PEMETAAN BERBAGAI PERMASALAHAN DALAM *SECURITY E-COMMERCE*

Jeni Beatrix Karay[1], Irwan Sembiring[2], Hindriyanto Dwi Purnomo[3]
Fakultas Teknologi Informasi, Program Magister Sistem Informasi
Universitasi Kristen Satya Wacana
karayjeni@gmail.com

ABSTRAK

Berbagai perkembangan teknologi membuat *e-commerce* memiliki berbagai varian serta beragam jenis permasalahan didalamnya. Untuk memastikan *e-commerce* ini dapat bertumbuh, bertahan, serta memiliki kepercayaan dari pihak konsumer, diperlukan adanya pemetaan tentang berbagai masalah yang kini dihadapi dalam penggunaan *e-commerce*. Peneliti menggunakan pendekatan studi literatur dari berbagai jurnal dalam jangka waktu enam tahun terakhir, yaitu 2012-2017 untuk memetakan dan mengkategorikan berbagai permasalahan *security e-commerce*. Pemetaan ini diharapkan memberikan ruang kepada peneliti yang bergerak dalam bidang internet dan *e-commerce* untuk mengembangkan berbagai pendekatan ataupun menyelesaikan berbagai permasalah yang dihadapi tentang *e-commerce*.

***Kata kunci** : e-commerce security, e-commerce, internet, security, literature review*

ABSTRACT

Various technology developments has made e-commerce withmany variants as well as a variety of problems in it. To ensure that e-commerce can grow, survive, and has the trust of the consumer, required the mapping of the problems now faced in the use of e-commerce. Researchers used the approach literature from various journals in the last six-year period, namely 2013-2017 to map and categorize the various problems of security of e-commerce. This mapping is expected to provide space for researchers engaged in the field of internet and e-commerce to develop approaches or solve problems encountered on e-commerce.

***Keywords**: e-commerce security, e-commerce, internet, security, literature review*

PENDAHULUAN

Dengan perkembangan internet, kini masyarakat dunia dibawa ke level baru dalam globalisasi ekonomi, perekonomian negara bergerak ke arah internet menjadi perdagangan secara elektronik (e-commerce). *e-Commerce* didefinisikan sebagai proses pembelian dan penjualan yang dilakukan melalui internet. Berbagai perkembangan teknologi membuat e-commerce memiliki berbagai varian seperti transfer dana secara elektronik, supply chain management, internet marketing, online transaction processing, EDI (*electronik data interchange*) dan masih banyak lagi. Dengan kata lain, e-commerce saat ini mendeskripsikan transaksi bisnis, pelayanan kostumer, pembelian, pengantaran (*delivery*) dan pembayaran dengan menggunakan publik internet dan jaringan digital komputer yang menghubungkan organisasi dan individu dalam bisnis, industri bahkan pemerintahan.

Internet memberikan alternatif untuk menghubungkan berbagai pihak dalam bisnis dengan biaya yang rendah dan akses tak terbatas. Kombinasi dari teknologi berbiaya rendah dan akses yang luas ini memberikan transformasi yang radikal bagaimana cara masyarakat saat ini berbisnis. Transformasi ini datang dengan berbagai benefit namun memberikan isu keamanan baru serta berbagai tantangan didalamnya. Akibatnya, masyarakat didorong untuk memberikan perhatian yang signifikan dalam keamanan e-commerce seperti sistem dan data pribadi konstumer untuk memastikan adanya privasi dan keamanan. Sampai saat ini regulasi yang

dibuat oleh negara-negara belum dapat melingkupi berbagai tindakan kriminal yang dilakukan dalam dunia maya.

Hal ini menjadikan dunia internet dapat menjadi medium baru tindakan kriminal yang belum dapat tersentuh oleh hukum. Untuk memastikan e-commerce ini dapat bertumbuh, bertahan, serta memiliki kepercayaan dari pihak konsumer, diperlukan adanya pemetaan tentang berbagai masalah yang kini dihadapi dalam penggunaan e-commerce. Pemetaan ini memberikan ruang kepada peneliti yang bergerak dalam bidang internet dan e-commerce untuk mengembangkan berbagai pendekatan ataupun menyelesaikan berbagai permasalah yang dihadapi tentang e-commerce.

Mengingat luasnya permasalahan e-commerce, dalam paper ini peneliti akan memetakan berbagai masalah yang sedang berkembang dalam berbagai jurnal dalam kurun waktu publikasi 5 tahun, yaitu dari tahun 2012 sampai dengan 2016 menggunakan studi literatur.

METODE

Penulis menggunakan pendekatan studi literatur menggunakan sumber dari berbagai jurnal sistem informasi yang fokus membahas tentang permasalahan-permasalahan tentang masalah keamanan e-commerce selama enam tahun terakhir, dari tahun 2012 sampai dengan 2017.

Pertaman-tama jurnal penelitian dalam bidang e-commerce dikumpulkan dari berbagai sumber website jurnal online, seperti IEEE, google.scholar, elsevier Science Direct, serta Emerald. kemudian setiap jurnal dipilah lagi dengan pembahasan security e-commerce. Setiap jurnal dilakukan pengecekan ganda agar tidak membahas permasalahan sayang sama dalam topik security e-commerce pada tahun yang sama.

Untuk pengkategorian, peneliti menggunakan kategori dari penelitian sebelumnya yang telah diolah dan disesuaikan dengan temuan permasalahan yang ditelaah oleh peneliti. Untuk mendapatkan gambaran yang menyeluruh, peneliti menggunakan daftar tabel sesuai dengan permasalahan yang di kumpulkan dari berbagai jurnal yang ada untuk mendeteksi dan mengkategorikan setiap permasalahan.

HASIL

E-commerce dapat didefinisikan sebagai transaksi bisnis, layanan pelanggan, dan intra-bisnis tugas yang memanfaatkan komunikasi digital. *e-commerce* secara luas, adalah: “Penggunaan jaringan elektronik untuk bertukar informasi, produk, jasa dan pembayaran untuk tujuan komersial dan komunikasi antara individu (konsumen) dan bisnis, antara individu itu sendiri, dalam pemerintah atau antara masyarakat dan pemerintah dan antara busoness dan pemerintah” [1]. Infrastruktur penting untuk e-commerce adalah lingkungan komputasi jaringan digital yang menghubungkan organisasi dan individu dalam bisnis, industri, pemerintah, dan rumah.

Berbagai penelitian terdahulu mengenai e-commerce security dengan metode studi pustaka telah dilakukan oleh beberapa peneliti yang berfokus dalam pengembangan e-commerce. Penelitian tentang permasalahan dalam e-commerce di bidang m-commerce [2], e-commerce security spesifik membahas malware [3]. Penelitian ini lebih menitik beratkan kepada kilasan tentang berbagai penelitian-penelitian yang membahas tentang berbagai permasalahan dalam bidang security e-commerce. Setelah berbagai penelitian dengan selang waktu yang ditentukan dikumpulkan, maka peneliti mengkaji dan mengkategorikannya.

Terdapat tiga komponen dalam e-commerce yang digunakan dalam klasifikasi permasalahan dalam jurnal ini [4].

A. *Client Level*

Banyak pelanggan menggunakan koneksi internet nirkabel dan perangkat mobile untuk mengakses sistem e-bisnis. jaringan nirkabel dan perangkat mobile menimbulkan bahaya keamanan, karena pengguna di luar bisa menguping komunikasi nirkabel. Mengamankan jaringan nirkabel dengan password dapat membuat lebih sulit bagi pengguna di luar untuk terhubung ke jaringan dan mengakses informasi sensitif, tetapi koneksi nirkabel tidak aman seperti sambungan kabel, bahkan

jika memiliki proteksi password [5]. Selain ini, perangkat mobile dapat menjadi perhatian keamanan karena mereka mudah untuk salah tempat. Beberapa isu keamanan terkenal terkait dengan jaringan nirkabel dan perangkat mobile yang mempengaruhi e-bisnis terdaftar dan dibahas di bawah.

Captured & Retransmitted Messages. Penyerang dapat mencegat sesi dan mengubah pesan yang dikirimkan sesi. mungkin skenario lain oleh penyerang adalah untuk mencegat sesi dengan memasukkan tuan berbahaya antara tuan rumah klien dan server host akhir untuk membentuk apa yang disebut man-in-the-middle. Dalam hal ini semua komunikasi dan transmisi data akan melalui host penyerang.

Eaves fropping. Ini adalah masalah keamanan terkenal dalam jaringan nirkabel. Jika jaringan tidak aman dan informasi yang dikirimkan tidak dienkripsi kemudian penyerang bisa meretas jaringan dan mengakses data sensitif.

Mobile Device Pull Attacks. Penyerang mengontrol perangkat mobile sebagai sumber data properti dan kontrol informasi. Data dapat diperoleh dari perangkat itu sendiri melalui antarmuka data ekspor, sinkronisasi desktop, aplikasi mobile yang berjalan pada perangkat, atau server intranet.

Mobile Devices Push Attacks. Penyerang menggunakan perangkat mobile untuk menanam kode berbahaya dan menyebar ke menginfeksi unsur-unsur lain dari jaringan. Setelah perangkat mobile dalam jaringan yang aman terganggu, dapat digunakan untuk serangan terhadap perangkat lain atau server di jaringan.

Lost Device. Kemungkinan perangkat hilang atau dicuri dan disalahgunakan oleh pengguna yang tidak sah harus dipertimbangkan dengan menerapkan beberapa langkah-langkah keamanan seperti fitur perlindungan sandi pada setiap perangkat mobile.

B. *Front-End Servers & Software Application Level*

Lubang keamanan yang ada di sebagian besar sistem software baru dan yang sudah ada terutama karena bug software / kesalahan yang ditinggalkan oleh ceroboh atau nit sangat terampil programmer atau pengembang perangkat lunak keamanan yang berfokus. sistem perangkat lunak E-commerce harus interoperable dan harus bertukar data dengan perangkat lunak sistem yang dimiliki dan dikendalikan oleh orang lain seperti pelanggan, pemasok, mitra, dan agen pengolahan dan pemenuhan perangkat lunak lain atau server. Oleh karena itu, mekanisme keamanan dikerahkan dalam sistem e-commerce harus fleksibel, berbasis standar, dan interopable dengan sistem lain. mereka harus mendukung browser, dan bekerja di arsitektur multi-tier dengan satu atau lebih tingkatan menengah seperti server web dan server aplikasi. di atas ini, jaringan dan komunikasi standar dan protokol yang dalam keadaan perubahan terus menerus yang membuat tetap up-to-date dengan semua petunjuk keamanan dan patch keamanan tugas yang sulit. hacker terus menemukan dan memanfaatkan kerentanan ini. Selain itu, hacker dapat menggunakan virus dan software berbahaya lainnya untuk menginfeksi sistem e-bisnis dan dapat mencuri informasi pelanggan, menyebabkan hilangnya data, atau membuat sistem e-bisnis tidak dapat diakses.

C. *Network & Server Level*

Jaringan memiliki masalah keamanan mereka sendiri terutama karena fakta bahwa sebagian besar jaringan tergantung pada jaringan swasta lainnya, dimiliki dan dikelola oleh orang lain, dan pada infrastruktur bersama masyarakat di mana Anda memiliki kontrol lebih sedikit dari, dan pengetahuan tentang, langkah-langkah keamanan yang diterapkan. meskipun bantuan enkripsi untuk beberapa meluas dalam mengamankan informasi bergerak melalui jaringan, tugas operator jaringan untuk memastikan bahwa informasi tersebut aman diangkut ke tujuan akhir. Beberapa isu keamanan terkenal terkait dengan jaringan sebuah server yang mempengaruhi sistem e-commerce yang terdaftar dan dibahas di bawah.

Permasahahan yang masuk dalam kategori ini yaitu:

Distributed Denial of Service (DDOS). Salah satu masalah keamanan yang paling merepotkan menghadapi e-bisnis adalah ketika hacker meluncurkan serangan penolakan layanan. Dengan demikian serangan ditandai dengan attemp eksplisit oleh penyerang untuk mencegah pengguna menggunakan sistem e-bisnis. serangan DDOS yang umum di semua jenis jaringan di mana penyerang tidak memerlukan infrastruktur fisik, semua apa yang dia lakukan adalah banjir utama server e-bisnis dengan sejumlah besar permintaan tidak valid memperlambat atau crash dan membuatnya dapat diakses.

Session Interception & Messages Modification. Penyerang dapat mencegat sesi dan mengubah pesan yang dikirimkan sesi. mungkin skenario lain oleh penyerang adalah untuk mencegat sesi dengan memasukkan sejumlah berbahaya antara tuan rumah klien dan server host akhir untuk membentuk apa yang disebut man-in-the-middle. Dalam hal ini semua komunikasi dan transmisi data yang akan pergi melalui host penyerang.

Firewall Loophole. Firewall adalah perangkat lunak atau perangkat keras yang digunakan dalam sistem e-commerce untuk memisahkan komunikasi antara back-dan server dari jaringan perusahaan firewall wajib untuk situs bisnis. Namun, mereka biasanya diimplementasikan pada lapisan protokol jaringan dan tidak melindungi sistem dari serangan ditujukan pada protokol yang lebih tinggi seperti HTTP. Jika pengguna mengakses komponen melalui permintaan HTTP yang menyebabkan buffer overflow, layanan dapat crash dan memberikan akses pengguna ke server perusahaan back-end intranet menggunakan beberapa dikenal celah firewall tidak tetap dan mencoba untuk kembali ke daftar harga, katalog dan daftar email dan mengubah atau menghancurkan data, yang dapat mengganggu atau bahkan operasi bisnis menonaktifkan.

Dari landasan ini teori ini peneliti mengadopsinya dalam penelitian ini. Terdapat tujuh belas permasalahan yang ditemukan dalam jurnal yang telah dikumpulkan oleh peneliti. Permasalahan-permasalahan tersebut dikategorikan berdasarkan tiga komponen dalam e-commerce yang digunakan dalam klasifikasi permasalahan dalam jurnal ini [4]:

Tabel 1. Pengkategorian Permasalahan Security e-commerce

Kategori	Permasalahan
Client Level	Lost Device (LD)
	Trojan Horse (TH)
	Spamming & Viruses (SV)
	Worm (WR)
	Phishing (PS)
	User Authentification (UA)
Front-End Servers and Software application Level	Identity Theft (IT) Digital Signature (DS)
	Electronic Payment (EP)
Network & Server Level	SQL Injection (SI)
	Privacy Data (PD)
	Debugging Information (DI)
	Scripting errors & code (SE)
	Electronic Protocol (ER)
	Fraud (FR)
	Unauthorized Access (NA)
	Email Bombing (EB)

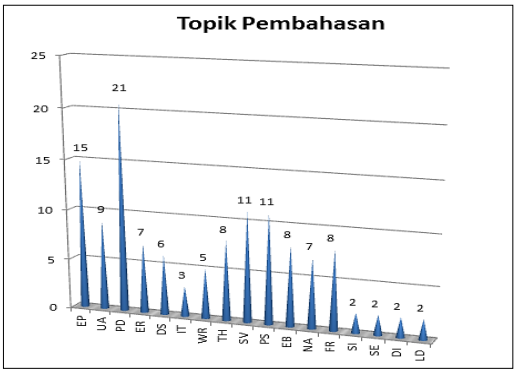
Penelitian	Permasalan e-commerce Security																
	EP	UA	PD	ER	DS	IT	WR	TH	SV	PS	EB	NA	FR	SI	SE	DI	LD
Oliveira et al, 2017 [6]		v	v	v													
Mollah et al, 2017 [7]			v														
Hillman & Neustaedler, 2017 [8]	v																
Khalilzadeh et al, 2017 [9]	v																
Coshin, 2017 [10]			v														
Aljukhadar & Senecal, 2016 [11]			v														
Yang, 2016 [12]	v																
Tan et al, 2016 [13]													v				
Alyoubi, 2015 [14]				v													
Nilashi et al, 2015 [15]				v													
Yapar et al, 2015 [16]				v													
Chan et al, 2014 [17]						v	v	v	v	v	v						
Zhang et al, 2013 [18]													v				
Hartono et al, 2014 [19]	v																
Junhu et al, 2012 [20]			v														
Zhang et al, 2012 [21]	v	v	v	v	v												
Mik, 2012 [22]					v	v											
Chou, 2016 [23]			v														
Meskaran et al, 2013 [24]	v																
Nepomuceno et al, 2014 [25]	v		v														
Niranjanamurthy, 2013 [26]		v			v		v	v	v		v	v	v				
King & Denis, 2013 [27]							v	v	v								
Treesintorus, 2012 [28]			v														
Wipawayangkool, 2015 [29]			v				v	v	v	v							
Chandratre, 2014 [30]	v											v					
Niranjamurthy, et al 2013 [31]		v											v				
Singh, 2016 [32]			v						v					V	v	v	
Ladan, 2014 [4]	v	v	v						v	v	v						v

Chatterje, 2015 [34]	v																
Sahinoglu et al, 2012 [35]		v	v														
Ahmad & Alam, 2016 [36]	v	v	v	v	v	v	v	v	v	v	v	v	v	V	v	v	v
Haufe et al, 2016 [37]			v														
Busalim & Hussin, 2016 [38]			v														
Grschow et al, 2016 [39]	v																
Mavlanova et al, 2016 [40]	v				v												
Li et al, 2017 [41]			v														
Chen et al, 2017 [42]			v						v	v	v	v					
Chang et al, 2017 [43]			v														
Morenofernndez et al, 2017 [44]										v							
James et al, 2017 [45]			v														
Kurnia & Mahbubur, 2015 [46]	v			v													
Arpaci et al, 2015 [47]			v														
Junadi & Sfenrianto, 2015 [48]	v																
Aldosari, 2015 [49]					v												
Fryer et al, 2015 [50]								v	v	v	v	v	v				
Jurcut et al, 2014 [51]		v						v	v	v	v	v	v				
Webb et al, 2014 [52]		v															
Baskerville, 2014 [53]								v	v	v	v	v	v				
Ramesh et al, 2014 [54]										v							
Gowtham & Krishnamurti, 2014 [55]										v							

Tabel 2.Pengkategorian dari setiap jurnal yang diambil dan diolah oleh Peneliti

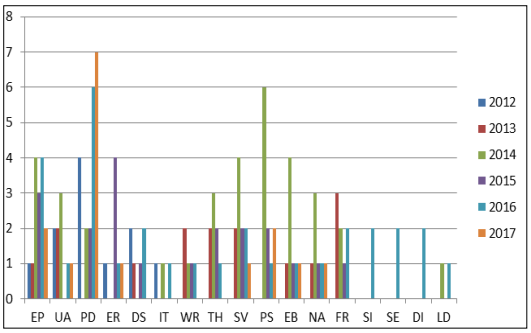
Dari hasil kategori diatas, ditemukaan bahwa dari jurnal tahun 2012 sampai dengan 2017 terdapat 5 isu besar yang dibahas dalam jurnal yang ada, yaitu dari kategori Network & Server Level yaitu Privacy Data (PD), Electronic Payment (EP) diikuti oleh Client Level yaitu Spamming & Viruses (SV), Phishing (PS) serta User Authentification (US).

Grafik 1. Tingkat Isu *security e-commerce*



berdasarkan topik pembahasannya

Terdapat 5 permasalahan dalam Isu E-commerce yang paling sedikit dibahas dalam 5 tahun belakangan ini yaitu SQL Injection (SI), Scripting errors & core (SE), Debugging Information (DI) dari Network & Server Level, Lost Device (LD) dari Client Level, serta Identity Theft (IT) dari Front End Server & Software Application.



Grafik 2. Tingkat Isu *security e-commerce* berdasarkan tahun penelitiannya

Pada tahun 2012 Isu paling banyak yang dibahas adalah tentang Privacy Data (PD). Di tahun 2013 yaitu isu tentang Fraud (FR). Memasuki tahun 2014 Email Bombing (EB) mejadi pembahasan terbanyak yang dibahas oleh kalangan peneliti. Sedangkan di tahun 2015 Electronic Protocol (EP), tahun 2016 dan 2017 Privacy Data (PD) kembali menjadi masalah yang banyak dibahas oleh peneliti dalam bidang e-commerce.

Dari grafik diatas ditemukan bahwa Kategori tertinggi dan terendah terdapat dalam satu kategori yang sama, yaitu Network & Server Level. Kategori ini menjadi bagian yang banyak dikaji oleh lebih dari lima puluh peneliti dalam lima tahun ini dikarenakan menjadi bagian yang begitu sering diserang dan bermasalah dibandingkan dengan kategori lainnya [4]. Selain itu *Network & Server Level* merupakan gerbang untuk mendapatkan data dari tiap pelanggan ataupun data yang disimpan oleh perusahaan [9]. Bahkan, dapat berkomunikasi server lain untuk mendapatkan akses dari berbagai database sehingga dipandang sebagai mission-critical business processes [12]. Oleh karena begitu pentingnya level ini sehingga berbagai peneliti di bidang e-commerce dan internet berusaha untuk meneliti berbagai permasalahan untuk menemukan inovasi ataupun pendekatan baru dalam membangun *Network & Server Level* yang lebih kuat untuk menghadapi serangan dari para peretas.

Privacy Data (PD) menjadi topik tertinggi yang dibahas dalam penelitian-penelitian pada tahun 2016 dan 2017. PD adalah salah satu tantangan utama dimana data rahasia pengguna ponsel atau aplikasi diproses dan bergeser dari perangkat mobile ke server untuk didistribusikan. Server ini terletak di tempat yang berbeda yang dimiliki dan dikelola oleh penyedia layanan saja. Di sini, pengguna tidak dapat secara fisik menjadi penilai penyimpanan data mereka dan dengan demikian, data pribadi dan tantangan perlindungan terkait berada di tangan penyedia layanan, dan pengguna tidak bertanggung jawab untuk privasi hilang [7]. Pemberdayaaan dalam PD juga terus meningkat dalam organisasi ataupun perusahaan online yang berusaha mengumpulkan sejumlah besar data konsumen, yang memungkinkan kemajuan dalam teknologi penyimpanan, jaringan, dan pengolahan data Informasi yang efisien dan efektif dalam rangkan pengambilan keputusan strategis. Organisasi semakin memanfaatkan artefak teknologi untuk mengumpulkan, menganalisis, dan berbagi

pribadi informasi, sedangkan konsumen telah menjadi semakin khawatir tentang privasi mereka informasi secara online. Memang, masalah privasi yang sangat penting tidak hanya untuk konsumen tetapi juga untuk perusahaan online karena pada akhirnya kedua belah pihak akan menghadapi perangkap bencana jika keadaan privasi tidak dapat diselesaikan dengan baik [41].

Phising (PS) dalam kategori client Level menjadi tertinggi kedua dalam penelitian 5 tahun belakangan ini. PS menjadi hal serangan populer walau tidak setinggi PS. PS menggunakan situs web yang disusupi di beberapa 90% kasus, dan situs media sosial menjadi semakin populer dengan peretas karena sebagian dari tingkat konversi yang lebih tinggi. Penelitian telah menunjukkan bahwa beberapa 8% dari semua URL di Twitter adalah spam dari beberapa deskripsi. Facebook juga ditargetkan melalui clickjacking, di mana "seperti" tombol atau serupa tersembunyi pada (spam) Halaman orang kunjungan yang membujuk teman-teman korban untuk mengunjungi halaman juga [50]. SI (SQL Injection), SE (Scripting error & Code) dan DI (Debugging Information) menjadi pembahasan yang tidak begitu diminati untuk diteliti oleh peneliti.

SIMPULAN

Perkembangan e-commerce yang dinamis memberikan berbagai permasalahan didalamnya. Terdapat beberapa hal penting yang ditemukan dalam penelitian ini:

1. Permasalahan tentang *Network & Server Level* secara spesifik yang berkaitan dengan *Privacy Data* (PD) masih merupakan Isu yang paling sering dibahas dalam topic e-commerce security. Terdapat 21 jurnal dari tahun 2012 sampai dengan 2017 yang membahas tentang hal tersebut.
2. SQL *Injection* (SI), *Scripting errors & core* (SE), *Debugging Information* (DI) dari kategori *Network & Server Level*, *Lost Device* (LD) dari *Client Level*, *serta Identity Theft* (IT) dari *Front End Server & Software Application*. Menjadi 5 topik yang kurang begitu banyak dibahas dalam 5 tahun belakangan ini.

DAFTAR PUSTAKA

[1] Spiegel, "Security Leaks Found at Dozens E-commerce Sites". E-commerce Times, January 17, 2000.

[2] [26] Niranjanamurthy et al, "The Study of E-commerce Security Issues and Solutions", International Journal of Advanced Research in Computer and Communication Engineering. 2(7), 2013.

[3] [29] Wipawayangkool & Villafranca, "Exploring Millennials' Malware Awareness and Intention to Comply with Information Security Policy," Review of Integrative Business & Economics Reserch. 4(3), 2015.

[4] Ladan, "E-commerce Security Issues". International Conference of Future Internet of Things and Cloud, 2014.

[5] Pham et al, "Commitment Issues In Delegation Process". Proceeding of the Sixth Australasian Conference on Information Security 2008 Wollonglong, Australia, 2008.

[6] Oliveira et al, "Modelling and Testing Consumer Trust Dimensions in E-commerce." Journal of Computers In Human Behavior, 2017.

[7] Mollah et al, "Security and Privacy Challenges in Mobile Cloud Computing: Survey and Way Ahead", Journal of Network and Computer Applications, 2017.

[8] Hillman & Neustaedter, "Trust and Mobile Commerce in North Amerca", Journal of Computers in Human Behavior, 2017.

[9] Khalilzadeh et al, "Security-Related Factors in Extended UTAUT model for NFC Based Mobile Payment In The Restaurant Industry", Journal of Computers in Human Behavior, 2017.

[10] Choshin & Ghaffari, "An Investigation Of The Impact of Effecctive Factors On The Succes Of E-commerce In Small-And Mendium-Sized Companies",

Journal of Computers in Human Behavior. 66, 67-74, 2017.

[11] Aljukhadar & Senecal, "The User Multifaced Expertise: Divergent Effects of the Website Versus E-commerce Expertise", International Journal of Information Management. 36, 322-332, 2016.

[12] Yangs et al, Scale, "Congestion, Efficiency and Effectiveness in E-commerce Firms", Journal of Electronic Commerce Research and Application, 2016.

[13] Tan et al, "Developing Business Analytic Capabilities for Combating E-commerce Identity Fraud: A Study of Trustev's Digital Verivication Solution", Journal of Information and Management, 2016.

[14] Alyoubi, "E-commerce in Developing Countriees and How to Develop Them During the Introduction of Modern Systems", Procedia Computer science. 65, 479-483, 2015.

[15] Nilashi et al, "The Role of Security, Design and Content Factors on Costumer Trust in Mobile Commerce", Journal of Retailing and Consumer Services. 26, 57-69, 2015.

[16] Yapar et al, "The Role of Taxation Problems on the Development of E-commerce", Procedia – Social and Behavioral Sciences. 195, 642-648, 2015.

[17] Chan et al, "Defending Against XML-Related Attacks In E-commerce Applications With Predictive Fuzzy Associative Rules", Journal of Applied Sift Computing. 24, 142-157, 2014.

[18] Zhang et al, "Trust Fraud: A Crucial Challenge for China's E-commerce Market", Journal of Electronic Commerce Research and Appications. 12, 299-308, 2013.

[19] Hartono et al, "Measuring Perceived Security in B2C Electronic Commerce Website Usage: A Respectification and Validation", Journal of Decision Support Systems, 2014.

[20] Junhu et al, "The Deficiency of E-cmmerce Contract and Some Propose to Perfect. Energy Procedia. 16, 633-638, 2012.

[21] Zhang et al, "Assessment of E-Commerce Securing Using AHP and Evidential Reasoning", Journal of Expert Systems with Applications. 39, 3611-3623, 2012.

[22] Mik Eliza, "Mistaken Identity, Identity Theft and Problems of Remote Autthentication in E-commerce", Journal of Computer Law & Security Review. 28, 396-402, 2012.

[23] Chou & Chao-Hsiu, "Beyond Identifying Privacy Issues in E-learning Setting – Implications for Instructional Designers", Journal of Computers & Education, 2016.

[24] Meskaran et al, "Online Purschase Intention: Effects of Trust and Security Perception", Australian Journal of Basic and Applied Sciences. 7(6), 307-315, 2013.

[25] Nepomuceno et al, "How to Reduce Perceived Risk When Buying Online: The Interactions Between Intangibility, product Knowledge, Brand Familiarity, Privacy and Security Concerns", Journal of Retailing and Consumer Services, 2013.

[27] King & Dennis, "Introduction to Internet and the Digital Economy", 46th Hawaii International Conference on System Sciences, 2013.

[28] Treesinthuros, "E-commerce Transaction Security Model Based on Cloud Computing", Proceedings Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on, 2012.

[30] Chandrate, "Security Issues Related to Web Services in E-commerce", International Conference on Advances in Communication and Computing Technologies, 2014.

[31] Niranjanamurthy et al, "Analysis of E-commerce and M-commerce: Advantages, Limitations and Security Issues", International Journal of

Advanced Research in Computer and Communication Engineering. 2(6), 2013.

[32] Singh, "A Survey of Threats to E-commerce Applications", Research Journal Science and Technology. 8(3), 2016.

[34] Chatterjee, "Security and Privvacy Issues in E-commerce: A Proposed Guidelines to Mitigate the Risk". Advance Computing Conference (IACC), 2015 IEEE International, 2015.

[35] Sahinoglu et al, "Can We Assess and Monitor Privacy and Security Risk for Social Networks?", Procedia – Social and Behavioral Science. 57, 163-169, 2012.

[36] Ahmad & Alam, " E-Commerce Security Through Elliptic Curve Cryptography", Procedia Computer Science. 78, 867-873, 2016.

[37] Haufe et al, "Security Management Standards: A Mapping", Procedia Computer Science. 100, 755-761, 2016.

[38] Busalim & Hussin, "Understanding Social Commerce: A Systematic Literature Review and Directions for Further Research", International Journal of Information Management. 36, 1075-1088, 2016.

[39] Grüschow et al, "How To Different Payment Methods Deliver Cost and Credit Efficiency in Electronic Commerce?", Journal Electronic Commerce Research and Applications, 2016.

[40] Mavlanova et al, "The Role of External and Internal Signals in E-commerce". Journal Decision Support Systems, 2016.

[41] Li et al, "Resolving The Privacy Paradox: Toward A Cognitive Apprisal and Emotion Approach to Online Privacy Behaviors", Journal Information & management, 2017.

[42] Chen et al, "Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors". Journal Computers In Human Behavior, 2017.

[43] Chang et al, "User Trust in Social Networking Services: A Comparison of Facebook and Linkedin", Journal Computers In Human Behavior, 2017.

[44] Moreno-Fernández et al, "Fishing for Phishers, Improving Internet Users' Sensitivity To Visual Deception Cues To Prevent Electronic Fraud", Journal Computers In Human Behavior, 2017.

[45] James et al, "Exposing Others' Information On Online Social Networks (OSNs): Perceived Shared Risk, Its Determinants, And Its Influence On OSN Privacy Control Use", Journal of Information & Management. 30, 2017.

[46] Kurnia, et al, "A Qualitative Study of Business-to-Business Electronic Commerce Adoption Within The Indonesia Grocery Industry: A Multi-Theory Perspective", Journal of Information & Management, 2015.

[47] Arpaci et al, "Effects of Security andd Privacy Cincerns on Educational Use of Cloud Services", Journal Computer In Human Behaviour. 45, 93-98, 2015.

[48] Junadi & Sfenrianto, "A model of Factors Influencing Consumer's Intention To Use E-Payment System in Indonesia", Journal Procedia Computer Science. 59, 214-220, 2015.

[49] Aldosari, "A Proposed Security Layer for The Internet of Things Communication Reference Model", Journal Procedia Computer Science. 65, 95-98, 2015.

[50]Fryer et al, "Malicious Web Pages: What If Hosting Providers Could Actually Do Something… ", Journal of Computer Law & Security Review. 31, 490-505, 2015.

[51] Jurcut et al, "Design Guidelines for Security Protocols To Prevent Replay & Parallel Session Attacks". Journal of Computers & Security. 45, 255-273, 2014.

[52] Webb et al, "A Situation Awareness Model for Information Security Risk Management", Journal of Computers & Security. 30, 1-15, 2014.

[53] Baskerville et al, "Incident-Centered Information Security: managing a Strategic Balance Between Prevention and Response", Journal of Information & Management. 51, 138-151, 2014.

[54] Ramesh et al, "An Efficacious Method for Detecting Phishing Webpages Through Target Domain Identification". Journal of Decision Support Systems. 61, 21-22, 2014.

[55] Gowtham & Krishnamurthi, "A Comprehensive and Efficacious Architecture for Detecting Phishing Webpages". Journal of Computer & Security. 40, 23-27, 2014.