

Verifikasi Penjualan Melalui Web Site e-Commerce dengan Menggunakan Metode Hashing (SHA)

Bernard Renaldy Suteja¹, Christian²

¹ Staf Pengajar Program Studi D-3 Teknologi Informasi

² Alumni Program Studi D-3 Teknologi Informasi

Fakultas Teknologi Informasi

Universitas Kristen Maranatha

Jl. Prof. Drg. Suria Sumantri no.65, Bandung 40164

Email : bernard.rs@eng.maranatha.edu, chrisagape@gmail.com

Abstract

e-Commerce is a dynamic set of technology, application and business process. It connects companies, customer, and certain community through electronic transactions. This also includes electronically based sales of products and services.

The method of Hashing, one that can also be called Hash Function is transforming certain input variables, returning a Hash value (a hashed variable) as output. Hash function is a one way operation, refers to a condition that the variable will be hard to re-digest to its previous value.

In a purchase verification, each product's data consisting a certain customer purchase will be hashed (using SHA) before it is sent through e-mail. It will be sent along with the purchased list of products performed by customer (included a server verification link using SHA).

Keyword: *E-commerce, Hashing Method (SHA), Verification*

1. Pendahuluan

e-Commerce merupakan kebutuhan esensial saat ini dalam dunia bisnis global, dan sebagai penunjang dalam pengembangan pasar, meningkatkan efisiensi, dapat menekan biaya, serta memberikan akses yang lebih luas bagi partner dan pelanggan perusahaan.

e-Commerce memiliki fleksibilitas dan keunikan bagi setiap perusahaan. Hal ini disebabkan setiap perusahaan memiliki perbedaan dalam pengembangan departemen IT, serta kebutuhan yang berbeda akan model teknologi informasi bagi bisnisnya. Fleksibilitas dan keunikan tersebut juga dimiliki oleh perusahaan - perusahaan di Indonesia, oleh karena itu penerapan *e-Commerce* sangat tergantung pada model bisnis dan teknologi informasi yang sedang dikembangkan oleh setiap perusahaan. Pengembangan *e-Commerce* harus bisa fleksibel dan bisa beradaptasi dengan software dan aplikasi teknologi yang ada di perusahaan.

e-Commerce merupakan salah satu cara untuk melakukan ekspansi pasar dan bersaing dengan pesaing secara global. *e-Commerce* dikembangkan untuk skala yang lebih luas dan terintegrasi dengan multiple computing system; semua lini dan departemen di perusahaan, organisasi atau perusahaan lain, serta sistem komputer global. Karena sifatnya terintegrasi secara langsung dengan dua atau lebih komputer, maka pengembangan *e-Commerce* harus benar-benar memperhatikan segi keamanan, terutama keamanan dalam bertransaksi.

e-Commerce sendiri bukan berarti tidak memiliki resiko, justru sebaliknya, dengan menggunakan *e-Commerce* banyak resiko yang akan dihadapi. Salah satu resiko adalah pada saat melakukan verifikasi data pembelian antara user dengan server. Untuk itu diperlukan verifikasi yang aman dengan cara metode hashing. Dimana data pembelian yang dikirim akan di hashing terlebih dahulu dengan menggunakan SHA (*Secure Hash Algorithm*) kemudian pada saat melakukan verifikasi akan di cocokan SHA yang dikirim dengan yang ada di server, jika cocok maka pembelian data di proses, jika tidak pembelian akan diabaikan.

2. E-Commerce

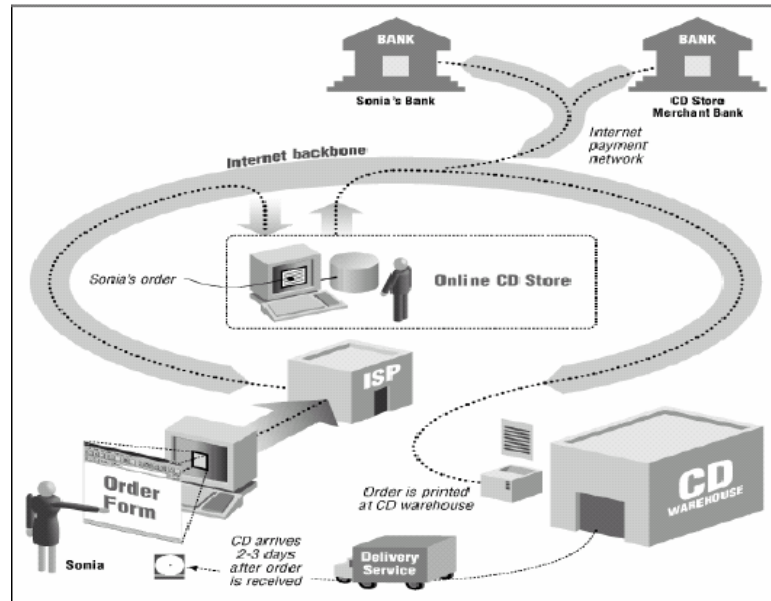
Saat ini definisi pasti *e-Commerce* yang sudah menjadi standar dan di disepakati bersama masih belum ada. Namun secara umum kita bisa mengartikan *e-Commerce* :

e-Commerce is dynamic set of technologies, applications, and business process that link enterprises, consumers, and communities through electronic transactions and the electronic exchange of goods, services, and information.

(David Baum, "Business Links," Oracle Magazine, No. 3, Vol. XIII, May/June, 1999, pp.36-44)

Jadi, *e-Commerce* merupakan suatu himpunan dinamis antara teknologi, aplikasi dan proses bisnis yang menghubungkan perusahaan, konsumen, dan komunitas tertentu melalui transaksi elektronik dan perdagangan barang, pelayanan, dan informasi yang dilakukan secara elektronik.

*Verifikasi Penjualan Melalui Web Site E-Commerce
dengan Menggunakan Metode Hashing (SHA)
(Bernard Renaldy Suteja, Christian)*



Gambar 1. Proses dalam e-Commerce

Keuntungan yang dapat diperoleh dengan adanya *e-Commerce* :

- *Revenue stream* (aliran pendapatan) baru yang mungkin lebih menjanjikan, yang tidak bisa ditemui di sistem transaksi tradisional.
- Dapat meningkatkan *market exposure* (pangsa pasar).
- Menurunkan biaya operasional (*operating cost*).
- Melebarkan jangkauan (*global reach*).
- Meningkatkan *supplier management*.
- Meningkatkan *customer loyalty*.
- Memperpendek waktu produksi.
- Meningkatkan *value chain* (mata rantai pendapatan).

Secara umum, *e-Commerce* dapat diklasifikasikan menjadi dua jenis, yaitu *Business to Business* (B2B) dan *Business to Consumer* (B2C). Berikut perbedaan dari kedua jenis *e-Commerce* :

a. ***Business to Business***, karakteristiknya adalah :

- *Trading partners* yang sudah saling mengetahui dan antara mereka sudah terjalin hubungan yang berlangsung cukup lama. Pertukaran informasi hanya berlangsung di antara mereka dan karena sudah mengenal, maka pertukaran informasi tersebut dilakukan atas dasar kebutuhan dan kepercayaan.
- Pertukaran data dilakukan secara berulang-ulang dan berkala dengan *format* data yang telah disepakati. Jadi service yang digunakan antar kedua sistem tersebut sama dan menggunakan standar yang sama pula.

- Salah satu pelaku tidak harus menunggu *partner* mereka lainnya untuk mengirimkan data.
 - Model yang umum digunakan adalah *peer-to-peer*, di mana *processing intelligence* dapat didistribusikan di kedua pelaku bisnis.
- b. ***Business to Consumer***, karakteristiknya adalah :
- Terbuka untuk umum, di mana informasi disebarluaskan secara umum pula.
 - Layanan yang dilakukan juga bersifat umum, sehingga mekanismenya dapat digunakan oleh orang banyak. Sebagai contoh, karena sistem web sudah umum di kalangan masyarakat maka sistem yang digunakan adalah sistem web pula.
 - Layanan yang diberikan adalah berdasarkan permintaan. Konsumen berinisiatif sedangkan produsen harus siap memerikan respon terhadap inisiatif konsumen tersebut.
 - Sering dilakukan sistem pendekatan *client-server*, di mana konsumen di pihak *client* menggunakan sistem yang minimal (berbasis *web*) dan penyedia barang/jasa (*business procedure*) berada pada pihak *server*.

Banyak sekali yang bisa dilakukan melalui *e-Commerce*. Namun umumnya orang menganggap *e-Commerce* sebagai kegiatan seperti membeli sebuah buku di toko *online*. Padahal *e-Commerce* tidak hanya sebatas itu, pengertian *e-Commerce* sangat luas dan masih banyak bidang-bidang yang dapat dikembangkan dalam *e-Commerce*. Ketepatan, kemudahan, dan kecepatan menjadi ciri *e-Commerce*. Berikut kegiatan yang bisa dilakukan di dalam *e-Commerce* :

- Perdagangan *online* melalui *world wide web* (*PC - Personal Computer*) merupakan contoh yang paling gampang dan umum diketahui orang.
- Transaksi *online* bisnis antar perusahaan.
- *Internet banking*.
- *TV interaktif*.
- *WAP (Wireless Application Protocol)*.

Meskipun *e-Commerce* merupakan sistem yang menguntungkan karena dapat mengurangi biaya transaksi bisnis dan dapat memperbaiki kualitas pelayanan kepada pelanggan, namun sistem *e-Commerce* ini beserta semua infrastruktur pendukungnya mudah sekali disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab, dan bisa juga terkena kesalahan-kesalahan yang mungkin timbul melalui berbagai cara.

Dari segi pandangan bisnis, penyalahgunaan dan kegagalan sistem yang terjadi, terdiri atas :

- Kehilangan segi finansial secara langsung karena kecurangan.
- Pencurian informasi rahasia yang berharga.
- Kehilangan kesempatan bisnis karena gangguan pelayanan.

- Penggunaan akses ke sumber oleh pihak yang tidak berhak.
- Kehilangan kepercayaan dari para konsumen.
- Kerugian-kerugian yang tidak terduga.

Berdasarkan semua uraian di atas, terlihat bahwa melakukan atau menyusun kegiatan *eCommerce* tidak semudah kita membalikan telapak tangan. Banyak sekali faktor yang harus diperhatikan dan dipertimbangkan. Kita harus mengasumsikan bahwa semua keuntungan yang akan diraih ekivalen/sebanding dengan nilai kerugian yang mungkin timbul.

Sistem keamanan informasi (*information security*) memiliki empat macam tujuan yang sangat mendasar, yaitu :

- *Confidentiality*
Menjamin apakah informasi yang dikirimkan tersebut tidak dapat dibuka atau tidak dapat diketahui oleh orang lain yang tidak berhak.
- *Integrity*
Menjamin konsistensi data tersebut apakah dia itu masih utuh sesuai aslinya atau tidak.
- *Availability*
Menjamin pengguna yang sah agar bisa mengakses informasi dan sumber miliknya sendiri. Jadi tujuannya untuk memastikan bahwa orang-orang yang memang berhak atau tidak ditolak untuk mengakses informasi yang memang menjadi haknya.
- *Legitimate Use*
Menjamin kepastian bahwa sumber tidak digunakan (informasi tidak diakses) oleh orang-orang yang tidak bertanggung jawab (orang-orang yang tidak berhak).

3. Fungsi Hash

Fungsi satu arah (*one-way function*) sering disebut juga sebagai fungsi *hash*, *message digest*, *fingerprint*, fungsi *kompresi*, dan *message authentication code* (MAC). Fungsi ini biasanya diperlukan bila kita menginginkan pengambilan sidik jari suatu pesan. Sebagaimana sidik jari manusia yang menunjukkan identitas si pemilik sidik jari, fungsi ini diharapkan pula mempunyai kemampuan yang serupa dengan sidik jari manusia, dimana sidik jari pesan diharapkan menunjuk ke satu pesan dan tidak dapat menunjuk kepada pesan lainnya.

Dinamakan sebagai fungsi kompresi karena masukan fungsi satu arah ini selalu lebih besar dari pada keluarannya, sehingga seolah-olah mengalami kompresi. Namun kompresi hasil fungsi ini tidak dapat dikembalikan ke asalnya sehingga disebut sebagai fungsi satu arah.

Dinamakan sebagai *message Digest* karena seolah-olah merupakan inti sari pesan, padahal tidak demikian. Sebab inti sari pesan mestinya merupakan