BLOCKCHAIN UNTUK KEAMANAN TRANSAKSI ELEKTRONIK PERUSAHAAN FINANCIAL TECHNOLOGY (STUDI KASUS PADA PT XYZ)

Maria Dolorosa Kusuma Perdani[1)], Widyawan[2)], Paulus Insap Santosa[3)]

[1, 2 ,3)] Departemen Teknik Elektro dan Teknologi Informasi, Universitas Gadjah Mada Yogyakarta
Jl. Grafika No.2, Sinduadi, Mlati, Yogyakarta 55281
Email : maria.dolorosa.k@mail.ugm.ac.id[1)], widyawan@ugm.ac.id[2)], insap@ugm.ac.id[3)]

Abstrak

Jenis bisnis online yang mulai banyak tumbuh di Indonesia yaitu financial technology atau lebih dikenal dengan sebutan FinTech Indonesia. Tujuan bisnis ini adalah untuk membuat masyarakat lebih mudah mengakses produk-produk keuangan, mempermudah transaksi dan juga meningkatkan literasi keuangan. Keamanan TI menjadi tantangan paling besar yang dihadapi dalam menangani perusahaan FinTech. Tidak sedikit perusahaan teknologi yang ada di Indonesia berada dalam posisi rentan akan serangan kriminal siber karena rendahnya level keamanan. Bergerak di industri jasa teknologi keuangan, PT XYZ dituntut untuk dapat memastikan kehandalan, efisiensi dan keamanan dari transaksi online agar tidak merugikan konsumen, karenanya PT XYZ menerapkan prinsip-prinsip dasar dalam keamanan sistem, yaitu: confidentiality, integrity, dan availability. Untuk membangun produk finansial yang inovatif dan aman, PT XYZ menggunakan teknologi kriptografi dan protokol internet seperti blockchain. Blockchain merupakan buku besar digital yang terdistribusi secara publik dan dikelola oleh ribuan komputer di dunia dalam waktu bersamaan. Semua transaksi dan penyimpanan data terjamin keamanannya karena tereplikasi di seluruh jaringan blockchain.

Kata kunci: *Startup, Financial Technology, Keamanan Siber, Blockchain*

1. Pendahuluan

Beberapa tahun terakhir munculnya fenomena media sosial dari Facebook, Twitter, Linkedin, Path, dan media sosial lainnya menandakan kemunculan perusahaan *startup* dunia yang merambah hingga Indonesia. Potensi pasar *e-commerce* dan bisnis aplikasi digital yang luas kedepan, mengundang para calon wirausaha untuk berlomba-lomba mendirikan perusahaan pemula atau lebih dikenal dengan *startup*. *Startup* merujuk pada perusahaan yang belum lama beroperasi dan berada dalam fase pengembangan untuk menemukan pasar yang tepat. Namun pada kenyataannya, *startup* lebih condong ke perusahaan yang bergerak dengan memanfaatkan teknologi informasi dan internet karena biasanya beroperasi melalui website.

Perkembangan *startup* di Indonesia memang cukup pesat, sekarang ini setidaknya terdapat lebih dari 1500 *startup* lokal di Indonesia yang tentunya akan bertambah seiring dengan semakin naiknya jumlah pengguna internet di Indonesia. *Startup* yang tumbuh di Indonesia tidak selalu bergerak dibidang *e-commerce* (toko *online*), ada jenis bisnis *online* lain yang juga mulai banyak tumbuh di Indonesia yaitu *financial technology* atau lebih dikenal dengan sebutan FinTech Indonesia. Tujuan bisnis ini adalah untuk membuat masyarakat lebih mudah mengakses produk-produk keuangan, mempermudah transaksi dan juga meningkatkan literasi keuangan. FinTech Indonesia memiliki banyak jenis, antara lain *startup* pembayaran, peminjaman, perencanaan keuangan, investasi ritel, pembiayaan, remitansi, dan riset keuangan. Pada dasarnya, FinTech adalah 'pengganggu' akses pada status quo, inklusi, dan interaksi dengan pasar keuangan, pendorong pada perkembangan pasar dan sebuah kompetisi dengan memberikan kesempatan bagi konsumen untuk menikmati *customer experience* yang lebih baik. Kehadiran FinTech merupakan peluang untuk terus meningkatkan perkembangan sektor jasa keuangan termasuk mendorong program inklusi keuangan. Karenanya, FinTech harus mampu mengatasi tantangan untuk senantiasa dapat memastikan kehandalan, efisiensi dan keamanan dari transaksi *online* agar tidak merugikan konsumen.

Survei yang dilakukan oleh PwC menunjukkan bahwa keamanan TI menjadi tantangan paling besar yang dihadapi dalam menangani perusahaan FinTech [1]. Pakar keamanan internet Indonesia, Alfons Tanujaya, menyebutkan bahwa tidak sedikit perusahaan teknologi yang ada di Indonesia berada dalam posisi rentan akan serangan kriminal siber karena rendahnya level keamanan [2]. David Belson dari *Akamai Research*, juga menyampaikan bahwa meningkatnya aksi kejahatan internet di Indonesia hingga menempatkan Indonesia di posisi pertama sebagai negara target peretas lebih dikarenakan lemahnya sistem keamanan internet dan komputer di Indonesia [3].

Perkiraan kerugian yang disebabkan oleh kejahatan siber di Indonesia pada tahun 2013 telah mencapai USD 895billion yang artinya mencapai 1,2% dari total keseluruhan perkiraan kerugian akibat kejahatan siber secara global yang mencapai USD 71.620 billion [4]. Selama tahun 2016, tercatat sebanyak 1207 kasus kejahatan siber yang ditangani oleh Polda Metro Jaya [5]. Kasus terbaru terkait peretasan situs yang merugikan

hingga hampir Rp4,1 miliar dialami oleh PT Global Network yang mengelola situs Tiket.com. Dalam kasus ini, pelaku berhasil mencuri *username* dan *password* agen perjalanan Tiket.com untuk melakukan login terhadap *server* maskapai Citilink dengan tujuan mendapatkan kode pemesanan tiket pesawat Citilink untuk dijual. Layanan digital yang didukung dengan fasilitas perbankan dan keuangan memang menjadi incaran karena perputaran uang yang begitu cepat disana [2].

Hasil riset yang dilakukan oleh *Communication and Information System Security Research* (CISSReC) [6], menemukan bahwa adanya kecenderungan masyarakat Indonesia enggan untuk melakukan pengamanan siber. Kesadaran masyarakat akan pentingnya keamanan menjadi pangkal persoalan. Hal ini bisa dikarenakan masyarakat belum merasakan dampak langsung dari serangan siber maupun dorongan dari pemerintah yang harus lebih kuat lagi. Kejahatan di internet yang tidak terlihat dan terjadi begitu cepat menjadi ancaman yang tidak bisa dianggap enteng. Karenanya, faktor privasi dan keamanan ini menjadi aspek yang penting untuk diperhatikan mengingat implementasi bisnis berbasis elektronik akan terganggu jika terjadi masalah yang menyangkut *confidentiality*, *integrity*, dan *availibility*.

Presiden Joko Widodo telah menetapkan Peraturan Presiden No.74 Tahun 2017 tentang Peta Jalan Sistem Perdagangan Nasional Berbasis Elektronik (*Road Map e-Commerce*) Tahun 2017-2019 [7] yang mendukung industri berbasis elektronik agar dapat tumbuh dengan manfaat yang dapat menetap di Indonesia, dimana salah satu poin strategis yang disasar dalam peta jalan ini adalah keamanan siber (*cyber security*). Ini menjadi bukti komitmen pemerintah dalam mendorong perluasan dan peningkatan kegiatan ekonomi masyarakat di seluruh Indonesia secara efisien dan terkoneksi secara global. Namun tentu saja kebijakan ini juga harus didukung oleh kesadaran seluruh masyarakat akan pentingnya keamanan.

Rendahnya level keamanan internet di Indonesia menjadi tantangan bagi pelaku *startup* terlebih yang mendukung fasilitas perbankan dan keuangan seperti perusahaan-perusahaan FinTech. Dalam penelitian ini akan dianalisa secara kualitatif penerapan keamanan siber pada salah satu *startup* digital yang bergerak di bidang FinTech. Tujuannya adalah untuk mengetahui kehandalan keamanan siber yang diterapkan guna menciptakan kepercayaan pelanggan untuk bertransaksi keuangan. Terciptanya kepercayaan pelanggan terhadap keamanan internet untuk bertransaksi keuangan merupakan kunci bagi keberhasilan bisnis ini.

Tinjauan Pustaka

Keamanan siber merupakan kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen resiko, tindakan, pelatihan, jaminan dan teknologi yang saat digunakan untuk melindungi lingkungan siber dan organisasi serta aset pengguna [8]. Secara teoritis, keamanan siber harus memenuhi tiga poin penting [9]:

1. Tindakan untuk melindungi teknologi informasi – komputer, jaringan komputer, perangkat keras, termasuk perangkat lunak terkait dan data serta informasi yang dikandung dan dikomunikasikan - dari serangan, gangguan, atau ancaman lainnya.
2. Tingkat perlindungan yang dihasilkan dari penerapan tindakan perlindungan tersebut.
3. Bidang usaha profesional yang terkait.

Deris [10] menyatakan bahwa keamanan komputer yang juga dikenal sebagai keamanan siber atau keamanan TI merupakan keamanan informasi yang diterapkan pada komputer atau jaringan. Keamanan siber bertujuan untuk membantu pengguna untuk mencegah penipuan atau mendeteksi setiap percobaan penipuan dalam sistem informasi yang memiliki makna realitas. Park dan Kim [11] mendefiniskan keamanan dalam transaksi *online* sebagai kemampuan suatu toko *online* dalam mengendalikan dan memelihara keamanan transaksi data. Disampaikan oleh mereka bahwa keamanan berperan penting dalam pembentukan kepercayaan untuk mengurangi kekhawatiran konsumen tentang penyalahgunaan data pribadi dan data transaksi yang dapat rusak dengan mudah.

Sistem keamanan siber semakin dibutuhkan saat ini seiring dengan meningkatnya penggunaan internet di segala aspek kegiatan masyarakat. Keamanan siber lebih lanjut dimaknai sebagai suatu mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan terhadap:

a. *Confidentiality*, biasanya terkait dengan data yang diberikan ke pihak lain dengan tujuan tertentu. Layanan ini dimaksudkan agar pesan tidak bisa dibaca oleh pihak yang tidak berhak.
b. *Integrity*, merupakan suatu keutuhan yang berkenaan dengan konsistensi informasi yang terdapat pada data yang ada pada jaringan komputer. Dimana modifikasi atau penghancuran data mengakibatkan ketidaktahuan data yang dihasilkan oleh kode berbahya. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi adanya manipulasi pesan oleh pihak yang tidak berwenang, antara lain seperti adanya penyisipan, pemindahan, dan penggantian data lainnya ke dalam pesan yang sebenarnya. Sehingga untuk mendukung aspek ini sering digunakan metode enkripsi misalnya tanda tangan digital.
c. *Availability*, berkaitan dengan ketersediaan informasi ketika dibutuhkan. Sebuah *server* yang diserang sampai mati, akan mengakibatkan pengguna tidak bisa lagi mengakses informasi yang terkandung di dalamnya.

Menurut National Research Council, terdapat tiga kelas serangan yang ditujukan ke internet, yaitu [12]:

1. *Service disruption*; hilangnya layanan yang diakibatkan karena adanya penonaktifan jaringan melalui berbagai serangan seperti *denial of service* (DoS) dan penghancuran informasi.

2. *Theft of assets*; penyalahgunaan informasi penting dalam skala yang cukup besar dan memiliki dampak besar.
3. *Capture and control*; melibatkan penguasaan dunia maya dan menggunakan sebagai senjata.

Kelas-kelas serangan tersebut kemudian diklasifikasikan sebagai kejahatan siber dan telah dimodifikasi dalam berbagai modus. Untuk menangani dan mencegah kejahatan siber tersebut, keamanan siber berperan penting dalam menjamin seseorang untuk menggunakan internet dengan aman.

Keamanan dan privasi memainkan peran penting dalam menjamin dan menjaga pelaku dan konsumen bisnis *online* karena tingginya pergerakan di dunia pelayanan *online* [13][11][14][15][16][17]. Memastikan privasi informasi dan keamanan data pelanggan merupakan salah satu kekhawatiran konsumen paling umum dalam melakukan transaksi *online* [18][17]. Agarwal dan Wu [13] menyebutkan bahwa integritas dari suatu transaksi merupakan kriteria yang paling penting yang akan menentukan keberhasilan *e-commerce*, terutama di negara berkembang dimana konsumen tidak memiliki modal kepercayaan yang dibangun sebelumnya.

Park dan Kim [11], Novitasari [15], serta Ariani [16] menyampaikan bahwa keamanan berperan penting dalam pembentukan kepercayaan untuk mengurangi kekhawatiran konsumen tentang penyalahgunaan data pribadi dan data transaksi yang dapat rusak dengan mudah. Ketika suatu tahap keamanan diterima dan sesuai dengan ekspektasi konsumen, maka konsumen mungkin akan bersedia untuk membuka informasi personal mereka dan akan melakukan transaksi dengan rasa aman. Hasil penelitian Alharbi [17] juga menunjukkan pentingnya menjaga privasi informasi pelanggan dan memastikan keamanan data untuk melindungi dan meningkatkan reputasi perusahaan dan hubungan dengan pelanggan serta untuk meningkatkan kepercayaan pelanggan. Karenanya, untuk membangun hubungan jangka panjang dengan pelanggan, perusahaan harus menyadari pentingnya membangun dan menjaga kepercayaan pelanggan dengan menjaga informasi pribadi mereka.

2. Pembahasan

PT XYZ merupakan perusahaan *startup* digital yang bergerak dibidang FinTech dan didirikan oleh 3 orang *founder* dengan latar belakang pendidikan berbeda-beda. Berdiri di tahun 2015, *startup* ini memfokuskan pada usaha dompet digital untuk aset digital atau lebih dikenal dengan sebutan *cryptocurrency*. Keunggulan utama *crytocurrency* seperti Bitcoin, Ripple dan yang lainnya dibanding mata uang tradisional adalah kecepatan dan kemudahan pengiriman kemanapun di seluruh dunia, bahkan mata uang digital ini dapat menjadi alternatif kartu kredit untuk membeli barang secara *online*.

Startup ini sedang membangun suatu aplikasi sebagai *gateway* yang menjalankan *smart wallet* untuk menciptakan cara terbaik untuk melakukan *peer-to-peer payment*. Untuk membangun produk finansial yang inovatif, PT XYZ menggunakan teknologi kriptografi dan protokol internet seperti *blockchain*. *Blockchain* ini semacam buku besar terdistribusi yang aman yang menggunakan proses konsensus untuk menyelesaikan transaksi. Dengan teknologi ini, orang dimanapun dapat mempercayai satu dengan yang lainnya, dapat melakukan transaksi secara langsung, dan kepercayaan ini dijamin bukan oleh institusi besar tapi oleh kolaborasi melalui kriptografi dan kode cerdas.

Transaksi menggunakan teknologi *blockchain* bersifat *peer-to-peer*, dalam arti dimana sebuah data dapat dipindahkan dari satu pengguna ke pengguna lain tanpa bantuan pihak ketiga untuk memprosesnya. Keuntungan lain yang didapat dengan memanfaatkan teknologi *blockchain* ini adalah perusahaan tidak harus bergantung pada satu server karena seluruh transaksi akan tereplikasi ke seluruh jaringan sehingga terhindar dari berbagai bentuk penipuan karena adanya data yang dimodifikasi, server *down*, maupun adanya kejahatan peretasan akun pengguna.

Cara kerja teknologi yang muncul di tahun 2008 ini cukup sederhana, aset digital misalnya uang, biasanya tidak disimpan di satu lokasi pusat namun biasanya terdistribusi di dalam buku besar global yang menggunakan kriptografi tingkat tinggi. Ketika suatu transaksi terlaksana, maka data transaksi ini akan dikirim secara global ke jutaan komputer. Diluar, terdapat sekelompok orang yang disebut "*miners*" yang memiliki kekuatan komputerisasi yang besar, 10 hingga 100 kali lebih besar dari Google diseluruh dunia. Setiap 10 menit, sebuah *block* tercipta dan punya data seluruh transaksi dari 10 menit terakhir. *Miners* ini bekerja dan berusaha memecahkan berbagai masalah. Mereka saling bersaing, *miners* pertama yang menemukan solusi dan berhasil memvalidasi *block* akan mendapat hadiah dalam bentuk mata uang digital. *Block* tersebut terhubung dengan *block* sebelumnya dan *block* sebelumnya lagi untuk membuat rangkaian *block*.

Semua transaksi dan penyimpanan data terjamin keamanannya karena tereplikasi di seluruh jaringan *blockchain*. Semisal 1 *block* akan diretas, katakanlah membayar 2 orang dengan menggunakan uang yang sama, maka harus meretas *block* tersebut, *block* sebelumnya dan seluruh sejarah transaksi dalam rangkaian *block* tersebut dan bukan hanya pada 1 komputer tapi jutaan komputer secara bersamaan yang semuanya menggunakan metode enkripsi level tinggi. Teknologi ini sudah pasti aman daripada sistem komputer yang ada sekarang karena semua transaksi bersifat transparan dan bisa dicek oleh semua orang sehingga kredibilitasnnya terjamin.

Bergerak di industri jasa teknologi keuangan, PT XYZ dituntut untuk dapat memastikan kehandalan, efisiensi dan keamanan dari transaksi *online* agar tidak merugikan konsumen, karenanya PT XYZ menerapkan prinsip-prinsip dasar dalam keamanan sistem, yaitu:

1. *Confidentiality*
   Founder PT XYZ menganggap bahwa keamanan dan privasi pelanggan itu penting, namun pada dasarnya keamanan itu sendiri

bagai makan buah simalakama. Data dan informasi yang dikumpulkan oleh PT XYZ akan terjaga kerahasiaannya, tapi ketika sudah menyangkut masalah hukum, maka perusahaan pun akan tunduk pada hukum yang berlaku. Hal ini berkaca dari kasus yang menyandung perusahaan teknologi besar dari Amerika, ketika *smartphone* hasil produksinya digunakan oleh terduga teroris akan 'dibuka' untuk keperluan penyidikan, pihak perusahaan tidak bersedia untuk 'membuka' kode penguncinya. Hal ini tentu saja justru menghambat penyelesaian suatu kasus. Bagaimanapun, wajib hukumnya untuk menyampaikan data dan informasi apapun bila hal tersebut dapat mempengaruhi kepentingan masyarakat luas. Dijelaskan lebih lanjut, data dan informasi yang nantinya terkumpul menjadi sebuah *big data* memang akan ada kemungkinan menjadi sarana komoditi, namun komitmen PT XYZ tetap akan menjaga privasi data pelanggan yaitu dengan memilih data dan informasi tertentu saja yang akan dibagi misalnya data pola jelajah pelanggan saat menggunakan aplikasi.

2. *Integrity*
   Sebagai upaya pencegahan dari akses yang tidak sah, PT XYZ menerapkan sistem login menggunakan otentifikasi *username* dan *password* untuk masuk kedalam sistem. Tidak hanya itu, PT XYZ juga menerapkan metode enkripsi dalam proses transaksi dan kedepan akan memberlakukan *digital signature* sebagai tanda keabsahan suatu transaksi. Teknologi *blockchain* diadopsi sebagai teknologi untuk memastikan keamanan transaksi karena dapat menghindarkan dari berbagai bentuk penipuan yang disebabkan adanya data yang dimodifikasi atau peretasan akun pengguna.
3. *Availability*
   PT XYZ menjamin ketersediaan data dan informasi saat diakses oleh pelanggan. Prosedur yang digunakan untuk menjamin ketersediaan data dan informasi adalah dengan menggunakan multi server. Pada prinsipnya, teknologi *blockchain* muncul untuk merevolusi teknologi dengan sistem kerja yang lebih instan, transparan, dan efisien tanpa perlu bergantung pada server yang tersentralisasi. Namun untuk saat ini, guna meminimalisir terjadinya resiko ketika satu server *down* dan taat pada peraturan Pemerintah yang menghendaki bahwa server-server yang digunakan sebagai *data center* berlokasi di Indonesia, maka PT XYZ tetap menggunakan 2 server, 1 *cloud server* digunakan sebagai *server* operasional berlokasi di luar Indonesia dan 1 server cadangan sebagai *data center* berlokasi di Indonesia.

Prosedur-prosedur yang diterapkan oleh PT XYZ dalam menjamin keamanan data dan informasi memang sudah menerapkan teknologi keamanan sistem level tinggi dan hingga saat ini merasa belum perlu melakukan konsolidasi dengan vendor keamanan jaringan diluar tim TI yang dibentuk perusahaan. Hal ini juga dikarenakan biaya operasional yang akan semakin melambung apabila harus melakukan konsolidasi dengan pihak ketiga. PT XYZ masih mengandalkan kemampuan tim TI untuk dapat terus mengembangkan diri mempelajari teknologi-teknologi keamanan sistem terbaru.

Pemilihan teknologi *blockchain* untuk merekam data statis maupun data dinamis (transaksi) juga merupakan solusi dari tingginya biaya operasional yang dihabiskan untuk pengamanan data. Perusahaan yang memproses pembayaran secara terpusat bisa menghabiskan jutaan per tahun untuk perangkat keras, perangkat lunak, karyawan, penelitian maupun pengembangan untuk mengkomunikasikan kepada pelanggan bahwa data mereka aman dalam setiap transaksi. Semua kartu kredit mewajibkan pedagang *e-commerce* memenuhi standar keamanan data industri kartu pembayaran yang mencakup keamanan jaringan, pemantauan dan beberapa standar lain yang juga berbiaya mahal. Memproses pembayaran pada *blockchain* pada dasarnya dapat menghindari biaya-biaya semacam ini.

Kesadaran masyarakat akan pentingnya keamanan serta dampak kejahatan siber menjadi perhatian pemerintah. Peningkatan literasi keamanan dalam transaksi *online* menjadi salah satu program dalam implementasi peta jalan *e-commerce*. PT XYZ sudah menerapkan kebijakan privasi sebagai bentuk perjanjian/kesepakatan penerapan prosedur keamanan dengan pelanggannya, namun PT XYZ tidak secara khusus memberikan edukasi kepada pelanggannya agar memahami pentingnya prosedur keamanan. Hal ini dikarenakan sasaran pelanggan PT XYZ adalah generasi milenial yang memang sudah menyadari pentingnya keamanan dalam bertransaksi di internet.

3. Kesimpulan

Memastikan keamanan data dan informasi pelanggan untuk melindungi dan meningkatkan reputasi perusahaan serta hubungannya dengan pelanggan dapat menciptakan kepercayaan pelanggan. Pemilihan teknologi yang efisien dan aman untuk bertransaksi keuangan menjadi tuntutan bagi perusahaan yang bergerak di bidang jasa teknologi keuangan. Teknologi *blockchain* dibangun untuk memecahkan masalah pembelanjaan ganda dan memverifikasi transaksi tanpa otoritas server pusat. Teknologi ini mampu mencegah adanya perubahan atau pemalsuan transaksi sehingga pengguna dapat melakukan perdagangan langsung satu sama lain secara aman. Sistem buku besar yang terdistribusi dan transparan ini, kiranya dapat juga menjadi solusi untuk bisa diterapkan pada pencatatan transaksi yang dilakukan oleh instansi pemerintah guna meminimalisir adanya upaya tindak korupsi.

Daftar Pustaka

[1] PWC, "83% dari Institusi Keuangan tradisional khawatir bisnis mereka akan direbut oleh FinTech," *www.pwc.com*, 2017. [Online]. Available: https://www.pwc.com/id/en/media-centre/press-release/2016/indonesian/83--dari-institusi-keuangan-tradisional--khawatir-bisnis-mereka-.html. [Accessed: 29-Dec-2017].

[2] A. Bintoro, "Ekonomi Digital Meningkat, Keamanan Siber Diperketat," *CNN Indonesia*, Jakarta, 09-May-2017.

[3] S. S. Alia, "Ketika Hacker Lebih Menakutkan Ketimbang Teroris – VIVA," *www.viva.co.id*, 2014.

[4] K. Andreasson, "Meeting the cyber security challenge in Indonesia An analysis of threats and responses," Jakarta, 2013.

[5] M. Amelia, "1207 Kejahatan Cyber Terjadi di Jakarta Selama 2016," *detikInet*, Jakarta, 31-Dec-2016.

[6] CISSReC, "HASIL SURVEY LEMBAGA RISET CISSReC 'Tingkat Kesadaran Masyarakat Tentang Keamanan Informasi.,'" Jakarta, 2017.

[7] "Peraturan Presiden No.74 Tahun 2017 tentang Peta Jalan Sistem Perdagangan Nasional Berbasis Elektronik (Road Map E-Commerce) Tahun 2017-2019." Jakarta, pp. 1–5, 2017.

[8] H. Ardiyanti, "Cyber-Security dan Tantangan Pengembangannya di Indonesia," *J. Polit.*, vol. V, no. 1, pp. 95–110, 2014.

[9] E. A. Fischer, "Creating a National Framework for Cybersecurity : An Analysis of," Washington, 2005.

[10] S. Deris, *Sistem Keamanan Komputer*. Jakarta: PT Elex Media, 2005.

[11] C.-H. Park and Y.-G. Kim, "The Effect of Information Satisfaction and Relational Benefit on ...," *J. Electron. Commer. Organ.*, vol. 4, no. 1, pp. 70–90, 2006.

[12] Maskun, A. Manuputty, S. M. Noor, and J. Sumardi, "CYBER SECURITY : RULE OF USE INTERNET SAFELY ?," *Procedia - Soc. Behav. Sci.*, vol. 103, pp. 255–261, 2013.

[13] J. Agarwal and T. Wu, "Factors Influencing Growth Potential of E-Commerce in Emerging Economies : An Institution-Based N-OLI Framework and Research Propositions," *Thunderbird Int. Bus. Rev.*, vol. 57, no. 3, pp. 197–215, 2015.

[14] M. M. Yenisey, A. A. Ozok, and G. Salvendy, "Perceived security determinants in e-commerce among Turkish university students," vol. 24, no. 4, pp. 259–274, 2005.

[15] S. Novitasari, "PERAN KEPERCAYAAN KONSUMEN PADA BISNIS ON LINE TERHADAP BELI ULANG PADA KONSUMEN DI MAGANDA," *J. Gema Ekon.*, vol. 5, no. 1, pp. 75–92, 2016.

[16] M. Ariani and Zulhawati, "Effect of Easy Transaction, Cosumer Interests, and Systems Security Level Measures Against Fraud Online Shopping in Lazada," vol. 10, no. 12, pp. 187–206, 2016.

[17] I. M. Alharbi, S. Zyngier, and C. Hodkinson, "Privacy by Design and Customers' Perceived Privacy and Security Concern in the Success of e-Commerce," *J. Enterp. Inf. Manag.*, vol. 26, no. 6, pp. 702–718, 2013.

[18] J. Godwin, "Privacy and Security Concerns as Major Barriers for e-Commerce : A Survey Study," *Inf. Manag. Comput. Secur.*, vol. 9, no. 4, pp. 165–174, 2001.

Biodata Penulis

Maria Dolorosa Kusuma Perdani, memperoleh gelar Sarjana Teknik (S.T), Jurusan Teknik Informatika Universitas Atma Jaya Yogyakarta, lulus tahun 2007. Sedang menempuh Magister Engineering (M.Eng) Program Pasca Sarjana *Chief Information Officer* Magister Teknik Elektro Universitas Gajah Mada Yogyakarta. Saat ini menjadi Peneliti di BPSDMP Kominfo Yogyakarta Kementerian Komunikasi dan Informatika.

Widyawan, memperoleh gelar Sarjana Teknik (S.T), Jurusan Teknik Informatika Universitas Gadjah Mada Yogyakarta, lulus tahun 1999. Memperoleh gelar *Magister of Science* (M.Sc.) dari *Erasmus University Rotterdam Netherlands*, tahun 2003 dan gelar *Doctor of Philosophy* (Ph.D.) dari *Cork Institute of Technology Ireland* tahun 2009. Saat ini menjadi Dosen di Universitas Gajah Mada Yogyakarta.

Paulus Insap Santosa, memperoleh gelar Insinyur (Ir), Jurusan Teknologi Sistem Komputer, lulus tahun 1984. Memperoleh gelar *Magister of Science* (M.Sc.) dari *University of Colorado*, lulus tahun 1991 dan gelar *Doctor of Philosophy* (Ph.D.) dari *National University of Singapore*, lulus tahun 2006. Saat ini menjadi Dosen di Universitas Gajah Mada Yogyakarta.

ISSN : 2302-3805