# Aplikasi *Digital Signature* Pada Sistem Pelelangan *On-Line* yang Menggunakan Model *Reverse* Paralel

**Ilden Abi Neri** [1)]

1) Program Studi Teknik Informatika STEI ITB, Bandung, email: if14145@students.if.itb.ac.id

***Abstract –*** *Digital signature dapat digunakan untuk mendukung keamanan terutama untuk menjaga keaslian suatu dokumen digital dan menghindari penyangkalan. Salah satu contoh bentuk pemanfaatannya adalah pada sistem pelelangan on-line. Disini digital signature berfungsi untuk menghindari penipuan dari orang yang ikut dalam pelelangan terutama menghindari penyangkalan oleh peserta pelelangan terhadap tawaran yang telah diberikannya.*

***Kata Kunci****: pelelangan on-line, digital signature, paralel reverse auction*

## 1. PENDAHULUAN

Internet telah memberikan peranan besar dalam mentransformasikan bisnis, bahkan internet merupakan bagian yang tidak terpisahkan lagi dari bisnis. Salah satu peranan internet dalam bisnis adalah pada pelelangan. Saat ini banyak sekali terdapat bisnis pelelangan yang dilakukan secara *on-line* atau dengan kata lain internet menjadi pemeran utama untuk keberjalanan bisnis tersebut. Diantaranya seperti, *BargainFinder*, *Jango*, *Ubid*, *Michigan Internet AuctionBot*, *Onsale*, *Amazon*, *eBay*, dan lain-lain.

Bisnis pelelangan *on-line* ini terus mengalami perkembangan. *eBay* dapat diambil sebagai contoh yang perkembangannya terus mengalami kemajuan dimana menurut data tahun 2003, pendapatannya mencapai 2,17 milyar dolar dengan keuntungan bersih mencapai 441,8 juta dolar [3]. Namun, tentu saja tidak sedikit perusahaan pelelangan *on-line* yang mengalami kemunduran bahkan gulung tikar.

Secara keseluruhan, dari sekian banyak masalah dan tantangan yang harus dihadapi oleh pelelangan *on-line*, salah satunya adalah masalah keamanan atau *security*. Untuk lebih spesifiknya adalah masalah penipuan. Hal ini didukung oleh hasil penelitian *Internet Fraud Complaint Center* (IFCC) pada tahun 2002 yang menyatakan bahwa dari sekian banyak daftar kejahatan penipuan melalui internet, yang paling besar adalah penipuan melalui pelelangan *on-line*.

Ada beberapa metode yang dapat digunakan untuk mencegah penipuan ini. Diantaranya dengan penyediaan informasi yang cukup ,baik kepada *customer* maupun penyelenggara bisnis, perbaikan *payment system* yang ada, audit sistem terutama untuk menjamin kualitas penyelenggara bisnis, dan pemanfaatan *digital signature* [5].

Pada makalah ini, akan dibahas pemanfaatan digital signature pada salah satu bentuk *sistem* pelelangan *on-line*.

## 2. DASAR TEORI

### 2.1. Pelelangan *On-line* [4] [6] [7] [8]

Pelelangan merupakan salah satu contoh aktivitas ekonomi manusia yang telah dilakukan sejak zaman dahulu. Salah satu sumber menyebutkan bahwa hal ini telah dilakukan semenjak 500 SM.

Menurut teori ekonomi, pelelangan didefinisikan sebagai salah satu metode untuk menentukan nilai dari suatu komoditas yang memiliki harga yang tak dapat dipastikan. Pelelangan yang dalam Bahasa Inggris disebut sebagai *auction*, diartikan oleh McAfee dan McMillan dengan "*a market institute with an explicit set of rules determining resource allocation and prices on the basis of bids from the market participants*".

Dan pelelangan *on-line* didefinisikan sebagai sebuah mekanisme pelelangan dengan memanfaatkan internet sebagai mediasinya sehingga dalam prosesnya :

1) Tidak terbatas oleh waktu
2) Tidak terbatas oleh tempat
3) Terdapatnya interaksi sosial secara virtual
4) Dimungkinkan terdapatnya peserta yang sangat banyak bahkan tidak terbatas [7][8]

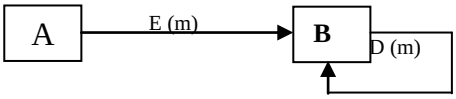
Pelelangan dapat terjadi dalam bentuk model bisnis *consumer-to-consumer* (C2C), *business-to-consumer* (B2C), *business-to-business* (B2B), *business-to-government* (B2G), dan *government-to public* (G2P). Pelelangan sendiri memiliki beberapa jenis atau kategori. Diantaranya adalah *reverse auction* (*English auction*), *Dutch auction*, *demand management auction*, *stock market*. Diantara kategori tersebut yang paling terkenal sekaligus paling banyak diaplikasikan baik secara tradisional maupun secara *on-line* adalah *reverse auction* (*English Auction*) dimana pada pelelangan tersebut barang/jasa yang akan dilelang ditawarkan oleh satu orang penjual (*seller*) kepada banyak calon pembeli atau penawar (*bidders*) yang dimulai dengan harga yang rendah kemudian pelelangan berakhir dengan *bidders* yang memiliki penawaran tertinggi sebagai pemenangnya. [4] [6]

### 2.2. *Digital Signature* [1]

Tanda tangan adalah salah satu cara yang dapat dipakai untuk membuktikan keaslian berbagai macam dokumen. Begitu pula dengan tanda tangan digital (*digital signature*) yang mana dapat digunakan untuk membuktikan keaslian dari dokumen digital.

Pemanfaatan *digital signature* dapat dilakukan dengan 2 cara :

1) Dengan meng-enkripsi pesan




**Gambar 1 Pengiriman Pesan Ter-enkripsi**

Pesan terenkripsi E(m) dikirim oleh A ke B, dan B mengetahui isi pesan yang dikirim oleh A dengan cara men-dekripsinya D(m).

2) Dengan mengenkripsi nilai fungsi hash (*hash function*) dari dokumen.
Pesan yang dikirim tidak dienkripsi tetapi nilai fungsi hash dari pesan tersebutlah yang dienkripsi kemudian ditambahkan ke dalam pesan yang dikirim.

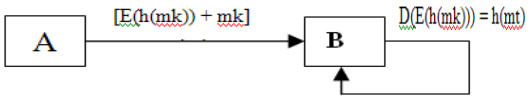
Proses enkripsi dan dekripsi pesan atau nilai hash dari pesan dapat dilakukan dengan memanfaatkan algoritma kunci simetri. Tetapi, terdapat suatu kelemahan pada algoritma ini karena tidak terdapat suatu mekanisme untuk mengatasi masalah dimana pihak yang mengirim pesan menyangkal bahwa telah mengirim pesan. Karena, kunci untuk meng-enkripsi diketahui kedua belah pihak (pengirim dan penerima pesan) sehingga mungkin saja terjadi kasus seperti ini : pengirim misal A, menyangkal telah mengirim pesan ke B, dan menuduh bahwa B-lah yang sebenarnya mengirim pesan tersebut.

Oleh karena itu, algoritma kunci publik yang ditemukan oleh Diffie dan Hellman, adalah algoritma yang tepat digunakan untuk mengatasi masalah diatas. Karena untuk membaca pesan, B menggunakan kunci publik dari A, dan A tidak dapat menuduh B telah mengirim pesan karena hanya A yang mengetahui kunci privat yang digunakan untuk meng-enkripsi pesan.

Namun, terdapat suatu masalah dengan algoritma kunci publik, karena algoritma ini biasanya menggunakan tingkat komputasi yang tinggi, maka enkripsi terhadap pesan akan sangat tidak efektif apalagi jika ukuran pesan yang akan dikirim sangat besar.

Untuk mengatasi permasalahan ini, maka yang di-enkripsi bukanlah isi dari pesan melainkan nilai hash dari pesan, kemudian menambahkan hasil enkripsi nilai hash tersebut sebagai tanda tangan pada dokumen yang ingin dikirim.

Tentunya solusi di atas hanya berlaku pada pengiriman pesan dimana isi pesan bukanlah sesuatu hal yang rahasia.




**Gambar 2 Pengiriman Pesan dan Hasil Enkripsi Nilai Hash Pesan**

E = Enkripsi dengan kunci privat A
D = Dekripsi pesan dengan kunci publik A
h = Fungsi hash
mk = pesan awal (yang dikirim A)
mt = pesan yang diterima B (tidak termasuk tanda tangan)

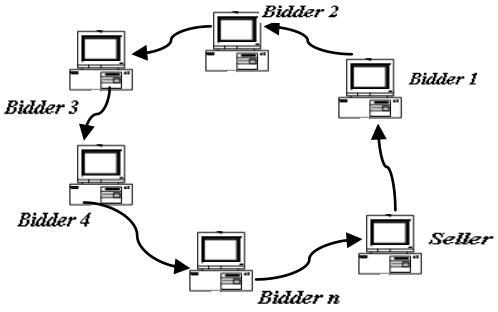
Jika nilai hash pesan yang diterima oleh B, h(mt), sama dengan hasil dekripsi terhadap tanda tangan, D(E(h(mk))), maka B dapat meyakini bahwa pesan tersebut betul dari A, dan A tidak dapat menyangkal telah mengirimkan pesan ke B.

Terdapat beberapa algoritma *digital signature* yang dapat digunakan untuk melakukan enkripsi pesan diantaranya adalah RSA, DSA (algoritma standar *digital signature standar* DSS), dan lain-lain.

## 3. *DIGITAL SIGNATURE* PADA PELELANGAN *ON-LINE*

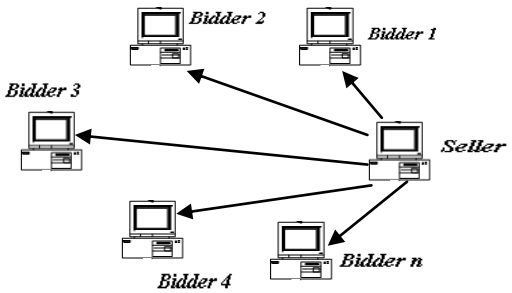
Model pelelangan *reverse* (*reverse auction*) pada pelelangan *on-line*, menurut penulis dapat dilakukan dengan 2 cara :

1) *Cycle mechanism*




**Gambar 3 *Cycle Mechanism***

2) *Paralel mechanism*




**Gambar 4 *Paralel Mechanism***

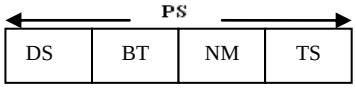
Pada mekanisme *cycle*, penawaran pertama dikirimkan oleh *seller* dan akan kembali lagi pada *seller* (mencapai satu *cycle*). Pada saat sedang dalam *cycle*, *bidder* berhak memutuskan apakah akan membuat penawaran yang lebih tinggi atau membiarkannya tetap setinggi seperti yang diterima dari node sebelumnya. Informasi dari setiap node ke-n akan diteruskan ke node (n+1), dan setiap perubahan yang dibuat pada node ke n diketahui oleh node (n+1). Jika dalam tiga kali *cycle*, penawaran yang dibuat oleh suatu *bidder* tidak berubah atau *bidder* yang lain tidak membuat penawaran yang lebih tinggi, maka *bidder* tersebut akan menjadi pada pemenang dalam pelelangan. Penjelasan rinci mengenai penerapan *digital signature* pada model dengan mekanisme *cycle* ini terdapat pada [2].

Sesuai dengan judul, pada makalah ini dibahas model *reverse* dengan mekanisme paralel. Pada model ini, penawaran pertama dikirimkan oleh *seller* secara serentak kepada semua *bidders* yang ikut dalam pelelangan. Penawaran dapat dilakukan oleh suatu *bidder* tanpa harus menunggu *bidder* lain selesai melakukan penawaran seperti yang terjadi pada mekanisme *cycle*. Jika dalam waktu tertentu tidak ada lagi penawaran yang lebih tinggi dari pada penawaran yang diberikan oleh suatu *bidder* maka *bidder* tersebutlah yang menjadi pemenang dalam pelelangan.

Pemanfaatan *digital signature* disini adalah untuk **menjamin bahwa suatu *bidder* tidak dapat menyangkal penawaran yang telah dilakukannya atau diberikannya dalam pelelangan**.

Berikut adalah rincian aturan/protokol sederhana pemanfaatan *digital signature* dalam sistem pelelangan *on-line* yang menggunakan *model reverse* dengan mekanime paralel :

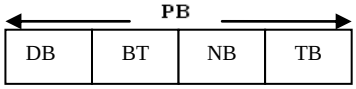
1) Setiap orang yang berhak atau ingin menjadi *bidder* dalam pelelangan terlebih dahulu harus melakukan registrasi atau mendaftar sebagai *member* dalam sistem pelelangan *on-line*. Pada tahap ini calon *member* memberikan informasi yang berguna sebagai identitas yang digunakan dalam pelelangan.
2) Setiap orang yang telah terdaftar pada sistem, berhak untuk ikut menjadi *bidder* pada semua pelelangan yang terjadi dalam sistem pelelangan *on-line*. Tahap 1) dan 2) ini bisa disebut sebagai tahap registrasi.
3) Orang yang telah terdaftar memilih salah satu pelelangan yang terjadi (sehingga menjadi *bidder* pada pelelangan tersebut).
4) *Seller* pada sistem pelelangan *on-line*, memperoleh semua *member* yang telah menjadi *bidder* untuk pelelangan suatu barang/jasa.
5) *Seller* memulai pelelangan dengan mengirimkan pesan PS yang berisi *timestamp* sistem *seller* (TS), nilai minimum (NM) bagi barang/jasa yang akan dilelang kepada semua *bidder*, informasi *bidder* dengan penawaran tertinggi saat ini (BT) yang mana tentunya pada awal pelelangan masih berisi kosong dan nilainya harus unik untuk setiap *bidder*, *digital signature* dari *seller* (DS) terhadap bagian pesan PS.




**Gambar 5 Pesan PS dari Sistem**

DS merupakan hasil enkripsi menggunakan kunci privat *seller* (Kprs) terhadap nilai hash (h) dari BT, NM, dan TS atau DS = $E_{Kprs\ (h(BT, NM, TS))}$

6) Masing-masing *bidder* menerima PS' (untuk membedakan pesan yang dikirim dengan yang diterima maka pesan yang diterima diberi tanda petik satu). *Bidder* mengetahui bahwa pesan PS' yang diterima adalah betul dari *seller* dengan cara mendekripsi DS' dengan kunci publik *seller* (Kpbs). Nilai hasil dekripsi disebut sebagai $D_{Kpbs}$(DS'). Kemudian menghitung nilai hash dari bagian PS' : BT', NM', dan TS' (h(BT', NM', TS')). Apabila $D_{Kpbs}$(DS') = h(BT', NM', TS') maka *bidder* dapat memastikan bahwa PS' yang diterima adalah betul dari *seller*.
7) Bagi *bidder* yang ingin melakukan penawaran, dapat langsung mengirimkan pesannya (PB) kepada *seller* yang berisi *timestamp* sistem *bidder* (TB), nilai tawaran yang diberikan *bidder* (NT) untuk barang/jasa yang dilelang (NT>NM), informasi *bidder* (BT), *digital signature* dari *bidder* (DB) terhadap bagian pesan PB.




**Gambar 6 Pesan PB dari Bidder**

DB merupakan hasil enkripsi terhadap PB dengan menggunakan kunci privat *bidder* (Kprb) terhadap nilai hash (h) dari BT, NB dan TB. DB = $E_{Kprb\ (h(BT, NB,TB))}$

8) *Seller* menerima PB' dari *bidder*. Sama seperti *bidder*, *seller* dapat mengetahui apakah pesan yang diterima adalah betul berasal dari *bidder* dengan cara melakukan dekripsi terhadap DB' menggunakan kunci publik *bidder* (Kpbb). Nilai hasil dekripsi disebut sebagai $D_{Kpbb}$(DB'). Kemudian *seller* menghitung nilai hash h(BT', NB', TS'). Apabila $D_{Kpbb}$(DB')= h(BT', NB', TS'), maka *seller* dapat memastikan bahwa pesan yang diterima adalah betul dari *bidder*.
9) Setiap tawaran yang diterima *seller* pada suatu waktu, akan membuat *seller* untuk langsung membuat/menghasilkan PS baru dengan NM yang telah di ubah sesuai dengan tawaran *bidder* yang tertinggi pada suatu waktu tersebut, BT yang berisi informasi *bidder* yang melakukan penawaran tertinggi tersebut, TS terbaru, kemudian mengirimkan kembali PS yang baru tersebut kepada semua *bidder*.

10) Jika untuk jangka waktu tertentu (lamanya bisa sebelumnya merupakan peraturan mutlak dari *seller* atau berdasarkan kesepakatan dengan semua *bidder* sebelum pelelangan dimulai) tidak terdapat lagi penawaran dengan harga yang melebihi harga minimum, maka pelelangan akan diselesaikan dengan pemenang adalah *bidder* dengan tawaran tertinggi terakhir. Atau bisa juga terdapat kemungkinan dimana dalam jangka waktu tertentu untuk harga minimum pertama kali yang ditawarkan *seller*, tidak ada *bidder* melakukan penawaran yang melebihi harga tersebut, maka pelelangan dihentikan atau *seller* menurunkan harga minimumnya.

Dari aturan/protokol sederhana diatas dapat disimpulkan dengan mudah, bahwa *bidder* tidak mungkin bisa melakukan penyangkalan terhadap tawaran yang telah dilakukannya, karena adanya pemanfaatan *digital signature* yang memakai algoritma kriptografi kunci publik untuk mengetahui *bidder* mana yang melakukan penawaran. Pesan ditandatangani dengan mengenkripsi nilai hash pesan dengan kunci privat *bidder*. Kemudian pesan diperiksa oleh *seller* dengan mendekripsi pesan menggunakan kunci publik dari *bidder*.

Aturan/protokol diatas memiliki beberapa isu yang patut untuk dicermati :

1) Karena aturan/protokol ini diterapkan pada mekanisme paralel, keunikan pesan yang diterima oleh *seller* dari setiap *bidder* adalah suatu hal yang menjadi keharusan, karena hal tersebut berguna bagi *seller* untuk mengetahui pesan tersebut berasal dari *bidder* yang mana. Keunikan ini dimungkinkan karena nilai BT unik untuk setiap *bidder*.
2) Aturan protokol ini hanya mungkin terlaksana jika pelelangan terjadi secara *real time*. Sehingga koneksi internet dari *seller* ke semua *bidder* adalah hal yang sangat berperan penting dalam pelelangan ini.
3) Tingkat keamanan algoritma kunci public yang digunakan untuk digital signature sangat berpengaruh pada kunci yang digunakan (biasanya tingkat keamanan semakin baik jika panjang kunci yang digunakan atau nilai yang digunakan sebagai kunci sangat besar[1]). Hal ini otomatis berpengaruh secara langsung terhadap keamanan dari pelelangan *on-line* itu sendiri karena *digital signature* yang digunakan memanfaatkan algoritma kunci publik.
4) Pada aturan/protokol disebutkan bahwa setiap terjadi penawaran baru, *seller* akan meng-*update* pesannya dan memberikannya langsung kepada semua *bidder*. Disini harus dipastikan bahwa setiap pesan baru yang diterima oleh *bidder* harus membuat pesan yang lama menjadi *obsolete* atau tidak valid lagi, hal ini dimungkinkan karena pada pesan terdapat *timestamp* yang menginformasikan kapan pesan pertama kali dibuat.
5) Karena pelelangan dilakukan secara parallel, maka komputer atau sistem pada *seller* harus dapat menjamin bahwa pengiriman pesan dilakukan secara serentak kepada semua *bidder*, hal ini penting sebagai bentuk perlakuan yang adil terhadap semua *bidder*.

## 4. KESIMPULAN

Peranan internet untuk mendukung bisnis pada saat ini sangatlah besar termasuk pada bisnis pelelangan *on-line*. Salah satu masalah atau tantangan yang harus dihadapi dalam menjalankan bisnis ini adalah menjaga tingkat keamanan (*security*) terutama untuk menghindari terjadinya penipuan yang dilakukan oleh *bidder*. Penipuan ini dapat diatasi dengan berbagai cara, salah satunya dengan mengaplikasikan *digital signature* untuk menjamin tidak terjadinya penyangkalan oleh bidder terhadap penawaran yang telah diberikannya.

Penerapan *digital signature* untuk setiap mekanisme pelelangan *on-line* dengan model *reverse* memiliki aturan yang berbeda (antara *cycle* dengan paralel memiliki aturan yang berbeda dalam penggunaan *digital signature*), karena proses pelelangan yang terjadi juga berbeda.

Secara keseluruhan, pemanfaatan *digital signature* dalam menjamin tidak akan terjadinya penipuan pada pelelangan *on-line* tidaklah cukup. *Digital signature* dan cara lainnya seperti audit penyelenggara bisnis untuk memberikan jaminan keamanan pada *bidder*, penyediaan informasi yang cukup, sistem *payment* yang baik juga merupakan komponen yang penting untuk mencegah terjadinya penipuan. Sebagai contoh, sebelum ikut dalam suatu sistem pelelangan *on-line*, seseorang harus yakin bahwa sistem yang diikutinya telah diaudit dan memberikan jaminan tidak akan melakukan penipuan. Karena, pada saat terjadinya pelelangan pemilik sistem pelelangan *on-line* bisa saja melakukan penipuan salah satunya dengan cara menciptakan *bidder-bidder* fiktif untuk meninggikan nilai tawar pada pelelangan.

Khusus untuk pembahasan mengenai aturan/protocol pada mekanisme paralel yang terdapat dalam makalah ini, penulis meyakini masih banyak terdapat kekurangannya. Salah satunya yang paling jelas adalah bahwa hal ini baru sebatas usulan dan belum disimulasikan dalam sistem pelelangan *on-line* yang sebenarnya. Sehingga penelitian masih harus terus dilakukan untuk mengembangkan usulan ini dan bahkan mungkin menerapkannya pada sistem pelelangan *on-line*.

Diantara peluang untuk penelitian lebih lanjut usulan ini adalah bagaimana mengatasi masalah ketika

koneksi internet antara *bidder* dengan *seller* terputus pada saat terjadi pelelangan yang disebabkan mungkin karena sistem di *bidder*/*seller crash*/rusak. Berikutnya adalah bagaimana mengatasi terjadinya kerusakan pada pesan ketika proses pengiriman sedang berlangsung (rusak di tengah jalan) baik dari *bidder* ke *seller* atau dari *seller* ke *bidder*.

Penulis terbuka untuk menerima usulan, ide atau hal lainnya berkaitan dengan perbaikan makalah ini. Dan tentunya penulis akan sangat berterima kasih karena hal tersebut bisa memberikan pengetahuan atau ilmu bagi penulis.

## DAFTAR REFERENSI


[1] Ir. Rinaldi Munir, M.T , "Diktat Kuliah IF5054 Kriptografi", Program Studi Teknik Informatika STEI ITB, 2006.

[2] Xun Yi, Chee Kheong Siew, "*Secure Agent-mediated Online Auction Framework*", *International Journal of Information Technology*, Vol 7 No 1.

[3] Dr. Subir Bandyopadhyay, Julie Wolfe, "*A critical review of online auction models* ", *Journal of the Academy of Business and Economics*, Jan 2004.

[4] "*Supplier Relationship Management : Integrating Suppliers into the e-Value Chain", Introduction to e-Supply Chain Management*.

[5] *International Working Group on Data Protection in Telecommunications*, "*Working Paper on Means and Procedures to Combat Cyber-Fraud in a Privacy-Friendly Way*", Pertemuan ke-36 di Berlin, 18-19 November 2004.

[6] Basem Shihada, "*Active Network Approach to the Design of Secure Online Auction Systems*", Dalhousie University, April 2001

[7] http://www.nowsell.com, "*Online Auction Business Model*", diakses 9 Desember 2007

[8] http://en.wipedia.org, "*Auction*", diakses 9 Desember 2007.