KEAMANAN WEB SERVICE PADA SITUS PENYEDIA BERITA XYZ MENGGUNAKAN WS-SECURECONVERSATION

Hastari Utama[1]

[1)] Staff Pengajar STMIK AMIKOM Yogyakarta
Jl Ring road Utara, Condongcatur, Sleman, Yogyakarta 55281
Email : utama@amikom.ac.id[1]

Abstrak

Pencapaian besar internet telah mengubah berbagai cara dalam melakukan sesuatu. Salah satu penggunaan internet adalah menyediakan berita. Berita ini dapat berupa berita. Berita dapat disajikan pada website oleh penyedia. Munculnya teknologi web service memungkinkan bagi penyedia berita untuk menjual layanan berita kepada pihak lainnya.

Penggunaan web service tersebut memungkinkan munculnya sejumlah ancaman yang akan mengganggu ketersediaan, kerahasiaan, dan integeritas data sehingga diperlukan adanya standar kemananan yang menanganinya. Salah satu dari standar keamanan dasar adalah WS-Security yang menggunakan standar enkripsi dan tanda tangan XML. Namun penggunaan WS-Security tersebut memiliki kekurangan saat terjadi pertukaran pesan dalam waktu yang lama karena setiap pesan harus ditandai. Solusi dari hal tersebut adalah penggunaan spesifikasi keamanan WS-SecureConversation. Konsep dasar WS-SecureConversation adalah membangun security context antara penyedia layanan dengan penggunanya.

Penelitian ini menghasilkan web penyedia berita yang diintegrasikan dengan web service untuk menjual layanan berita ke pelanggan. Web service yang diimplementasikan menggunakan spesifikasi WS-SecureConversation. Kemudian, web service tersebut dibandingkan dengan spesifikasi WS-Security dalam hal waktu proses request atau respon pesan. Proses request dan respon pesan dilakukan sebanyak 100 kali pada masing-masing spesifikasi keamanan. Hasil yang didapatkan adalah WS-SecureConversation memiliki waktu proses lebih rendah daripada WS-Security. Hal ini membuktikan bahwa dalam pertukaran pesan yang banyak, WS-SecureConversation memiliki waktu proses lebih rendah daripada WSSecurity.

Kata kunci:*Penyedia Berita, WS-Security, WS-SecureConversation, Security Context.*

1. Pendahuluan

Penggunaan internet dengan berbagai cara untuk keperluan yang bermacammacam semakin marak pada masa kini. Pencapaian besar internet dan world wide web telah mengubah berbagai cara yang tidak akan pernah mungkin terpikirkan hanya 20 tahun yang lalu [1]. Beberapa kegiatan yang berhubungan dengan internet seperti konsumen berinteraksi secara langsung dengan penjual, siswa mengikuti kelas online, dan perusahan bisnis beroperasi dengan suplier dan partner melalui aplikasi kantor dan pertukaran data dilakukan secara elektronik, serta pemerintah menyediakan layanan online secara langsung untuk pelayanan terhadap masyarakat. Kegiatan bisnis melalui internet sangat menguntungkan. Bahkan setelah munculnya teknologi lainnya yang mendukung seperti search engine, blog, social networking, web services dan sebagainya. Hal tersebut membuat kemudahan dalam mengakses informasi yang mendukung untuk berlangsungnya kegiatan bisnis. Implementasi dari web service tersebut merupakan dampak dari munculnya tren bisnis *virtual enterprise*. Istilah ini mengindikasikan bahwa, secara eksternal perusahaan melihat kenyataan kinerja semua proses bisnisnya tetapi dalam praktik hal tersebut tidak terjadi [2]. Hal ini memiliki maksud bahwa tidak semua proses bisnis dijalankan dalam satu perusahaan tetapi sebagian proses bisnis juga dijalankan partnernya. Banyak penyedia berita yang menerbitkan beritanya melalui internet dalm bentuk *website*. Hal ini dilakukan agar berita mudah diakses oleh siapa pun sehingga orang yang akan mengakses berita hanya mengunjungi website penyedia berita saja. Permasalahan muncul saat penyedia web lain ingin menyediakan berita pada *website*-nya sendiri. Penyedia web lain harus mencari berita untuk memenuhi hal tersebut tetapi membutuhkan waktu yang lama. Salah satu solusinya adalah penyedia berita menjual layanan berita dengan web service kepada penyedia web lain. Penyedia web lain dapat menggunakannya dengan cara berlangganan. Penyedia web lain menggunakan hal ini sebagai faktor untuk menaikkan rating web dan mengikat pengunjungnya. Dengan demikian, penyedia berita diuntungkan karena penjualan layanan berita tersebut melalui web service.

Penggunaan teknologi web service memungkinkan munculnya acaman dari pihak lain mengenai keamanan data dan informasi. Data dan informasi yang akan diakses tersebut sangat penting untuk dijaga integritas dan kerahasiannya. Salah satu langkah keamanannya adalah menggunakan *WS-Security* yang merupakan spesifikasi dasar penggunaan keamanan web service sesuai dengan kerangka kerja standar keamanan web service. *WS-Security* memiliki kekurangan ketika

penyedia web service dan penggunanya melakukan pertukaran pesan dalam jumlah yang relatif banyak [2]. Kekurangan tersebut adalah penandaan sejumlah besar data dengan kunci publik dipertimbangkan sebagai bentuk yang buruk dan mengurangi keamanan kunci.

Salah satu spesifikasi yang termasuk dalam *Web Services Standards Framework* yang dikeluarkan oleh perusahaan IBM dan Microsoft adalah *WS-SecureConversation*. Spesifikasi ini akan mengatur keamanan hubungan antara penyedia dan pengguna web service pada pertukaran pesan dengan menggunakan *security context*. Pada penelitian ini akan dibangun web penyedia berita sebagai penggambaran ide bisnis dalam penjualan layanan berita yang berbasis web service. Selain itu, sistem dibangun dengan spesifikasi keamanan menggunakan *WS-SecureConversation* untuk mengamankan pertukaran pesan dalam waktu yang lama antara penyedia layanan dan pelanggan.

Meninjau dari penelitian sebelumnya, ternyata penggunaan teknologi web service dapat diterapkan dalam bidang bisnis. Hal ini merupakan dampak dari tren bisnis yang disebut *virtual enterprise*. Salah satu contoh penerapan web service dalam bidang bisnis adalah integrasi aplikasi pemesanan tiket pesawat *online* dengan web service [3]. Layanan yang disediakan dalam web service akan digunakan agen perjalanan dalam menjual tiket pesawat secara online. Penggunaan web service akan memudahkan agen perjalanan dalam menjual tiket karena tidak perlu lagi membuat sistem penjualan yang baru. Kemudian, implementasi web service dalam bidang bisnis lainnya juga dapat diterapkan pada suatu toko online. Widjaja (2008) telah mengimplementasikan toko buku online berbasis web service. Keamanan yang diterapkan adalah enkripsi dan tanda tangan dengan metode Digital Right Management (DRM).

Penggunaan teknologi web service juga tidak lepas dari ancaman keamanan yang menyangkut aspek kerahasian, integritas, dan ketersediaan data. Salah satu spesifikasi keamanan yang untuk menagani ancaman tersebut adalah *username token*. Metode ini diterapkan oleh Rakhim (2010) dalam melakukan penelitiannya. Username token digunakan untuk otentifikasi pengguna layanan [4]. Penyedia layanan akan memvalidasi pesan request yang berisi token/penanda dengan username yang sesuai.

Username token juga dapat digunakan pada sistem manajemen pasien [5]. Fungsionalitas yang ada pada sistem manajemen pasien yaitu penjadwalan konsultasi pasien, mencatat informasi pasien, mencatat informasi dokter, dan mencatat resep obat yang diberikan dokter ke pasien. Layanan yang diintegrasikan dengan web service memuat fungsi-fungsi tersebut. Spesifikasi keamanan lainnya juga diterapkan yaitu otentifikasi HTTP (*Hypertext Transfer Protocol*) dengan SSL (*Secure Sockets Layer*) dan SAML.

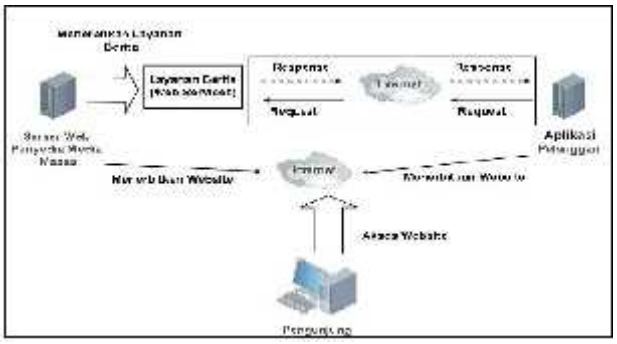
Penggunaan SAML (*Security Assertion Markup Language*) juga dapat dikombinasikan dengan spesifikasi keamanan XACML. XACML (*Extensible Access Control Markup Language*) adalah bahasa standar untuk menyatakan dan menukarkan kebijakan kontrol akses [6]. Hwang dkk. (2007) menggunakan kombinasi SAML dan XACML pada implementasi sistem delegasi. Sistem delegasi tersebut berada pada lingkungan komputasi pervasif. Pada sistem tersebut pengguna yang akan mengakses layanan pada penyedia web service harus melakukan otentifikasi dulu. Spesifikasi keamanan *WS-Security* juga diterapkan pada sistem ini untuk kerahasian dan integritas pesan.

WS-Security sendiri ternyata digunakan oleh *Apache Foundation* dalam mengembangkan sub proyek dibawah proyek WSS4J. Sub Proyek itu dinamakan *SecureZone* [7]. Fernando dkk. (2004) menggunakan *SecureZone* untuk mengimplementasikan *WS-SecureConversation* dan *WS-Trust*. *WS-SecureConversation* merupakan peningkatan dari *WS-Security* untuk pertukaran pesan yang banyak. Hasil pengujian penelitan ini menyatakan bahwa *WS-SecureConversation* memiliki waktu respon yang rata-rata lebih rendah dengan *WS-Security* pada pertukaran banyak pesan.

Pada penelitian ini digunakan beberapa metode secara prosedural. Beberapa metode penelitian tersebut adalah sebagai berikut:

a) Studi literatur. Tahap ini dilakukan dengan mencari dan mengumpulkan beberapa literatur.
b) Analisis. Tahap ini dilakukan dengan menganalisis masalah dan kebutuhan dari penelitian ini.
c) Perancangan. Hal ini terdiri dari dua tahap yaitu perancangan logikal dan fisik.
d) Implementasi. Tahap ini dilakukan dengan merealisasikan atau membangun rancangan sistem yang telah dilakukan.
e) Pengujian. Tahap ini dilakukan dengan menguji operasional data pada sistem. Kemudian melakukan pembandingan terhadap pesan SOAP baik pesan request atau respon yang menggunakan WS-SecureConversation dengan yang tidak.

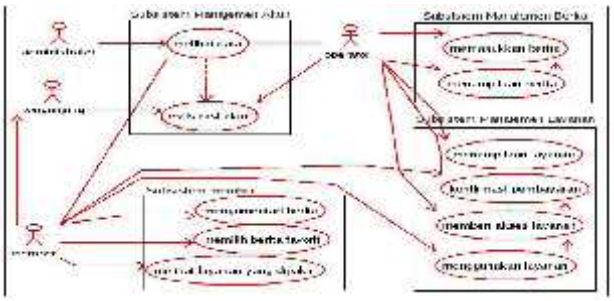
Penjelasan pada tahap analisis dan perancangan tersebut mencakup tentang analsis permasalahan sampai dengan rancangan antarmuka pengguna. Gambaran umum sistem yang dibangun adalah sesuai dengan gambar 1. Setelah arsitektur tersebut didefinisikan, langkah selanjutnya adalah mendokumentasikan kebutuhan dengan menggunakan *use case*. *Use case* merupakan urutan yang terhubung dari beberapa langkah (skenario) baik keduanya secara otomatis dan manual, untuk maksud melengkapi tugas bisnis tunggal [8].



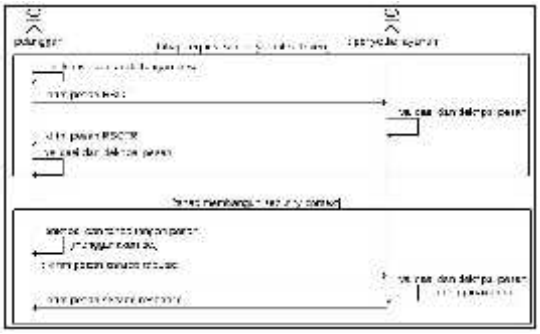
Gambar 1.*Gambaran umum sistem*

2. Pembahasan

Pada gambar 2 ditampilkan anlisis kebutuhan yang dideskripsikan pada use case. Proses membagun *security contex*t terdiri dari dua tahap pertukaran pesan. Tahap pertama adalah meminta *security context*. Saat pelanggan mengirimkan pesan *request security context token* (RSCT) ke penyedia layanan, penyedia layanan akan menerima pesan tersebut dan memvalidasi integritas pesannya. Kemudian, penyedia layanan mengirimkan pesan *request security context token response* (RSCTR) ke pelanggan sebagai balasan dari pesan RSCT yang telah disetujui oleh penyedia layanan. Pada pesan RSCT terdapat *security context token* yang akan digunakan oleh pelanggan untuk menghasilkan kunci enkripsi dan tanda tangan. Tahap kedua dalam proses membangun *security context* adalah menggunakan *security context token*. Pelanggan menggunakan *security context token* untuk mengenkripsi dan menandatangani pesan *service request* ke penyedia layanan. Proses dalam membangun *security context* tersebut ditampilkan pada Gambar 3.



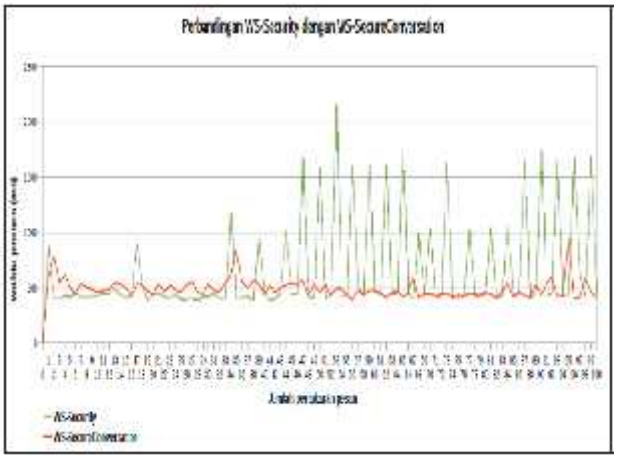
Gambar 2.*Use case diagram*



Gambar 3.*Membangun security context*

Setelah melakukan implementasi terhadap penyedia berita dan pelanggan paket layanan, langkah berikutnya adalah menguji layanan web services. Pengujian yang dilakukan dengan melihat pesan saat *request* dan *response*. Kemudian, membandingkan dengan penggunaan web services tanpa menggunakan spesifikasi keamanan *WS-SecureConversation*.

Pengujian yang telah dilakukan dengan spesifikasi keamanan menggunakan *WS-Security* dan *WS-SecureConversation* menghasilkan beberapa pesan SOAP (*Simple Access Object Protocol*) baik *service request* maupun *service response*. Dari pertukaran pesan tersebut memiliki beberapa perbedaan mekanisme. WS-Security hanya mengenkripsi dan menandatangani pesan kemudian dikirimkan ke pengguna layanan atau sebaliknya. Namun, *WS-SecureConversation* menggunakan enkripsi dan tanda tangan pesan untuk dua tahap pertukaran pesan yaitu *request/response security context token* dan *service request/response*. Selain perbedaan mekanisme yang telah dijelaskan tersebut terdapat perbedaan waktu proses dari kedua spesifikasi keamanan tersebut. Perbedaan waktu proses tersebut dapat diketahui dengan melakukan pengujian. Pengujian ini dilakukan dengan melakukan request terhadap aplikasi yang menggunakan web service menggunakan spesifikasi keamanan *WS-Security* dan *WS-SecureConversation*. Pengujian tersebut menggunakan aplikasi berbasis web dimana sebelumnya juga telah digunakan untuk mendapatkan data dari pertukaran pesan. Request dilakukan sebanyak 100 kali. Pada gambar 4 ditampilkan hasil dari perbandingan waktu proses antar kedua spesifikasi keamanan tersebut.



Gambar 4. *Perbandingan waktu proses WS-SecureConversation dan WS-Security*

Pesan yang terjadi baik menggunakan spesifikasi keamanan *WS-Security* atau *WS-SecureConversation* juga diterapkan enkripsi standar XML (*Extended Markup Language*). Paket algoritma yang digunakan tersebut telah didefinisikan pada konfigurasi *WS-SecurityPolicy*. Saat terjadi pertukaran pesan (pesan yang ditukarkan dapat berupa pesan *Request Security Context Token*, *Request Security Context Token*, *service request*, dan *service response*), pesan menggunakan

enkripsi standar XML. Jadi, semua pesan yang dikirimkan telah dienkripsi. Pesan yang terenkripsi tersebut memiliki kunci yang dihasilkan dari kunci klien secara acak. Kunci untuk mengenkripsi pesan yang akan dikirimkan tersebut juga dienkripsi dan diletakkan pada tag *EncryptedKey* sehingga pihak yang akan menyadap dan ingin membaca pesan harus mendekripsi kuncinya juga. Hal tersebut akan menyulitkan bagi pihak yang ingin membuka kerahasian pesan tersebut bahkan pada penggunaan spesifikasi *WS-SecureConversation*, *security context* akan menghasilkan dua kunci untuk enkripsi dan tanda tangan. Kerentanan keamanan pada kerahasian data bisa terjadi saat pihak lain mendapatkan kunci klien dari pelanggan yang sedang menggunakan layanan. Hal ini harus diperhatikan oleh pelanggan sendiri dalam menyimpan kunci klien yang diberikan oleh penyedia layanan. Penyedia layanan juga telah memberikan pengamanan pada kunci klien tersebut dengan menambahkan username dan password pada kunci klien yang diberikan melalui email pelanggan.

Pada pertukaran pesan dilakukan penandatangan pesan menggunakan tanda tangan standar XML. Pesan-pesan tersebut dapat berupa pesan *Request Security Context Token, Request Security Context Token, service request,* dan *service response*. Jadi, semua pesan yang dikirimkan telah ditandatangani. Pesan yang ditandatangani tersebut memiliki kunci yang dihasilkan dari kunci klien secara acak.

Pesan yang telah ditandatangani akan dijaga keamanannya. Hal ini telah diuji dimana mekanisme yang digunakan adalah melakukan penyadapan pada pertukaran pesan. Kemudian, pesan yang diambil diganti isi pesannya lalu dikirimkan ke alamat *endpoint* penyedia layanan. Penyedia layanan akan mengirimkan pesan *service response* yang berisi pesan *error*. Hal ini terjadi karena pesan yang telah ditandatangani tersebut akan dikomputasi kemudian dihasilkan nilai yang sesuai jika isi pesannya tepat.

Pengujian mengenai ketersedian data pada penyedia layanan dilakukan dengan melakukan akses terhadap layanan yang menggunakan kunci klien tidak sesuai. Penyedia layanan menerima pesan RSCT dari pengguna layanan lalu memvalidasi. Jika pesan tersebut tidak valid maka penyedia layanan akan mengirimkan pesan error *service response*. Hal ini juga berlaku jika pelanggan menggunakan kunci yang sesuai tetapi salah dalam memasukkan alias atau *password* kunci klien pada konfigurasi *WS-SecurityPolicy*. Hal itu terjadi karena penyedia layanan selalu memvalidasi pesan yang diterima.

3. Kesimpulan

Kesimpulan yang didapatkan dari penelitian ini adalah sebagai berikut:
1. Telah dibangun sistem penyedia berita berbasis web services menggunakan spesifikasi keamanan *WS-SecureConversation*. *Security context* dibangun oleh penyedia berita pada spesifikasi keamanan ini.
2. Hasil yang didapatkan setelah melakukan pengujian mengenai waktu proses *request* dan *respon* pesan adalah *WS-SecureConversation* memiliki waktu proses yang lebih rendah daripada *WS-Security* saat pertukaran pesan yang banyak.
3. Pengujian mengenai kerahasian menunjukkan pesan dalam keadaan terenkripsi dan rahasia. Selanjutnya, pengujian dengan aspek integritas menunjukkan bahwa sistem tidak akan memproses pesan yang telah dimodifikasi. Kemudian, pengujian mengenai aspek ketersediaan menunjukkan sistem menolak untuk melayani permintaan layanan sehingga ketersedian data hanya untuk pengguna yang sah.

Daftar Pustaka

[1] R. Hollar dan R. Murphy, *Enterprise Web services Security*, Hingham: Charles River Media, 2006.
[2] S. Weerawarana, F. Curberam, F. Leyman, T. Storey, dan D.F. Ferguson, *Web Services Platform Architecture: SOAP, WSDL, WS-Policy, WS-Addressing, WS-BPEL, WS-Reliable Messaging, and More*, Crawfordsville: Prentice Hall PTR, 2005.
[3] Salim, "Integerasi Aplikasi Pemesanan Tiket Pesawat Online Berbasis Web Services", *Tesis*, MIPA/Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta, 2009.
[4] T. Rakhim, "Keamanan Web Service Menggunakan Token, *Tesis*, MIPA/Ilmu Komputer", Universitas Gadjah Mada, Yogyakarta, 2010.
[5] S. Rajput, S. Vadivel, dan S.D. Shetty, "Design and Security Analysis of Web Application Based and Web Services Based Patient Management System (PMS)", *Int. J. of Computer Science and Network Security*,vol. 10, pp. 22-28, 3 Mar., 2010.
[6] H. Hwang, H.J. Ko, K.I. Kim, H.K. Lee, W. Kang, dan U.M. Kim, "A Safe Delegation Method for Web Services in Pervasive Computing Environments", *Int. J. of Computer Science and Network Security*, vol. 7, pp. 348-355, 1 Jan., 2007.
[7] R. Fernando, D. Leelarathne, M. Kaushalye, "A Framework for WSSecure-Conversation and WSTrust", *Int. Information Technology Conference*, 2004.
[8] L. Whitten dan L.D. Bentley, *System Analysis And Desaign Methods*, 7th edition, New York: McGraw-Hill Irwin, 2007

Biodata Penulis

Hastari Utama, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika STMIK AKAKOM Yogyakarta, lulus tahun 2009. Memperoleh gelar *Master of Computer Science* (MCs) Program Pasca Sarjana Ilmu Komputer Universitas Gajah Mada Yogyakarta, lulus tahun 2012.Saat ini menjadi Dosen di STMIK AMIKOM Yogyakarta dan dosen luar di AMIK Bina Sarana Informatika Yogyakarta.