e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 9 No 5 Tahun 2022 Hal. : 1786-1794

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

available online http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

ANALISIS MANAJEMEN RESIKO OPERASIONAL PENGGUNA APLIKASI E-WALLET "DANA"DENGAN IMPLEMENTASI PCI DSS

Nidya Rofi

Fakultas Ekonomi dan Bisnis, Perbanas Institute

Abstrak

Penyedia layanan e-wallet yang menggunakan teknologi untuk penyediaan layanan keuangan perlu memastikan keamanan dan privasi informasi, sistem, dan jaringan. Penelitian ini berfokus pada penilaian kerentanan yang terkait dengan transaksi e-wallet dan melakukan manajemen risiko eksternal penggunaan aplikasi e-wallet "DANA" dan untuk melihat bagaimana implementasi PCI DSS oleh DANA bisa meningkatkan keamanan penggunanya. Penelitian ini merupakan sebuah penelitian deskriptif dengan pendekatan kualitatif. Adapun manfaat praktis dari penelitian ini adalah agar masyarakat semakin memahami tentang aplikasi- aplikasi pembayaran digital beserta resiko-resiko yang mungkin dialami penggunanya. Diharapkan dari penelitian ini masyarakat khususnya pengguna aplikasi pembayaran digital "DANA" ataupun pengguna aplikasi pembayaran digital lainnya lebih berhati-hati dalam penggunaannya, dalam menjaga keamanan PIN agar tidak terjadi penyalahgunaan oleh pihak-pihak yang tidak berkepentingan. Aspek kebaruan dari penelitian ini adalah penelitian ini secara khusus membahas tentang manajemen resiko operasional pada penggunaan aplikasi pembayaran digital e wallet "DANA" dan menjelaskan bagaimana penerapan standar keamanan nasional dapat melindungi para pengguna e-wallet DANA. Setelah melakukan penelusuran referensi-referensi belum ditemukan adanya penelitian yang membahas tujuan yang sama.

Kata Kunci: Manajemen Resiko, Security Standard, Aplikasi e-Wallet, DANA.

*Correspondence Address : nidyarofi@gmail.com
DOI : 10.31604/jips.v9i5.2022.1786-1794

PENDAHULUAN

Pada tahun 1990, munculnya perdagangan elektronik (e-commerce) memperkenalkan cara unik dalam melakukan bisnis perdagangan kepada konsumen dan dunia bisnis. Sejak itu, e-commerce telah tumbuh dan berubah secara luar biasa dengan menghasilkan manfaat luar biasa bagi pelanggan dan bisnis di seluruh dunia. Dengan sejumlah besar organisasi melakukan bisnis dengan cara ini, telah menjadi jelas bahwa bidang e-commerce memiliki masa depan yang menjanjikan di masa depan dan bisnis akan mendapatkan manfaat maksimal darinya (Abrazhevich, 2004).

Sebagian besar popularitas yang diperoleh oleh e-commerce adalah karena perspektif online dalam melakukan bisnis. E-commerce memungkinkan pembelian dan penjualan barang secara online, penyediaan berbagai layanan dan informasi di internet dan pertukaran uang instan antara pihak-pihak yang bertransaksi. Menggunakan e-commerce, pembayaran bisnis telah mengambil bentuk pertukaran uang secara elektronik dan disebut sebagai pembayaran elektronik. Sistem pembayaran elektronik dianggap sebagai tulang punggung e- commerce dan salah satu aspek terpentingnya. Pembayaran elektronik atau digital dapat didefinisikan sebagai layanan pembayaran yang memanfaatkan teknologi informasi dan komunikasi termasuk kartu sirkuit terpadu (IC), kriptografi, dan jaringan telekomunikasi (Raja et. Al., 2008). Sistem pembayaran elektronik yang efisien mengurangi biaya perdagangan dan dianggap penting untuk berfungsinya pasar modal dan antar bank. Dengan kemajuan teknologi, sistem pembayaran elektronik telah mengambil banyak bentuk termasuk kartu kredit, kartu debit, sistem pembayaran dan cek elektronik, kartu pintar, dompet digital, metode pembayaran tanpa kontak dan pembayaran mobile, dan sebagainya.

Seperti kita ketahui bahwa keamanan adalah perhatian utama orang saat ini ketika menggunakan teknologi apa pun karena penggunaan setiap teknologi terkena penipuan, pencurian data, dan pencurian. Ini menjadi lebih berbahaya ketika data mengandung informasi keuangan yang signifikan (Raja et. Al., 2008). Dengan demikian, terlepas dari kenyataan bahwa e-commerce adalah bidang yang berkembang dengan meningkatnya penggunaan layanan pembayaran online, pengembangan lebih lanjut dan penggunaan luas di masa depan tergantung pada stabilitas keamanan dan otentikasi berbagai sistem pembayaran elektronik (Aigbe dan Akpojaro, 2014). Masa depan sistem pembayaran elektronik tertentu tergantung pada bagaimana ia mengatasi tantangan praktis dan analitis yang dihadapi oleh berbagai cara pembayaran online. Tantangan- tantangan ini mencakup masalah hukum dan peraturan (perlindungan pembeli dan penjual), kemampuan teknologi penyedia layanan pembayaran elektronik, hubungan komersial, dan pertimbangan keamanan seperti masalah verifikasi dan otentikasi (Paunov dan Vickery, 2006).

Studi sebelumnya menunjukkan bahwa metode pembayaran mobile memberi pelanggan mereka sejumlah keuntungan termasuk akses bebas lokasi (Laukkanen & Lauronen, 2005), berbagai kemungkinan pembelian, alternatif mudah untuk pembayaran tunai, dan kontak tepat waktu dengan sumber daya keuangan mereka. Keuntungan ini telah menarik konsumen untuk melakukan pembayaran melalui perangkat seluler.

Mempelajari berbagai sistem pembayaran elektronik, Koponen (2006) menjelaskan bahwa ada berbagai macam sistem pembayaran online yang telah dikembangkan dalam beberapa tahun terakhir dan sistem ini dapat

secara luas diklasifikasikan ke dalam sistem mata uang berbasis akun dan elektronik. Sistem berbasis akun memungkinkan pengguna untuk melakukan pembayaran melalui rekening bank pribadi mereka; sedangkan sistem lainnya memungkinkan pembayaran hanya jika konsumen memiliki jumlah mata uang elektronik yang memadai. Sistem ini menawarkan sejumlah metode pembayaran yang meliputi: (1)Kartu pembayaran elektronik (kartu debit, kredit, dan tagihan)(2) Dompet elektronik (e-wallet), (3)Kartu kredit virtual(4) Pembayaran seluler (5) Kartu loyalitas dan kartu pintar (6) Uang elektronik (tunai elektronik).

Keamanan sangat penting ketika melakukan bisnis baik itu online atau offline. Di dunia maya, informasi yang diperlukan adalah nomor kartu kredit, kode verifikasi, dan alamat penagihan untuk memverifikasi identitas pemegang kartu dan transaksi penipuan selalu ada. (Sahut, 2008). Oleh karena itu, sistem keamanan yang dirancang dengan baik dapat mengatasi masalah keamanan ini yang sangat penting untuk penerimaan pembayaran online. VISA misalnya, telah mengembangkan daftar "praktik terbaik" untuk digunakan oleh pedagang ketika melakukan transaksi yang menggunakan pembayaran online atau dengan kartu.

Penggunaan kartu pembayaran seperti kartu kredit, kartu debit, dan kartu prabayar, terus bertambah. Pelanggaran keamanan terkait kartu pembayaran telah menyebabkan kerugian miliaran dolar setiap tahun. Untuk mengimbangi tren ini, jaringan kartu pembayaran utama telah mendirikan Dewan Standar Keamanan Industri Kartu (PCI), yang telah merancang dan merilis Standar Keamanan Data PCI (DSS). Standar ini memandu penyedia layanan dan pedagang untuk menerapkan infrastruktur keamanan yang lebih kuat yang mengurangi risiko pelanggaran keamanan.(Liu, 2010)

Siau et al. (2004) telah mempertimbangkan kurangnya keamanan dan kepercayaan konsumen pada penyedia layanan sebagai penghalang utama untuk adopsi transaksi e-commerce. Konsumen membutuhkan kerahasiaan, otentikasi, integritas data, dan non-penolakan sebagai persyaratan utama untuk melakukan pembayaran yang aman melalui internet. Menurut Karp (2015), salah satu tantangan utama yang dihadapi oleh sistem pembayaran mobile adalah meningkatnya tingkat kejahatan dunia maya yang mengakibatkan pencurian data dan serangan dunia maya pada data keuangan. Selain itu, risiko keamanan yang disertai dengan pembayaran seluler dapat digolongkan sebagai muncul atau tradisional. Risiko yang muncul memerlukan penggunaan mode pembayaran ini dalam pendanaan teroris dan pencucian uang sementara risiko tradisional melibatkan pencurian data dan layanan, kehilangan pendapatan, basis pelanggan, dan reputasi merek

The Payment Card Industry Data Security Standard (PCI DSS) atau Standar keamanan PCI adalah persyaratan teknis dan operasional yang ditetapkan oleh Dewan Standar Keamanan Industri Kartu Pembayaran untuk melindungi data pemegang kartu. Standar ini secara global mengatur semua pedagang dan organisasi yang menyimpan, memproses atau mengirimkan data ini dengan persyaratan baru untuk pengembang perangkat lunak dan produsen aplikasi dan perangkat yang digunakan dalam transaksi tersebut. Kepatuhan terhadap standar PCI adalah wajib untuk masing-masing pemangku kepentingan.

Salah satu aplikasi online yang memerlukan perlindungan data adalah e-wallet. e-Wallet adalah instrumen pembayaran uang elekttronik. Merupakan sebuah mikroprosesor yang

ingatannya dikreditkan dengan daya beli yang disimpan dalam rekening user yang sebelumnya telah disimpan di perusahaan khusus (bank atau perusahaan penerbit uang elektronik). Rekening ini didebit pada setiap pembelian tanpa keterlibatan dari penerbit. E-wallet menawarkan banyak keuntungan diantaranya transaksi aman, disesuaikan untuk melakukan pembayaran mikro, mudah digunakan, universal (tidak ada tautan dengan rekening bank selama proses pembayaran), dan memiliki beragam penggunaan (Sahut, 2008).

METODE PENELITIAN

Pendekatan penelitian menggunakan pendekatan normatif, karena ada aturan-aturan dan ketentuan yagn berlaku dalam sistem manajemen resiko operasional pembayaran digital. Penelitian ini merupakan sebuah penelitian deskriptif dengan pendekatan kualitatif. Bogdan dan Taylor dalam Moloeng (2007:4) mendefinisikan penelitian kualitatif sebagai prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang diamati dari fenomena yang terjadi. Didalam penelitian ini penulis menggambarkan permasalahan dengan didasari data-dara yang ada lalu dianalisis lebih lanjut untuk diambil kesimpulannya. Data yang dikumpulkan dari penelitian ini berasal dari sumber data sekunder. Data sekunder yaitu berupa dokumen- dokumen atau literatur-literatur, internet, surat kabar, jurnal dan lain sebagainya. Pengumpulan data sekunder dilakukan dengan mengambil atau menggunakanya sebagian/seluruhnya dari sekumpulan data yang telah dicatat atau dilaporkan. Proses analisa data dimulai dengan membaca, mempelajari dan menelaah data yang diperoleh secara seksama. Analisis data dilakukan dengan mengorganisasikan dan mengurutkan data kedalam pola, kategori dan saturan uraian sehingga dapat ditemukan tema dan dapat menjawab pertanyaan penelitian.

HASIL DAN PEMBAHASAN

Menurut laporan Global Mobile Money tahunan ketiga MEF 2015, e-commerce dan mobile banking terus tumbuh dengan 69% pengguna ponsel menjalankan aktivitas perbankan mereka melalui perangkat seluler (Perelmuter, 2015). Laporan tersebut melakukan penelitian terhadap 15.000 pengguna ponsel di 15 negara berbeda di dunia. Laporan tersebut mendefinisikan istilah Uang Seluler untuk layanan termasuk pembayaran di dalam toko, tagihan operator, pembayaran online, pembayaran rekan kerja, dan pembayaran melalui dompet seluler. Meningkatnya penggunaan metode pembayaran seluler juga mendorong pasar maju untuk menginstal sistem dan infrastruktur penetrasi perangkat yang seharusnya mendukung transaksi seluler di dalam toko. Selain itu, metode pembayaran tanpa kontak juga menjadi populer dengan teknologi yang dapat dikenakan (Sacco, 2015) yang menawarkan cara pembayaran yang cepat, mudah, dan aman di berbagai tempat. Teknologi pembayaran yang dapat dikenakan termasuk jam tangan pintar, cincin, gelang tangan, dan sejumlah aplikasi smartphone Android atau iOS. Laporan GSMA State of the Industry untuk 2013 juga telah menampilkan beberapa statistik yang memberi cahaya pada masa depan pembayaran seluler. Menurut laporan ini, "Pada pertengahan 2013, ada lebih dari 203 juta akun uang seluler terdaftar di seluruh dunia dengan outlet uang seluler melebihi jumlah cabang bank di lebih dari 80% pasar di seluruh dunia" (Oracle, 2014). Tingkat transaksi pembayaran seluler meningkat di seluruh dunia dan nilainya diperkirakan akan meningkat dari US $ 12,8 miliar

(diperkirakan pada 2012) menjadi US $ 90 miliar pada 2017 (Oracle, 2014).

Statistik ini jelas menunjukkan bahwa masyarakat memiliki masa depan tanpa uang tunai di depan dengan opsi yang lebih aman dan nyaman untuk melakukan pembayaran melalui smartphone dan tablet. Di mana sistem pembayaran seluler telah membawa peluang baru bagi pedagang dan pelanggan, yang juga membuat mereka menghadapi risiko baru terkait masalah privasi dan keamanan. Menurut laporan pembayaran seluler, perencanaan yang cermat diperlukan untuk menjadikan keamanan sebagai elemen intrinsik dari metode pembayaran online di masa depan. Untuk masa depan pasar pembayaran mobile yang makmur, produsen ponsel, perusahaan telekomunikasi dan industri pembayaran perlu berkolaborasi satu sama lain sehingga platform dapat dikembangkan untuk memastikan lingkungan yang paling aman untuk transaksi pembayaran online. Namun, diyakini bahwa sistem pembayaran mobile memiliki potensi untuk mengatasi semua masalah keamanan dan privasi utama yang terkait dengan industri ini, dan perkembangan saat ini mengungkapkan bahwa inovasi sudah dikerahkan (Oracle, 2014). Resiko pasti selalu ada ketika kita memilih untuk menggunakan uang pembayaran elektronik seperti e-wallet.

Risiko adalah sesuatu yang mengarah pada ketidakpastian atas terjadinya suatu peristiwa selama selang waktu tertentu yang mana peristiwa tersebut menyebabkan suatu kerugian baik itu kerugian kecil yang tidak begitu berarti maupun kerugian besar yang berpengaruh terhadap kelangsungan hidup dari suatu perusahaan. Risiko pada umumnya dipandang sebagai sesuatu yang negatif, seperti kehilangan, bahaya, dan konsekuensi lainnya. Kerugian tersebut merupakan bentuk ketidakpastian yang seharusnya dipahami dan dikelolah secara efektif oleh organisasi sebagai bagian dari strategi sehingga dapat menjadi nilai tambah dan mendukung pencapaian tujuan organisasi.

Dalam hal ini resiko operasional yang bisa dialami oleh pengguna e-wallet misalnya penipuan kode pengguna e-wallet. Ada oknum yang menggunakan data dari pemilik dan menggunakan dana yang ada untuk membeli barang atau mencairkannya. Selain itu resiko operasional juga termasuk resiko teknologi misalnya error pada sistem. Bisa saja ketika digunakan aplikasi e-wallet tertutup atau mengirimkan uang ke pihak lain dikarenakan sistem yang sedang tidak berfungsi kembali.

Menurut Reddy (2004), masa depan pembayaran mobile dapat diamankan dengan menggunakan teknologi terbaru untuk mengatasi tantangan praktis dan analitis yang dihadapi oleh industri ini. Teknologi barcode radio diyakini sebagai tambahan revolusioner untuk sistem pembayaran mobile. Kode batang radio ini mengirimkan sinyal radio yang dapat digunakan untuk menemukan posisi benda-benda yang disematkan padanya. Dengan menggunakan barcode radio, pasar pembayaran seluler dapat menikmati masa depan yang menjanjikan dengan memberikan keamanan dan kenyamanan yang ditingkatkan kepada konsumennya. Teknologi kode batang radio dapat memungkinkan personal penjualan untuk membaca angka-angka dan tanggal kedaluwarsa pada kartu kredit konsumen saat mereka berjalan. Dengan meningkatkan protokol keamanan dan menggunakan teknologi terbaru seperti kode batang radio, penyedia layanan pembayaran seluler dapat membuat sistem yang tidak hanya dapat diskalakan di tingkat yang lebih tinggi tetapi juga paling nyaman digunakan bagi konsumen.

The Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS berlaku untuk entitas apa pun yang menyimpan, memproses, dan / atau mentransmisikan data pemegang kartu. Ini mencakup komponen sistem teknis dan operasional yang termasuk dalam atau terhubung ke data pemegang kartu. PCI DSS berlaku untuk produsen yang menentukan dan menerapkan karakteristik dan manajemen perangkat untuk terminal entri nomor identifikasi pribadi (PIN) yang digunakan untuk transaksi keuangan kartu pembayaran. PC-DSS adalah untuk pengembang perangkat lunak dan integrator aplikasi yang menyimpan, memproses, atau mengirimkan data pemegang kartu sebagai bagian dari otorisasi atau penyelesaian. Ini juga mengatur aplikasi-aplikasi ini yang dijual, didistribusikan atau dilisensikan kepada pihak ketiga.

Dewan Standar Keamanan PCI menetapkan standar untuk keamanan PCI tetapi setiap merek kartu pembayaran memiliki program sendiri untuk kepatuhan. Pertanyaan spesifik tentang kepatuhan harus diarahkan ke lembaga keuangan yang mengakuisisi. Adapun syarat-syarat untuk bisa dilakukannya Pengujian PCI DS pada sebuah aplikasi digital seperti e-Wallet DANA adalah dengan penilai yang berkualitas dimana dewan menyediakan program untuk dua jenis sertifikasi: Qualified Security Assesment (QSA) dan Approved Screening Validation (ASV).

Perkembangan Penggunaan Aplikasi e-Wallet "DANA"

e-Wallet adalah komponen perangkat lunak yang diunduh pengguna ke desktop mereka dan di mana pengguna menyimpan nomor kartu kredit dan informasi pribadi lainnya. Ketika pengguna berbelanja di merchant yang menerima e-Wallet, pengguna mengklik e-wallet dan formulir secara otomatis diisi dengan semua informasi yang diperlukan hanya dalam satu klik. Perusahaan kartu kredit seperti Visa dan MasterCard juga menawarkan e-Wallet ini. (Turban et al, 2004)

Temuan penelitian menunjukkan bahwa penggunaan perangkat seluler untuk melakukan pembayaran online semakin populer karena basis pengguna ponsel yang besar. Metode pembayaran ini paling sesuai dengan pembayaran mikro dan menawarkan transaksi pembayaran yang lebih nyaman dan aman jika diterapkan dengan tepat. Sistem uang elektronik sedang berjalan dalam mencapai penerimaan tinggi oleh konsumen meskipun kekuatan mereka untuk melayani pembayaran kecil dan bervariasi. Tantangan utama, untuk semua metode pembayaran ini, adalah penyediaan sistem otentikasi yang harus memastikan keamanan dan kenyamanan setiap transaksi yang dilakukan. (Bezhovski, 2016)

Menurut data yang diperoleh dari situs CNBC Indonesia (2019) bahwa DANA sebagai pendatang baru aplikasi e-walllet di Indonesia langsung menunjukkan kegigihannya untuk menjadi pioner aplikasi e-wallet di Indonesia. Berdasar data riset iPrice Group, DANA memiliki pengguna aktif bulanan yang relatif stabil sejak Q2 2018 hingga Q2 2019. Dana berhasil naik satu peringkat di kuartal 2 2019 menggantikan LinkAja di posisi ketiga dari aplikasi pembayaran yang paling banyak digunakan di Indonesia.

Dalam sebuah penelitian mengenai adopsi konsumen dari dompet seluler, Doan (2014) menjelaskan bahwa e-wallet terbentuk ketika Smartphone berfungsi sebagai dompet kulit: dompet ini dapat memiliki kupon digital, uang digital (transaksi), kartu digital, dan penerimaan digital.Layanan e-wallet memungkinkan pengguna untuk menginstal aplikasi dari toko online di smartphone mereka dan

menggunakannya untuk membayar pembelian online dan offline mereka. Menggunakan teknologi terbaru yang menghubungkan ponsel cerdas ke dunia fisik seperti NFC (Near Field Communication), gelombang suara, dan kode QR, solusi berbasis cloud, dompet seluler diyakini dapat memberikan solusi pembayaran yang lebih nyaman bagi pelanggan di masa mendatang.

Manajemen Resiko Operasional Penggunaan Aplikasi E-wallet Data dengan Implementasi PCI SPSS

Salah satu cara untuk melakukan manajemen resiko oleh DANA yaitu bahwa pihak DANA juga melakukan kerjasama dengan Direktorat Jenderal Kependudukan dan Catatan Sipil (Dukcapil) Kementerian Dalam Negeri. Dimana pada pemohon atau pengguna aplikasi DANA harus mempunyai data pribadi yang valid yang sesuai dengan data yang disimpan di Dukcapil untuk melakukan validasi layanan. Manajemen resiko yang dilakukan oleh pihak DANA ini tentunya bisa mengantipasi berbagai upaya negatif seperti pemalsuan data oleh pengguna. Disamping itu pula kerjasama antara DANA dan Dukcapil dapat menghindarkan terjadinya penyalahgunaan data pengguna oleh oknum yang tidak bertanggung jawab. Resiko pengguna e-Wallet sendiri akan menjadi berkurang dengan adanya DANA Protection apabila didukung dengan perilaku penggunaan yang sehat dari para pengguna. Untuk meminimalisirnya adalah agar para penggunan DANA tidak menggunakan smartphone yang sama secara bergantian dan tidak menginformasikan PIN atau OTP ke pihak lain secara sembarang yang dapat mengakibatkan terjadinya penyalahgunaan akun serta tindak kejahatan yang merugikan penggunanya.

Tujuan dari perlindungan dana ini sendiri disamping dari memudahkan para penggunaanya, yang menjadi plus adalah bahwa pengguna menjadi lebih yakin dan percaya dana yang ada didalam e- Wallet tersebut aman dan terlindung sehingga mereka bisa tenang melakukan transaksi. Apabila jaminan dirasakan mampu melindungi transaksi online yang mereka lakukan maka tingkat kepercayaan akan meningkat, dan para pengguna akan beralih menggunakan transaksi non kartu atau non tunai. Disamping itu juga dengan program Dana Protection maka masalah atau isu-isu yang menjadi kekhawatiran melakukan transaksi digital akan menjadi menurun.

Program Dana Protection ini sendiri didukung oleh teknologi keamanan yang mutakhir. Dimana DANA berani menjamin 100 persen perlindungan terhadap semua dana yang tersimpan didalam aplikasi DANA milik para penggunanya. Sehingga para pengguna tidak perlu cemas akan keamanan saldo, dan juga semua jenis transaksi yang menggunakan saldo DANA mereka. DANA memastikan bahwa apabila pengguna mengalami kerugian akibat dana yang disimpan dalam e-wallet DANA menghilang maka akan diberikan garansi pada uang mereka akan kembali. Hal ini disebabkan karena DANA sebagai e-wallet yang mengimplementasikan layanan transaksi digital adalah berada dibawah pengawasan Bank Indonesia dan sudah memiliki sertifikasi PCI DSS (The Payment Card Industry Data Security Standard). Sertifikasi ini merupakan standar keamanan tinggi setingkat keamanan perbankan. Selain itu, DANA juga memiliki Data Center dan Data Recovery Center di Indonesia, yang sudah sesuai dalam mengelola transaksi keuangan digital dalam skala tinggi dan melakukan manajemen risiko untuk melindungi pengguna.

SIMPULAN

Dengan teknologi canggih yang berkembang yang mendukung transaksi seluler dan menjadikannya transparan dan lebih nyaman, konsumen telah mengembangkan kepercayaan dan kebiasaan mereka dalam menggunakan sistem pembayaran seluler. Perubahan perilaku konsumen yang beralih dari metode pembayaran tradisional ke sistem pembayaran online yang lebih maju cukup jelas dalam perbankan dan ritel, dan dengan sebagian besar perangkat seluler tersedia. Karena terbukti bahwa perangkat seluler menjadi bagian tak terhindarkan dari hampir setiap kehidupan dari satu sisi dan peluang teknologi ini memungkinkan pembayaran online dan offline terkait kenyamanan dan keamanan, tidak dapat dihindari bahwa penggunaan sistem pembayaran seluler akan semakin meningkat dengan ambisi untuk melampaui atau bahkan mengganti uang tunai dan opsi pembayaran tanpa uang tunai lainnya.

The Payment Card Industry Data Security Standard (PCI DSS) atau Standar keamanan PCI adalah terbukti mampu membantu meminimalisasikan berbagai resiko operasional dari penggunaan e-wallet. PCI DSS sebagai persyaratan teknis dan operasional yang ditetapkan oleh Dewan Standar Keamanan Industri Kartu Pembayaran untuk melindungi data pemegang kartu. Standar ini secara global mengatur semua pedagang dan organisasi yang menyimpan, memproses atau mengirimkan data ini dengan persyaratan baru untuk pengembang perangkat lunak dan produsen aplikasi dan perangkat yang digunakan dalam transaksi

Kenyamanan dijelaskan sebagai konsistensi antara kemajuan dan pengalaman, nilai-nilai, dan kebutuhan konsumen. Aspek penting kompatibilitas bagi pengguna untuk mengadopsi metode pembayaran mobile adalah fleksibilitas sistem ini sehingga mereka dapat dengan mudah diintegrasikan ke dalam konsumen setiap hari.

Penelitian ini juga menyimpulkan bahwa untuk masa depan yang menjanjikan dari industri ini, sistem pembayaran mobile harus lebih terintegrasi dengan telekomunikasi dan infrastruktur keuangan saat ini. Meningkatkan kompatibilitas dengan berbagai pengguna, penggunaan teknologi terbaru dan penetapan standar umum untuk berbagai penyedia layanan, dan mengatasi masalah keamanan dan privasi dapat membantu memfasilitasi proses adopsi metode pembayaran elektronik yang lebih cepat dan memajukan pasar meningkatnya pembayaran mobile. Penelitian ini bertujuan untuk merangkul spektrum singkat masalah yang mungkin terjadi dengan metode pembayaran elektronik dan adopsi konsumen dari e-commerce untuk melakukan pembayaran untuk pembelian mereka. Penelitian di masa depan dapat fokus pada validasi faktor yang dapat berkontribusi pada keberhasilan penerapan metode pembayaran seluler di seluruh dunia.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah membantu didalam proses penyelesaian jurnal ini baik secara langsung maupun tidak langsung.

DAFTAR PUSTAKA

Abrazhevich, Dennis, (2004) Electronic Payment Systems: a User-Centered Perspective and Interaction Design. Netherlands: Technische Universiteit Eindhoven

Aigbe, Princewill and Akpojaro, Jackson (2014) Analysis of Security Issues in Electronic Payment Systems. Nigeria: International Journal of Computer Applications (0975-8887), Vol. 108 No, 10

Bezhovski, Z (2016) The Future of the Mobile Payment as Electronic Payment System. European Journal of Business and Management

www.iiste.org ISSN 2222-1905 Management www.iiste.org ISSN 2222-1905

Doan, Ngoc, (2014) Consumer adoption in Mobile Wallet. The Turku University of Applied Sciences

Karp, Nathaniel (2015). Biometrics: The Future of Mobile Payments. U.S. Economic Watch, BBVA Research

Koponen, A. (2006) E-Commerce, Electronic Payments. Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory.

Laukkanen, T., & Lauronen, J. (2005) Consumer value creation in mobile banking services. International Journal of Mobile Communications, 3(4), 325-338

Liputan 6 (2020). jamin-100-persen-keamanan-transaksi-pengguna- dengan-dana-protection https://www.liputan6.com/tekno/read/4034045/dana

PCI Security Standards Council LLC (2008) Payment Card Industry Security Standards.At A Glance Standard Overview. Akses pada 19 Januari 2020

Paunov, Caroline and Vickery, Graham (2006) Online Payment systems for E-Commerce. Organization for Economic Co-operation and development (OECD).

Raja, J., Velmurgan, Senthil M. and Seetharaman A. (2008) E-Payments: Problems and Prospects. Malaysia: Journal of Internat Banking and Commerce

Sahut, Jean-Michel. (2008). The Adoption and Diffusion of Electronic Wallets. Journal of Internet Banking and Commerce. 13

Siau, K., Sheng, H., Nah, F., & Davis, S. (2004). A qualitative investigation on consumer trust in mobile commerce. International Journal of Electronic Business, 2(3), 283-300

Turban,E et al (2004) A Managerial Perspective. Pearson Prentice Hall, New Jersey