STUDI LITERATUR : PERBANDINGAN SSL, SET, SEP BERDASARKAN END-USER IMPLEMENTATION REQUIREMENTS

Tirsa Ninia Lina[1*], **Irwan Sembiring**[1], **Hindriyanto Dwi Purnomo**[1]
Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50711
[*]Email: tirsawp@gmail.com

Abstrak

Sistem pembayaran elektronik (e-payment) dianggap sebagai tulang punggung e-commerce. Agar diterima secara luas metode pembayaran di seluruh dunia, sistem e-payment harus mengikuti protokol keamanan yang efisien yang menjamin keamanan yang tinggi untuk transaksi online. Secure Socket Layer (SSL) dan Secure Electronic Transaction (SET) merupakan dua protokol yang banyak dibahas untuk mengamankan pembayaran kartu kredit online. Namun, SSL maupun SET telah gagal dalam implementasi pada pengguna akhir, sehingga munculah protokol Secure Electronic Payment (SEP) yang merupakan protokol e-payment yang aman dan efisien yang menawarkan lapisan tambahan perlindungan bagi cardholder dan merchant. Tujuan penulisan ini untuk menentukan protokol mana yang paling cocok untuk keamanan e-payment berdasarkan perbandingan pada end-user implementation requirements. Metode yang digunakan berupa studi literatur dengan melihat karya terkait yang membahas mengenai protokol SSL, SET, SEP yang selanjutnya akan dilakukan perbandingan. Hasil yang didapatkan dari perbandingan protokol keamanan e-payment SSL, SET, dan SEP berdasarkan faktor end-user implementation requirements (usability, flexibility, affordability, reliability, availability, interoperability) yaitu bahwa protokol SEP yang memenuhi syarat dan paling cocok untuk diterapkan dalam keamanan e-payment.

***Kata kunci**: SSL, SET, SEP, security requirements of e-payment, end-user implementation requirements*

1. PENDAHULUAN

Munculnya *e-commerce* pada tahun 1990 memperkenalkan cara unik melakukan bisnis perdagangan untuk konsumen dan dunia usaha (Bezhovski, 2016). Sejak itu, *e-commerce* telah berkembang dan berubah dengan menghasilkan manfaat yang 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 dan bisnis akan mendapatkan manfaat maksimal (Abrazhevich, 2014). Sistem pembayaran elektronik (*e-payment*) dianggap sebagai tulang punggung *e-commerce*. Hal ini dapat didefinisikan sebagai layanan pembayaran yang memanfaatkan teknologi informasi dan komunikasi termasuk kartu *integrated circuit* (IC), kriptografi, dan jaringan telekomunikasi (Raja dkk., 2008). Dengan kemajuan teknologi, sistem *e-payment* telah mengambil berbagai bentuk termasuk kartu kredit, kartu debit, *e-cash* dan *check system*, *smart card*, *digital wallet*, dan pembayaran *mobile* dan sebagainya (Bezhovski, 2016).

Agar diterima secara luas metode pembayaran di seluruh dunia, sistem *e-payment* harus mengikuti protokol keamanan yang efisien yang menjamin keamanan yang tinggi untuk transaksi *online*. SSL dan SET merupakan dua protokol yang banyak dibahas untuk mengamankan pembayaran kartu kredit *online*. SSL adalah protokol yang umum digunakan untuk mengenkripsi pesan antara *web browser* dan *web server* (Craft dkk., 2009). SSL juga banyak digunakan oleh *merchant* untuk melindungi informasi konsumen selama transmisi, seperti nomor kartu kredit dan informasi sensitif lainnya. SSL digunakan untuk menyediakan integritas keamanan dan data melalui internet dan karena itu memegang peran penting. Salah satu masalah utama SSL adalah bahwa *merchant* dapat menyimpan informasi sensitif dari *cardholder*, dan protokol tidak mencegah *non-repudiation* karena otentikasi klien adalah opsional.

SET datang untuk menyelesaikan kelemahan SSL dalam otentikasi dan perlindungan informasi sensitif. SET menjamin integritas pembayaran, kerahasiaan dan otentikasi dari *merchant* dan *cardholder* (Houmani dan Mejri, 2012). Tapi SET ditandai dengan kompleksitas dan biaya didukung oleh *merchant* karena logistik sertifikat distribusi dan instalasi perangkat lunak klien.

Selain itu, karena masalah implementasi, SET belum benar-benar diadopsi oleh pelaku *e-commerce*. Berdasarkan hal tersebut yang menyatakan bahwa SSL maupun SET telah gagal dalam implementasi pada pengguna akhir, maka Ismaili dkk (2015) merancang protokol *e-payment* yang aman dan efisien yang menawarkan lapisan tambahan perlindungan bagi *cardholder* dan *merchant*. Protokol ini disebut SEP.

Ketiga protokol tersebut harus memenuhi syarat keamanan *e-payment* yaitu *information confidentiality*, *data integrity*, *authentication of participants*, *non-repudiation*, dan *end-user implementation requirements*. Namun, terkait dengan masalah implementasi pengguna akhir maka fokus penelitian ini adalah membandingkan antara protokol SSL, SET, dan SEP berdasarkan *end-user implementation requirements* (dimana terdiri dari beberapa poin yaitu *usability, flexibility, affordability, reliability, availability, interoperability*) sehingga mendapatkan protokol mana yang cocok untuk *e-payment* dalam hal ini implementasi pengguna akhir.

2. METODOLOGI

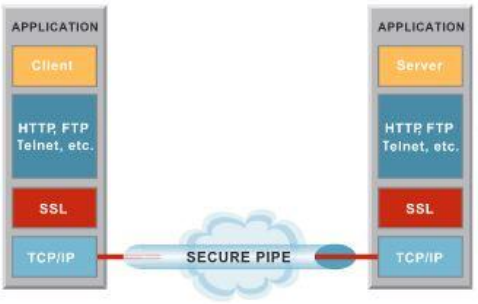
Metode yang digunakan adalah studi literatur dengan mencari referensi terkait pembahasan protokol SSL, SET, dan SEP dari segi *end-user implementation requirements*. Selanjutnya akan dilakukan perbandingan dari ketiga protokol tersebut.

3. HASIL DAN PEMBAHASAN

Hasil dan pembahasan dibagi menjadi beberapa sub topik yaitu *Secure Sockets Layer, Secure Electronic Transaction,* dan *Secure Electronic Payment*.

3.1. *Secure Sockets Layer*

SSL adalah protokol yang umum digunakan untuk mengenkripsi pesan antara *web browser* dan *web server*. Ini mengenkripsi datagrams dari protokol *Transport Layer*. SSL juga banyak digunakan oleh *merchant* untuk melindungi informasi konsumen selama transmisi, seperti nomor kartu kredit dan informasi sensitif lainnya. SSL digunakan untuk menyediakan integritas keamanan dan data melalui internet dan karena itu memegang peran penting. Salah satu masalah utama SSL adalah bahwa *merchant* dapat menyimpan informasi sensitif dari *cardholder*, dan protokol tidak mencegah *non-repudiation* karena otentikasi klien adalah opsional (Ismaili dkk., 2015).



Gambar 1. Protokol SSL (*sumber : RSA Data Security*)

3.1.1 SSL dan *End-user implementation requirement*

Keterkaitan SSL dengan *end-user implementation requirements*, didapatkan beberapa penelitian yang membahas mengenai *usability, flexibility, affordability, reliability, availability, speed of transaction,* dan *interoperability* sebagai berikut.

(1) *Usability*

Menurut Kawatra dan Kumar (2011), SSL sudah dibangun ke *web browser* yang sering digunakan dan tidak perlu menginstal perangkat lunak tambahan, sehingga memberikan kemudahan penggunaan bagi pelanggan. Rehman dkk (2012), juga mengatakan SSL mudah digunakan berdasarkan tabel yang dibuat mengenai perbandingan protokol yang umum digunakan untuk sistem *e-payment*, didapatkan *usability* untuk SSL bernilai *high* yang artinya SSL sangat mudah digunakan. Yolanda dan Elfira (2007) mengatakan bahwa implementasi SSL untuk transaksi elektronik dalam hal *usability* sangat mudah. Pemakaian

yang mudah karena cukup dengan mengaktifkan layanan SSL dan tidak perlu ada tambahan apa pun yang disediakan. Al-Refai dkk (2014) menguraikan beberapa hal perbandingan antara SSL dan SET. Berdasarkan hasil tersebut didapatkan kemudahan penggunaan SSL adalah bagus. Hal ini menunjukkan bahwa SSL mudah untuk digunakan. Takyi dan Gyaase (2012), mengatakan bahwa protokol SSL mudah untuk diterapkan dan lebih nyaman untuk digunakan. Begitu pula dengan Jarupunphol dan Mitchell (2003) yang menguraikan kemudahan penggunaan untuk pengguna akhir *e-commerce*. *Cardholder* dapat menggunakan SSL dengan benar-benar transparan karena sudah dibangun ke *web browser* yang sering digunakan, dan *merchant* juga dapat menerapkan SSL tanpa mengubah model pembayaran mereka dengan cara apapun.

(2) *Flexibility*
Jarupunphol dan Mitchell (2003) dalam peneltiannya mengatakan bahwa, kemudahan penggunaan untuk pengguna akhir *e-commerce*. *Cardholder* dapat menggunakan SSL dengan benar-benar transparan karena sudah dibangun ke *web browser* yang sering digunakan, dan *merchant* juga dapat menerapkan SSL tanpa mengubah model pembayaran mereka dengan cara apapun. Setiawan juga mengatakan protokol ini bebas dipergunakan siapa saja, bahkan didukung oleh dua *browser* utama, yaitu Netscape Navigator dan Microsoft Internet Explorer. SSL juga tidak mengkhususkan diri untuk hanya mendukung protokol tertentu seperti HTTP, karenanya SSL menggunakan *port* 443 untuk berhubungan dengan pelayan internet yang juga memiliki fasilitas SSL (Setiawan, 1999).

(3) *Affordability*
Berdasarkan uraian dari para peneliti pada poin *usability*, mereka mengatakan SSL mudah digunakan dan juga tidak membutuhkan perangkat lunak tambahan. Hal ini berarti tidak perlu adanya biaya tambahan dan ini membuat SSL sangat terjangkau bagi konsumen *e-commerce* (Kawatra dan Kumar, 2011;Yolanda dan Elfira, 2007).

(4) *Reliability*
Ismaili dkk (2015) mengatakan bahwa salah satu masalah utama SSL adalah bahwa merchant dapat menyimpan informasi sensitif dari *cardholder*, dan protokol tidak mencegah *non-repudiation* karena otentikasi klien adalah opsional. Jarupunphol dan Mitchell (2013) juga mengatakan bahwwa *merchant* tidak dapat dipercaya mengidentifikasi *cardholder*. SSL berbasis *e-commerce* memungkinkan *merchant* untuk melihat informasi pembayaran konsumen, berpotensi menyebabkan masalah keamanan untuk *cardholder*.

(5) *Availability*
Menurut Setiawan (1999), SSL sudah terintegrasi dengan *browser-browser* yang terkenal, seperti Internet Explorer &Netscape Navigator.

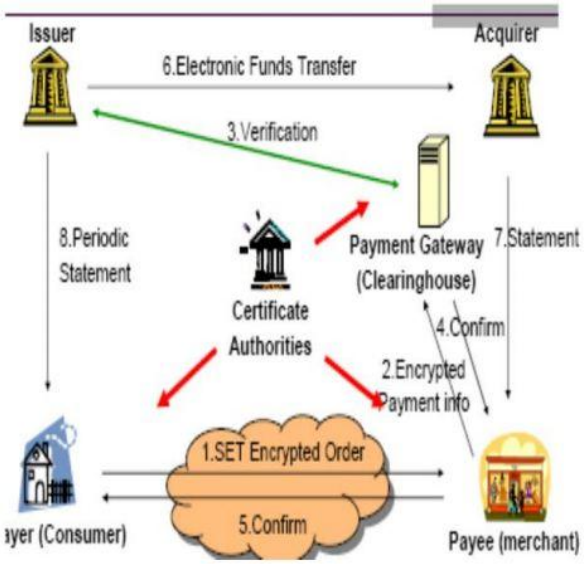
(6) Speed of transaction
Jarupunphol dan Mitchell (2003) mengatakan bahwa sistem ini tidak rumit, sehingga dampak minimal pada kecepatan transaksi. Hal itu dikarenakan algoritma kriptografi yang digunakan tidak lah rumit.

(7) *Interoperability*
Gambar 1 di atas menunjukan bahwa SSL belum dapat bekerja sama dengan beberapa *platform* yang berbeda, dapat digunakan jika pada *client* dan *server* mengggunakan *platform* yang sama. Seperti yang diungkapkan oleh Setiawan (1999), bahwa SSL hanya didukung oleh *browser* Internet Explorer &Netscape Navigator.

3.2. *Secure Electronic Transaction*

SET adalah protokol keamanan untuk sistem pembayaran elektronik. Hal ini ditemukan oleh Visa dan MasterCard pada tahun 1996 (Loeb, 1998;Merkow dkk., 1998).

SET datang untuk menyelesaikan kelemahan SSL dalam otentikasi dan perlindungan informasi sensitif, SET menjamin integritas pembayaran, kerahasiaan dan otentikasi dari *cardholder* dan *merchant* (Houmani dan Mejri, 2012). Tapi SET ditandai dengan kompleksitas dan biaya didukung oleh *merchant* (dibandingkan dengan alternatif yang diusulkan oleh SSL) karena logistik sertifikat distribusi dan instalasi perangkat lunak klien, juga sulit untuk mengelola *non-repudiation*.



Gambar 2. ***Secure Electronic Transaction*** **(Kawatra dan Kumar, 2011)**

3.2.1 SET dan *End-user implementation requirement*

Keterkaitan SET dengan *end-user implementation requirements*, didapatkan beberapa penelitian yang membahas mengenai *usability, flexibility, affordability, reliability, availability, speed of transaction,* dan *interoperability* sebagai berikut.

(1) *Usability*

Menurut Kawatra dan Kumar (2011), pelanggan harus menginstal perangkat lunak tambahan, yang dapat menangani transaksi SET. Selain itu, pelanggan harus memiliki sertifikat digital yang *valid*. Rehman dkk (2012), mengatakan SET sulit digunakan berdasarkan tabel yang dibuat mengenai perbandingan protokol yang umum digunakan untuk sistem *e-payment*, didapatkan *usability* untuk SET bernilai *low*. Ini berarti SET sulit untuk digunakan. Yolanda dan Elfira (2007) mengatakan bahwa SET yang melibatkan banyak pihak tentu mendatangkan kerumitan dalam implementasinya. Setiap pihak harus bersedia memiliki sertifikat digital yang *valid*. Selain itu, juga dibutuhkan perangkat lunak khusus yang perlu dipasang untuk kepentingan komunikasi antar partisipan. Al-Refai dkk (2014), menguraikan beberapa hal perbandingan antara SSL dan SET. Berdasarkan hasil tersebut didapatkan kemudahan penggunaan SET adalah kurang bagus. Hal ini karena dalam SET diperlukan sertifikasi kartu kredit konsumen. Sehingga ini membuat penggunaan SET menjadi sulit. Takyi dan Gyaase (2012), mengatakan bahwa pelaksanaan SET masih kompleks. Begitu pula dengan Jarupunphol dan Mitchell (2003) yang mengatakan menggunakan SET jauh lebih rumit daripada menggunakan SSL.

(2) *Flexibility*

Menurut Kawatra dan Kumar (2011), pelanggan harus menginstal perangkat lunak tambahan, yang dapat menangani transaksi SET. Selain itu, pelanggan harus memiliki sertifikat digital yang *valid*. Takyi dan Gyaas (2012) mengatakan SET juga memfasilitasi interoperabilitas antara perangkat lunak dan jaringan penyedia. Sama hal nya dengan Singh, dkk, yang mengatakan SET memfasilitasi dan mendorong interoperabilitas antara penyedia *software* dan jaringan. Hal ini membuat SET menjadi fleksibel sehinga konsumen dapat memesan produk atau jasadari lokasi manapun dan bukan hanya dari 1 PC saja.

(3) *Affordability*

Menurut Kawatra dan Kumar (2011), pelaksana SET lebih mahal daripada SSL. Takyi dan Gyaase (2012) SET, mengatakan bahwa pelaksanaan SET masih kompleks, karena biaya *overhead* dalam memperoleh PKI. Jarupunphol dan Mitchell (2003), mengungkapkan bahwa menerapkan SET lebih mahal daripada SSL bagi konsumen maupun *merchant*. Begitu pula dengan Singh dkk (2012), mereka mengatakan bahwa menerapkan SET lebih

mahal daripada SSL untuk *merchant* juga. Mereka beradaptasi dengan sistem untuk bekerja dengan SET lebih rumit daripada mereka beradaptasi untuk bekerja dengan SSL. Selain itu, *merchant* harus memiliki akun yang dibuka di bank bisnis yang mampu menangani transaksi SET.

(4) *Reliability*
Jarupunphol dan Mitchell (2003), mengatakan 3 hal mengenai *reliability* yaitu SET menjamin kerahasiaan informasi pembayaran pada semua tahap proses transaksi, termasuk transmisi data dan penyimpanan data, SET mencegah *merchant* dari melihat informasi pembayaran konsumen, karena informasi pembayaran diteruskan ke pengakuisisi dalam bentuk terenkripsi (dienkripsi menggunakan *public key* pengakuisisi), dan untuk memastikan privasi *merchant*, SET mencegah pengakuisisi dari melihat informasi pesanan konsumen yang tersimpan di *web server merchant*.

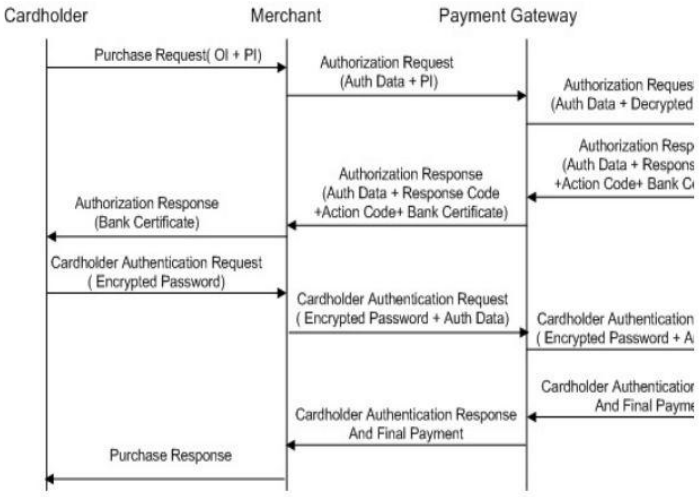
(5) *Availability*
Karena SET dibuat oleh 2 vendor besar yaitu Master Card dan Visa, sehingga in menjadikan SET memiliki cakupan ketersediaan yang lebih luas dibandingkan dengan SSL (Loeb, 1998;Merkow dkk., 1998).

(6) *Speed of transaction*
Kawatra dan Kumar (2011), menguraikan bahwa SET mempekerjakan mekanisme kriptografi yang kompleks yang mungkin berdampak pada kecepatan transaksi. Jarupunphol dan Mitchell (2003) mengatakan bahwa SET mempekerjakan mekanisme kriptografi yang kompleks yang dapat mengakibatkan kecepatan transaksi tidak dapat diterima. Begitu pula dengan Singh dkk (2012), mengatakan demikian bahwa SET mempekerjakan mekanisme kriptografi yang kompleks yang mungkin berdampak pada kecepatan transaksi.

(7) *Interoperability*
Takyi dan Gyaas (2012) mengatakan SET juga memfasilitasi interoperabilitas antara perangkat lunak dan jaringan penyedia. Sama hal nya dengan Singh dkk (2012), yang mengatakan SET memfasilitasi dan mendorong interoperabilitas antara penyedia *software* dan jaringan.

3.3. *Secure Electronic Payment*

Ide Ismaili dkk (2015), adalah untuk merancang protokol yang aman dan efisien untuk melindungi transaksi pembayaran *online* terhadap penipuan tanpa melibatkan pihak ketiga, protokol ini menanggapi dengan persyaratan keamanan *e-payment*: kerahasiaan, integritas, otentikasi dan *non-repudiation*.



Gambar 3. Deskripsi protokol SEP

Protokol SEP menghindari kompleksitas yang berkaitan dengan pelaksanaan tidak seperti SET, integrasi dan pemanfaatan juga lebih mudah dari sebelumnya.

3.3.1 SEP dan *End-user implementation requirement*

Berdasarkan *end-user implementation requirements*, didapatkan :

(1) *Usability* : *cardholder*, *merchant* menginstal *plug* khusus. Proses inisialisasi sangat sederhana, karena *cardholder* tidak perlu memiliki sertifikatnya.
(2) *Flexibility* : protokol SEP memiliki properti yang diinginkan yang dapat digunakan dari PC manapun, seperti saat ini kasus untuk transaksi *e-commerce* mengandalkan hanya pada SSL untuk keamanan komunikasi *cardholder-merchant*.
(3) *Affordability* : SEP hanya membutuhkan atribusi sertifikat keamanan untuk *merchant*, *payment gateway* dan *issuer bank*, dan *plug-in setup*.
(4) *Reliability*: Tentu saja, sementara kehadiran fungsi dalam keamanan penting unsur protokol SEP tidak mungkin, masih ada kemungkinan nyata bahwa kerentanan disengaja akan hadir dalam pelaksanaannya. Pengalaman masa lalu menunjukkan bahwa sangat sulit untuk memproduksi perangkat lunak yang tidak memiliki kerentanan dieksploitasi oleh perangkat lunak berbahaya.
(5) *Availability* : untuk protokol SEP *cardholder* dan pengakuisisi tidak diwajibkan untuk menerapkan sistem apapun dengan VISA. Setelah *issuer* memiliki perangkat lunak, mereka dapat mendukung transaksi SEP. Sama, konsumen akan senang untuk melakukan proses pendaftaran sederhana untuk mendapatkan pengkode kata sandi dan menginstal *plug-in*, tidak ada sertifikat keamanan yang dibutuhkan.
(6) *Speed of transaction* : protokol SEP menggunakan DES untuk enkripsi simetris dan RSA untuk verifikasi sertifikat. Verifikasi penerbit identitas *cardholder* merupakan faktor penting untuk kinerja transaksi. Sulit untuk memutuskan mengenai kecepatan transaksi karena itu terkait juga dengan kecepatan jaringan dan kinerja *server*.
(7) *Interoperability* : *plug-in* SEP dapat diinstal pada PC konsumen dengan mudah, sehingga masalah interoperabilitas kecil kemungkinannya untuk muncul.

Berdasarkan uraian di atas mengenai SSL,SET, dan SEP, maka hasil yang ditemukan yang berkaitan dengan keamanan *e-payment* terkait *end-user implementation requirements* dapat dilihat pada Tabel 1 berikut.

Tabel 1. Perbandingan SSL, SET, SEP

End-user implementation Requirements	**SSL**	**SET**	**SEP**
Usability	Mudah	Sulit	Mudah
Flexibility	Ya	Ya	Ya
Affordability	Terjangkau	Tidak	Terjangkau
Reliability	Tidak	Handal	Handal
Availability	Ya	Ya	Ya
Speed of transaction	Cepat	Lambat	Cepat
Interoperability	Tidak	Ya	Ya

Berdasarkan tabel perbandingan di atas, terlihat bahwa SSL yang sederhana dalam pelaksanaannya juga tidak memenuhi semua persyaratan keamanan *end-user implementation*. Kriteria yang terpenuhi oleh implementasi SSL yaitu *usability, flexibility, affordability, availability,* dan *speed of transaction*.

SET juga menunjukan hasil bahwa telah gagal memenuhi persyaratan *end-user implementation*. Kriteria yang terpenuhi oleh implementasi SET yaitu *flexibility, reliability, availability,* dan *interoperability*.

Sedangkan untuk Protokol SEP menunjukkan hasil yang baik, yaitu memenuhi seluruh persyaratan *end-user implementation* yaitu *usability, flexibility, affordability, availability, reliability, speed of transaction,* dan *interoperability*. Hal ini membuat SEP menjadi protokol yang paling cocok digunakan untuk keamanan *e-payment* dan cocok untuk pembayaran kartu kredit.

4. KESIMPULAN

Beberapa kesimpulan yang dapat ditarik berdasarkan hasil dan pembahasan adalah sebagai berikut:

(1) Persyaratan keamanan *e-payment* harus memenuhi syarat *information confidentiality*, *data integrity, authentication of participants, non-repudiation,* dan *end-user implementation requirements*. Untuk syarat *end-user implementation requirements* harus memenuhi kriteria *usability, flexibility, affordability, reliability, availability, speed of transaction,* dan *interoperability*.

(2) SSL yang sederhana dalam pelaksanaan juga tidak memenuhi semua persyaratan keamanan *end-user implementation*. Kriteria yang terpenuhi oleh implementasi SSL *yaitu usability, flexibility, affordability, availability,* dan *speed of transaction*.

(3) SET gagal memenuhi persyaratan *end-user implementation*. Kriteria yang terpenuhi oleh implementasi SET yaitu *reliability*, *availability*, dan *interoperability*.

(4) Protokol SEP memenuhi persyaratan *end-user implementation*. Hal ini membuat SEP menjadi protokol yang paling cocok digunakan untuk keamanan *e-payment* dan cocok untuk pembayaran kartu kredit.

4.1. Saran

Penelitian ini berupa studi literatur yang membahas perbandingan protokol SSL, SET, dan SEP berdasarkan *end-user implementation requirements*. Namun, dalam penulisan ini belum membahas kelemahan dan kinerja SEP yang berkaitan dengan keamanan yang ditawarkan SEP dalam melakukan transaksi *e-payment*. Maka dari itu, untuk penelitian selanjutnya diharapkan dapat menganalisis kinerja dan keamanan protokol SEP terkait keamanan dalam *e-payment* sehingga nantinya dalam melakukan perbandingan dengan protokol SSL maupun SET akan mendapatkan hasil perbandingan yang lebih baik.

DAFTAR PUSTAKA

A.Craft, T A and R. Kakar, (2009), E-Commere Security, Conference on information systems Applied Research v2 Washington.

A. Singh, K. Singh and Shahazad, (2012), A Review: Secure Payment System for Electronic Transaction, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, pp. 236-243.

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

Al-Refai. H, A. Alawneh, K. Batiha and A. Jarah, (2014), Enhanced model of Payment Phase for SET Protocol, International Journal of Video&Image Processing and Network Security, Vol.14, No.01, pp. 2.

Bezhovski, Z., (2016), The Future of the Mobile Payment as Electronic Payment System, European Journal of Business and Management, Vol.8, No.8, pp. 127-132.

H. Houmani, M. Mejri, (2012), Formal Analysis of SET and NSL Protocols Using the Interpretation Functions-based Method, Journal of Computer Networks and Communications, Volume 2012, Article ID 254942, pp. 18.

Ismaili, H, H. Houmani, H. Madroumi, (2015), A Secure Electronic Payment Protocol Design and Implementation, International Journal of Computer Science and Network Security, Vol.15, No.5, pp. 76 – 84.

Kawatra. N, Vijay Kumar, (2011), Analysis of E-Commerce Security Protocols SSL and SET, Proceedings published in International Journal of Computer Applications, pp. 3.

L. Loeb, (1998), Secure Electronic Transactions: Introduction and Technical Reference, Boston: Artech House.

M. S. Merkow, J. Breithaupt, and K. L. Wheeler, (1998), Building SET Applications for Secure Transactions, New York.

P. Jarupunphol, C. Mitchell, (2003), Measuring 3-D Secure and 3D SET against e-commerce end-user requirements, Proceedings of the 8th Collaborative Electronic Commerce Technology and Research Conference Europe.

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

Rehman. S, J. Coughlan and Z. Halim, (2012), Usability Based Reliable and Cashless Payment System (RCPS), International Journal of Innovative Computing, Information and Control, Vol.8, No.4, pp. 11.

Setiawan, I. B., (1999), SmartWallet – Java Wallet Berbasis Smartcard dan Protokol SET, Tugas Akhir, Fakultas Ilmu Komputer, Universitas Indonesia.

Takyi. A, P.O Gyaase, (2012), Enhancing Security of Online Payments: A Conceptual Model for a Robust E-Payment Protocol for E-Commerce, Contemporary Research on E-business Technology and Strategy, CCIS 332, pp. 232–239.

Yolanda S, Elfira, (2007), Studi dan Perbandingan Penerapan Protokol Kriptografi Kunci Publik pada Transaksi Elektronik, Institut Teknologi Bandung, pp. 14.

Treese, G. W. and Stewart, L. C., (1998), Designing Systems for Internet Commerce, Addison-Wesley, Massachusetts.

Z. Jiemiao, (2011), Research on E-Payment Protocol, Information Management, Innovation Management and Industrial Engineering, pp. 121 – 123.