lain, pedagang perlu memperhatikan keamanan

konsumen, *privasi* konsumen, dan reputasi toko mereka untuk mempengaruhi kepercayaan konsumen dalam berbelanja *online*, sehingga dapat disimpulkan bahwa kepercayaan adalah faktor terpenting dalam melakukan transaksi baik *online* maupun *offline* (Nurhatinah, 2018). Beberapa cara yang dapat dilakukan untuk menghindari penipuan dalam *e-commerce* adalah tidak mudah tergoda oleh harga murah, menyimpan bukti pembayaran dengan benar, jangan mudah tertipu oleh testimonial, meminta foto asli barang yang akan dibeli, selalu meminta pengiriman nomor tanda terima. Saran yang dapat diberikan untuk pedagang adalah lebih meningkatkan kepercayaan konsumen dan pedagang harus memberikan hak-hak konsumen, yaitu memberikan informasi yang jelas tentang produk yang akan dibeli, produk yang dijual tidak berbahaya, produk yang dikirim sesuai dengan keinginan konsumen, konsumen tahu cara menggunakannya, jaminan bahwa produk yang dibeli konsumen dapat bermanfaat dan berfungsi dengan baik, serta jaminan bahwa jika barang yang dibeli konsumen tidak sesuai maka konsumen akan mendapatkan pengganti dalam bentuk baik produk ataupun uang (Keraf & Hidup, 2010). Pemerintah juga berpartisipasi dalam menegakkan hukum yang berlaku pada Undang-Undang Nomor 8 Tahun 1999 tentang perlindungan konsumen. Menurut Wiralestari (2017), penipuan adalah sesuatu yang melanggar hukum dan dilakukan dengan sengaja yang diperjuangkan oleh akuntansi forensik dan dibuktikan secara khusus oleh audit investigasi. Untuk alasan ini, akuntansi forensik dan audit investigasi adalah cara terbaik untuk mendeteksi dan mencegah penipuan. Beberapa studi merekomendasikan teknik untuk memerangi penipuan dalam e-commerce, tetapi seiring waktu akan ada banyak literatur tentang penipuan dalam *e-commerce*

yang menawarkan praktik terbaik berkelanjutan (Shah *et al*., 2019). Penting dan perlu untuk mengembangkan dan menerapkan teknik yang dapat membantu mendeteksi penipuan dalam transaksi. Tidak ada sistem deteksi penipuan yang sempurna, perlu ada pendekatan alternatif untuk mengantisipasi kegagalan yang terjadi dalam memerangi penipuan pada *e-commerce.* Misalnya dalam Zhao *et al*., (2018) penelitian berfokus pada penjual mereka yang dapat memaksimalkan laba *platform,* dan mengabaikan pengaruh pada perilaku penipuan penjual.

SIMPULAN DAN SARAN

Meningkatkan sistem informasi telah mendorong kemajuan teknologi di bidang bisnis komersial yaitu munculnya pendagangan elektronik (*e-commerce*). Dengan adanya perkembangan yang terus-menerus tidak menutup kemungkinan bahwa penipuan-penipuan juga semakin marak terjadi. Penipuan yang paling banyak terjadi adalah mengenai sistem pembayaran yang menggunakan transaksi tanpa uang tunai serta penipuan yang berkaitan dengan ulasan konsumen karena beberapa pelanggan cenderung melihat ulasan sebagai acuan membeli suatu barang. Penipuan juga dapat terjadi pada keempat kategori *e-commerce* yaitu: penipuan pada B2B dengan adanya perilaku yang tidak bertanggung jawab dari perusahaan ritel hingga mengakibatkan kerugian bagi pengecer, kemudian penipuan pada C2B misalnya individu yang membuat logo membawa kabur sejumlah uang dari perusahaan *platform,* selanjutnya penipuan pada C2C contohnya banyaknya akun-akun ganda yang terdapat di situs lelang elektronik, yang terahir penipuan pada B2C

yang merupakan penipuan yang paling sering terjadi karena konsumen sebagai pengguna terahir tidaklah memiliki posisi yang kuat seperti perusahaan, contohnya kualitas barang yang dipesan tidak sesuai dengan yang dijanjikan oleh pedagang, waktu pengiriman yang terlambat, dan kerusakan barang dalam proses pengiriman. Maka dari itu, dalam penelitian ini disajikan berbagai metode modern pendeteksi penipuan, seperti *data mining*, jaringan *bayesan*, algoritma, mesin pendukung vector, pemrograman genetik, pohon pengambilan keputusan, *Adaptive Neuro-Fuzzy Inference System*, Situs Web Bantuan Perlindungan (PAW), *Model Privacy Antecedent-Privacy Concern-Outcomes* (APCO), dll.

Dengan adanya penelitian ini, diharapkan agar konsumen baik penjual maupun pembeli harus lebih waspada dalam bertransaksi di situs *e-commerce*. Saat melakukan transaksi jual-beli dalam *e-commerce*, pastikan semua transaksi dilakukan di dalam *platform* yang tersedia dan jangan pernah mengirim uang langsung ke rekening pribadi penjual. Semua *platform* sudah memiliki aturannya masing-masing, jadi patuhilah standard dan ketentuan yang berlaku.

REFERENSI

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, *68*, 90–113. https://doi.org/10.1016/j.jnca.2016.04.007

Akintoye, K. A., & Araoye, O. I. (2011). Combating E-Fraud on Electronic Payment System. *International Journal of Computer Applications*, *25*(8), 48–53. https://doi.org/10.5120/3048-4144

Amasiatu, C. V., & Shah, M. H. (2019). The management of first party fraud in e-tailing: a qualitative study. *International Journal of Retail and Distribution Management*, *47*(4), 433–452. https://doi.org/10.1108/IJRDM-07-2017-

0142

Amiruddin, M. M., Haq, I., Hasanuddin, H., Ilham, M., Syatar, A., & Arief, M. (2019). Mitigating Fraud in e-commerce by adapting the Concept of Siri' na pacce. KURIOSITAS: Media Komunikasi Sosial Dan Keagamaan, 12(1), 76-93. https://doi.org/10.35905/kur.v12i1.799

Beránek, L., Nýdl, V., & Remeš, R. (2016). Click Stream Data Analysis for Online Fraud Detection in E-Commerce. *České Budějovice*, 175–180.

Caldeira, E., Brandao, G., & Pereira, A. C. M. (2014). Fraud analysis and prevention in e-commerce transactions. *Proceedings - 9th Latin American Web Congress, LA-WEB 2014*, (August 2016), 42–49. https://doi.org/10.1109/LAWeb.2014.23

Carta, S., Fenu, G., Reforgiato Recupero, D., & Saia, R. (2019). Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model. *Journal of Information Security and Applications*, *46*, 13–22. https://doi.org/10.1016/j.jisa.2019.02.007

Chang, W. H., & Chang, J. S. (2012). An effective early fraud detection method for online auctions. *Electronic Commerce Research and Applications*, *11*(4), 346–360. https://doi.org/10.1016/j.elerap.2012.02.005

Chaudhary, K., & Mallick, B. (2012). Credit Card Fraud: The study of its impact and detection techniques. *International Journal of Computer Science and Network*, *1*(4), 2277–5420.

Choi, D., Chung, C. Y., & Young, J. (2019). Sustainable online shopping logistics for customer satisfaction and repeat purchasing behavior: Evidence from China. *Sustainability (Switzerland)*, *11*(20). https://doi.org/10.3390/su11205626

Chun, S. H. (2019). E-commerce liability and security breaches in mobile payment for e-business sustainability. *Sustainability (Switzerland)*, *11*(3). https://doi.org/10.3390/su11030715

Fitrianda, M. I. (2016). *Digital Digital Repository Repository Universitas Universitas Jember Jember Digital Digital Repository Repository Universitas Universitas Jember diakses tahun 2018*.

Gerlach, A., Pavlovic, S., & Gerlach, A. (2016). *Improving e-commerce fraud investigations in virtual , inter-institutional teams : Towards an approach based on Semantic Web technologies Master Thesis Contact details :* (August 2016).

Giulietti, & Assumpção. (2019). Perlindungan Pengguna E-commerce agar Tetap Aman Bertransaksi di Kiosdelima.com. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Goswami, K., Park, Y., & Song, C. (2017). Impact of reviewer social interaction on online consumer review fraud detection. *Journal of Big Data*, *4*(1). https://doi.org/10.1186/s40537-017-0075-6

Hasanadi, H. (2019). Kearifan Lokal Dalam Ungkapan Tradisional: Membaca Ulang Karakteristik Masyarakat Pasaman Barat. *Jurnal Penelitian Sejarah Dan Budaya*, *4*(1), 1032–1047. https://doi.org/10.36424/jpsb.v4i1.100

Hu, N., Liu, L., & Sambamurthy, V. (2011). Fraud detection in online consumer reviews. *Decision Support Systems*, *50*(3), 614–626. https://doi.org/10.1016/j.dss.2010.08.012

Hughes, R. (2008). 済無No Title No Title. *Journal of Chemical Information and Modeling*, *53*(9), 287. https://doi.org/10.1017/CBO9781107415324.004

Hwang, R. J., & Lai, C. H. (2015). Provable fair document exchange protocol with transaction privacy for e-commerce. *Symmetry*, *7*(2), 464–487. https://doi.org/10.3390/sym7020464

JRana, P., & Baria, J. (2015). A Survey on Fraud Detection Techniques in Ecommerce. *International Journal of Computer Applications*, *113*(14), 5–7. https://doi.org/10.5120/19892-1898

Keraf, S., & Hidup, E. L. (2010). Etika Bisnis Dalam E-commerce. *Jakarta: PT Kompas Media Nusantara*, hlm.71-75.

Leung, V. C. M., Lai, R. X., Chen, M., & Wan, J. (2014). Cloud computing: 5th International Conference, CloudComp 2014 Guilin, China, october 19-21, 2014 revised selected papers 123. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *142*, 98–106. https://doi.org/10.1007/978-3-319-16050-4

Lima, R. F., & Pereira, A. C. M. (2016). A fraud detection model based on feature selection and undersampling applied to web payment systems. *Proceedings - 2015 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology, WI-IAT 2015*, (January 2018), 219–222. https://doi.org/10.1109/WI-IAT.2015.13

Makarti, A. (2011). *100 Among Makarti, Vol.4 No.8, Desember 2011*. *4*(8), 100–122.

Massa, D., & Valverde, R. (2014). A Fraud Detection System Based on Anomaly Intrusion Detection Systems for E-Commerce Applications. *Computer and Information Science*, *7*(2), 117–140. https://doi.org/10.5539/cis.v7n2p117

Mussardo, G. (2019). Perlindungan Hukum Terhadap Nasabah Pengguna Kartu Kredit Dalam Transaksi E-commerce. *Statistical Field Theor*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Nurhatinah. (2018). *Pengaruh Keamanan, Privasi, Dan Reputasi Terhadap Kepercayaan Konsumen Online Shopping Di Kota Padang*. *1*.

Porwal, U., & Mukund, S. (2018). *Credit Card Fraud Detection in e-Commerce: An Outlier Detection Approach*. Retrieved from http://arxiv.org/abs/1811.02196

Pranita, N. K. P., & Suardana, I. W., A. An. W. (2018). Perlindungan Hukum Terhadap Konnsumen Transaksi e-commerce Dalam Hal Terjadinya Kerugian. *Kertha Semaya : Journal Ilmu Hukum*, *7*(2), 1-16. Retrieved from https://ojs.unud.ac.id/index.php/kerthasemaya/article/view/52982/31328

Prisha, P., Neo, H. F., Ong, T. S., & Teo, C. C. (2017). E-Commerce security and identity integrity: The future of virtual shopping. *Advanced Science Letters*, *23*(8), 7849–7852. https://doi.org/10.1166/asl.2017.9592

Raghava-Raju, A. (2017). Predicting Fraud in Electronic Commerce: Fraud Detection Techniques in E-Commerce. *International Journal of Computer Applications*, *171*(2), 18–22. https://doi.org/10.5120/ijca2017914977

Raghavan, P., & Gayar, N. El. (2019). Fraud Detection using Machine Learning and Deep Learning. *Proceedings of 2019 International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2019*, *10*(9), 334–339. https://doi.org/10.1109/ICCIKE47802.2019.9004231

Raj, S. B. E, & Portia, A. A. (2011). Analysis on credit card fraud detection methods. *2011 International Conference on Computer, Communication and Electrical Technology, ICCCET 2011*, 152–156. https://doi.org/10.1109/ICCCET.2011.5762457

Ramadhan, M., & Amelia, M. (2016). *Membangun Protection Assistance Website (PAW) untuk Mendeteksi Kecurangan Pada Situs E-Commerce*. *7*(1), 43–50.

Renjith, S. (2018). Detection of Fraudulent Sellers in Online Marketplaces using Support Vector Machine Approach. *International Journal of Engineering Trends and Technology*, *57*(1), 48–53. https://doi.org/10.14445/22315381/ijett-v57p210

Rofiq, A., & Mula, J. M. (2010). *Impact of Cyber Fraud and Trust on e-Commerce Use : A Proposed Model by Adopting Theory of Planned Behaviour*. 1–9.

Rofiq, Ainur. (2012). *Impact of cyber fraud and trust of e-commerce system on purchasing intentions: analysing planned behaviour in Indonesian business*. 259. Retrieved from https://eprints.usq.edu.au/23432/

Saputro, R. B., Hukum, F., & Maret, U. S. (2011). *Analisis Asuransi Kerugian Dalam Transaksi Bisnis Melalui Internet (E-Commerce)*.

Save, P., Tiwarekar, P., N., K., & Mahyavanshi, N. (2017). A Novel Idea for Credit Card Fraud Detection using Decision Tree. *International Journal of Computer Applications*, *161*(13), 6–9. https://doi.org/10.5120/ijca2017913413

Shah, M. H., Jones, P., & Choudrie, J. (2019). Cybercrimes prevention: promising organisational practices. *Information Technology and People*, *32*(5), 1125–1129. https://doi.org/10.1108/ITP-10-2019-564

Shaji, J., & Panchal, D. (2017). Improved fraud detection in e-commerce transactions. *2017 2nd International Conference on Communication Systems, Computing and IT Applications, CSCITA 2017 - Proceedings*, 121–126. https://doi.org/10.1109/CSCITA.2017.8066537

Shivagangadhar, K., & Sathyan, S. (2015). Fraud Detection in Online Reviews using Machine Learning Techniques. *ISSN || International Journal of Computational Engineering Research*, *05*, 2250–3005. Retrieved from www.ijceronline.com

Singh, P., & Singh, M. (2015). Fraud Detection by Monitoring Customer Behavior and Activities. *International Journal of Computer Applications*, *111*(11), 23–32. https://doi.org/10.5120/19584-1340

Soomro, Z. A., Ahmed, J., Shah, M. H., & Khoumbati, K. (2019). Investigating identity fraud management practices in e-tail sector: a systematic review. *Journal of Enterprise Information Management*, *32*(2), 301–324. https://doi.org/10.1108/JEIM-06-2018-0110

Sun L., Wang Y., Cao B., Yu P.S., Srisa-an W., Leow A.D. (2017) Sequential Keystroke Behavioral Biometrics for Mobile User Identification via Multi-view Deep Learning. In: Altun Y. et al. (eds) Machine Learning and Knowledge Discovery in Databases. ECML PKDD 2017. *Lecture Notes in Computer Science*, vol 10536. Springer, Cham. https://doi.org/10.1007/978-3-319-71273-4_19

Sun, Y., Fang, S., & Hwang, Y. (2019). Investigating privacy and information

disclosure behavior in social electronic commerce. *Sustainability (Switzerland)*, *11*(12). https://doi.org/10.3390/su10023311

Syed, A., & Shabbir, K. R. (2013). An Effective Fraud Detection System Using Mining Technique. *International Journal of Scientific and Research Publications*, *3*(5), 3–6. Retrieved from www.ijsrp.org

Tee, H. H., & Ong, H. B. (2016). Cashless payment and economic growth. *Financial Innovation*, *2*(1), 1–9. https://doi.org/10.1186/s40854-016-0023-z

Tripathi, K. K., & Pavaskar, M. A. (2012). Survey on Credit Card Fraud Detection Methods. *International Journal of Emerging Technology and Advanced Engineering*, *2*(11), 721.

Valentin, S. B. (2013). Fraud in Electronic Commerce. *Perspectives of Business Law Journal*, *2*(1).

Ventre, I., & Kolbe, D. (2020). The Impact of Perceived Usefulness of Online Reviews, Trust and Perceived Risk on Online Purchase Intention in Emerging Markets: A Mexican Perspective. *Journal of International Consumer Marketing*, *0*(0), 1–13. https://doi.org/10.1080/08961530.2020.1712293

Wariati, A., & Susanti, N. I. (2014). E-Commerce Dalam Perspektif Perlindungan Konsumen. *Jurnal Ekonomi &Bisnis. Edisi Nopember*, *1*(2). Retrieved from http://www.????

Weng, H., Li, Z., Ji, S., Chu, C., Lu, H., Du, T., & He, Q. (2018). Online e-commerce fraud: A large-scale detection and analysis. *Proceedings - IEEE 34th International Conference on Data Engineering, ICDE 2018*, (2), 1441–1452. https://doi.org/10.1109/ICDE.2018.00162

Wiralestari, W. (2017). Fraud: Akuntansi Forensik Dan Audit Investigatif. *Media Riset Akuntansi*, *6*(1), Hal. 43-59.

Yang, Q., Wei, X., & QuanLiu, Y. (2016). Anti-Fraud Schema System for Identification and Prevention of Fraud Behaviors in E-Commerce Services. *Global Journal of Computer Science and Technology*, *16*(4), 6-16

Zhao, M., Li, Z., An, B., Lu, H., Yang, Y., & Chu, C. (2018). Impression allocation for combating fraud in E-commerce via deep reinforcement learning with action norm penalty. *IJCAI International Joint Conference on Artificial Intelligence*, *2018-July*, 3940–3946. https://doi.org/10.24963/ijcai.2018/548

Zheng, L., Liu, G., Yan, C., & Jiang, C. (2018). Transaction fraud detection based on total order relation and behavior diversity. *IEEE Transactions on Computational Social Systems*, *5*(3), 796–806. https://doi.org/10.1109/TCSS.2018.2856910