IMPLEMENTASI SISTEM AUTENTIFIKASI TERINTEGRASI PADA DOMAIN CONTROLLER DAN APPLICATION SERVER LABKOM STIKOM SURABAYA

[1)]Diki Anggoro Putra [2)]Antok Supriyanto [3)]Kurniawan Jatmika

S1 / Sistem Informasi. Sekolah Tinggi Manajemen Informatika & Teknik Komputer Surabaya
Email : 1)dikigema@gmail.com 2)antok@stikom.edu 3)kjatmika@stikom.edu

Abstract: When the practice process begins, practitioner are able to access the PDC-Labkom system. But, at the same time, one computer can be used by the other practices. Problems that come on the surface are one computer can be worn for multiple accounts when accessing domain controller and there is no login managemet recording to actuate the practician's history.
Single sign on is a technology that granted the user's network for accessing rescources inside using one single account. They only need to authenticate once and then granted to access all the services on the network. For application services, the system is using web-service. Web-service is a bunch of logics application providing data and services for the application which used by it.
From that existing problems, the system have been bulit using web-service and SSO method as an integrated authentification at domain controller and application server on the practice system Labkom Stikom Surabaya. This SSO is a technology using the user and the password taken from login domain. And it can handle multi account security on the practice process. Furthermore, Labkom are able to record practitioner' histroy or mutli account for cheating history and login management safety.
Keywords : Practicum, Login, Single Sign-On

Praktikum adalah sebuah pembelajaran kuliah yang dilakukan di laboratorium komputer (Labkom) dan diharapkan dapat menerapkan ilmu yang telah didapat di pembelajaran kuliah di kelas (Mfatihhurrizqi, 2010). Praktikum di STIKOM merupakan mata kuliah (MK) dengan bobot sebesar 1 (satu) sks yang dimaksutkan untuk membekali mahasiswa mengaplikasikan ilmu dan pengetahuan yang diperoleh saat pembelajaran dikelas, melalui kegiatan praktikum ini mahasiswa dapat mengerti bagaimana cara mengaplikasikan konsep yang didapat dikelas dengan mempraktekkan pada saat di Labkom.

Selama proses praktikum, praktikan akan *log in application server* untuk dapat masuk ke dalam sistem praktikum. Namun praktikan dapat *log in* lebih dari satu *user* pada komputer dan sesi yang sama pada saat melakukan proses praktikum. Permasalahannya adalah 1 (satu) komputer pada sesi yang sama dapat multi *account* praktikan pada saat akses PDC-Labkom. Sehingga praktikan dapat membuka akses *login* PDC-Labkom yang bukan milik dirinya sendiri. Hal ini dapat mengakibatkan praktikan salah satunya dapat *download* jawaban milik temannya yang sudah di*upload*. Praktikan juga dapat membuka tes awal milik temannya, sehingga praktikan tersebut mengetahui soal tes awal lebih dulu dengan menggunakan *login* temannya. Saat ini Labkom belum dapat menangani masalah

multi *account* tersebut, sehingga praktikan dapat melakukan kecurangan-kecurangan multi *account* pada saat praktikum. Dengan adanya indikasi praktikan dapat melakukan multi *account,* nilai yang didapat oleh praktikan bisa dikatakan ada yang tidak murni dari hasil kerja sendiri, dan dibutuhkan sistem yang dapat menangani masalah multi *account* tersebut.

Salah satu metode yang dapat menangani multi *account* ini adalah *Single sign on*. Menurut Hursti Jani (1997), *Single sign on* (SSO) adalah teknologi yang mengizinkan pengguna jaringan agar dapat mengakses sumber daya dalam jaringan hanya dengan menggunakan satu akun pengguna saja. Dengan menggunakan SSO, seorang pengguna hanya cukup melakukan proses autentikasi sekali saja untuk mendapatkan izin akses terhadap semua layanan yang terdapat di dalam jaringan. Sistem SSO ini dapat diterapkan pula pada konsep *multitasking*, jadi meskipun praktikan membuka beberapa layar *browser* maka SSO ini dapat menanganinya. Keuntungan menerapkan SSO ini dapat meminimalisir *input user* dan *password* yang berulang-ulang dalam kurun waktu tertentu.

Berdasarkan latar belakang di atas, dibuat *web service* teknologi SSO sebagai sarana autentifikasi terintegrasi pada *domain controller* dan *application server* pada sistem praktikum Labkom STIKOM Surabaya. SSO ini merupakan teknologi yang dapat menggunakan *user* dan *password* yang diambil dari *login domain*. Data *user* dan *password* tersebut dapat digunakan untuk mengakses PDC-Labkom sehingga tes awal, tugas praktikum serta ujian praktikum tanpa memasukkan kembali *user* dan *password* kembali. Setiap praktikan hanya dapat *log in application server* di satu komputer untuk sesi tertentu. Dengan cara ini diharapkan dapat meminimalisasikan adanya kecurangan multi *account* praktikan pada saat melakukan kegiatan praktikum. Dengan adanya metode SSO ini, maka Labkom dapat meminimalisir kemungkinan praktikan akan melakukan kecurngan multi *account* pada saat praktikum. Karena SSO ini dapat berfungsi sebagai autentifikasi atau keamanan multi *account user* dan *password* yang hanya dapat digunakan oleh masing – masing praktikan STIKOM

Konsep Dasar Keamanan Informasi

Selama lebih dari 20 tahun, keamanan informasi telah dibangun atas 3 (tiga) kunci dasar dari prinsip kunci keamanan informasi yaitu : confidentiality (kerahasiaan), integrity (integritas), dan availability (ketersediaan) (Dani, 2008).

Gambar 1. CIA TRIAD

Confidentiality (kerahasiaan) berfokus pada upaya untuk menghindari pengungkapan secara tidak sah terhadap informasi yang bersifat rahasia maupun sensitif. Pengungkapan informasi tersebut dapat terjadi secara disengaja, seperti pemecahan sandi untuk membaca informasi, atau dapat terjadi secara tidak disengaja, dikarenakan kecerobohan dari individu dalam menangani informasi.

Dalam keamanan informasi, integrity (integritas atau keutuhan) berarti bahwa data tidak dapat dibuat, diganti, atau dihapus tanpa proses otorisasi. Dengan kata lain, integrity merupakan prinsip yang ditujukan untuk menjaga keakuratan suatu informasi.

Availability (ketersediaan) menjamin bahwa pengguna sistem yang berhak memiliki akses tanpa interupsi terhadap sistem dan jaringan. Hal tersebut memastikan bahwa informasi atau sumber daya akan selalu tersedia ketika dibutuhkan.

Kontrol Akses

Akses terhadap informasi yang dilindungi harus dibatasi kepada individu-individu yang berhak mengakses informasi tersebut. Program komputer, dan komputer yang memproses informasi juga harus dilindungi. Hal ini tentunya membutuhkan mekanisme pada tempatnya untuk mengontrol akses terhadap informasi yang dilindungi tersebut. Dalam implementasinya, mekanisme kontrol akses hendaknya seimbang dengan nilai informasi yang dilindungi. Fondasi dasar mekanisme kontrol akses dibangun atas mekanisme Identifikasi dan otentifikasi (Dani, 2008).

1. Identifikasi

Identifikasi merupakan pernyataan siapakah seseorang tersebut atau apakah sesuatu tersebut. Jika seseorang membuat pernyataan “Hello, my name is John Doe”, maka ia membuat klaim atas jati dirinya. Namun, klaim tersebut bisa berarti benar atau sebalikanya. Sebulum John Doe diberikan akses terhadap informasi yang dilindungi, maka akan menjadi penting untuk dipastikan bahwa seseorang yang mengklaim sebagai John Doe tersebut adalah benar John Doe (Dani, 2008).

2. Otenfikasi

Otentifikasi tidak lain adalah metode vervikasi atas identitas user, proses-proses, dan peranti-peranti (Rafiudin, 2005).

What a Person Knows (apa yang diketahui user)

What a Person Has (apa yang dimiliki user)

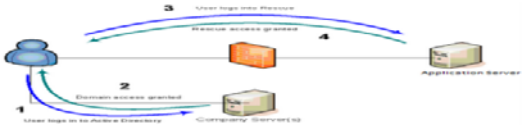
What a Person Is (Siapakah user)

3. Otorisasi

Otorisasi adalah pemberian hak (privilege) melalui perancangan utiliti spesial untuk akses layanan-layanan atau informasi spesifik bagi user atau grup user. Di lingkungan sistem-sistem yang sifatnya publik, otorisasi terbuka untuk user guest atau anonymous. Otorisasi tidaklah lain dari kunci untuk meyakinkan bahwa hanya user yang sah saja yang dapat mengakses informasi (Rafiudin, 2005).

Single Sign On (SSO)

Teknologi *Single-sign-on* (sering disingkat menjadi SSO) adalah teknologi yang mengizinkan pengguna jaringan agar dapat mengakses sumber daya dalam jaringan hanya dengan menggunakan satu akun pengguna saja. Teknologi ini sangat diminati, khususnya dalam jaringan yang sangat besar dan bersifat heterogen (di saat sistem operasi serta aplikasi yang digunakan oleh komputer adalah berasal dari banyak *vendor*, dan pengguna dimintai untuk mengisi informasi dirinya ke dalam setiap *platform* yang berbeda tersebut yang hendak diakses oleh pengguna). Dengan menggunakan SSO, seorang pengguna hanya cukup melakukan proses autentikasi sekali saja untuk mendapatkan izin akses terhadap semua layanan yang terdapat di dalam jaringan (Hursti, 1997).



Gambar 2. Arsitektur *single sign on*

Password

Password bisa diartikan sebagai suatu bentuk dari data otentifikasi rahasia yang digunakan untuk mengontrol akses ke dalam suatu sumber informasi. Password akan dirahasiakan dari mereka yang tidak diizinkan untuk mengakses. Selain itu, bagi mereka yang ingin mengetahui akses tersebut akan diuji, apakah layak atau tidak untuk memperolehnya. Walaupun demikian, password bukan berarti suatu bentuk kata-kata. Pasword yang tidak berbentuk kata dan memiliki suatu arti akan lebih sulit untuk ditebak. Password kadang-kadang digunakan juga dalam suatu bentuk yang hanya berisi angka (numeric), salah satu contoh adalah Personal Identification Number (PIN) (Malik, 2009).

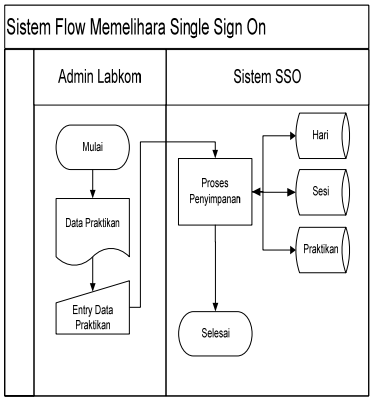
Web service

Web service merupakan kumpulan aplikasi logika yang menyediakan data dan *service* bagi aplikasi-aplikasi yang lain (Danny Ryan dan Tommy Ryan, 2002). Adapun aplikasi terdistribusi tersebut dapat diakses oleh aplikasi-aplikasi *client* tanpa memperhatikan sistem oprasi maupun bahasa pemongaraman. Sebelum adanya

web service terdapat teknologi CORBA dan OMG yang menggunakan bahasa Java dan DCOM dari *Microsoft.*

Alur Sistem

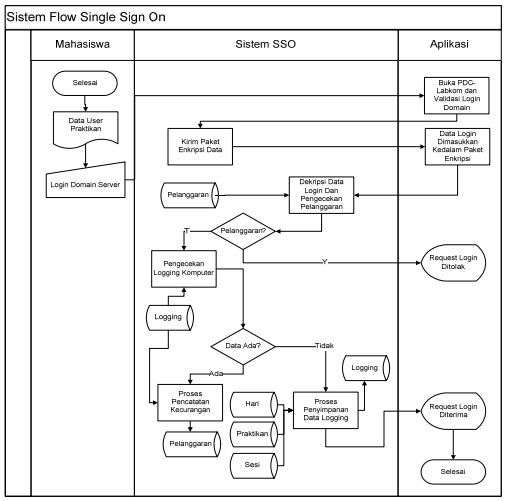
Diagram alir memelihara master berfungsi untuk mengelolah data master, baik menambah ataupun merubah data master terdapat pada Gambar 3.



Gambar 3. Diagram Alir Memelihara Master

System flow diawali oleh bagian admin Labkom melakukan maintance data login praktikan, hari dan sesi. Data login praktikan tersbut akan dibagikan pada setiap praktikan.

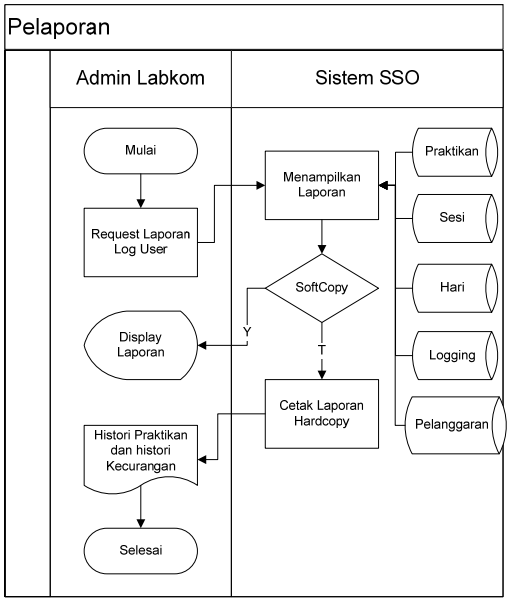
Diagram alir implementasi teknologi *single sign on* terdapat pada Gambar 4.



Gambar 4. Diagram Alir Implementasi Teknologi Single Sign On

Pada saat proses praktikum berlangsung, praktikan memasukkan data login berupa user dan password pada saat awal Windows. Dan jika data login benar, maka dapat masuk ke dalam Windows. Kemudian praktikan membuka sistem praktikum yang di sebut PDC-LABKOM. Pada saat PDC-LABKOM diakses, maka PDC-LABKOM akan meminta request login otomasis ke dalam web-servis. Web-servis akan menerima request tersebut dan akan mengirimkan enkirpsi data login ke PDC-LABKOM. PDC-LABKOM akan memasukkan data login Windows praktikan ke dalam paket enkripsi data tersebut yang kemudian akan dikirim kembali ke web-servis. Web-servis akan membuka paket enkripsi tersebut dengan dekripsi untuk dapat membuka paket enkripsi tersebut. Setelah data login didapatkan, maka web-servis akan memeriksa data login praktikan ada atau

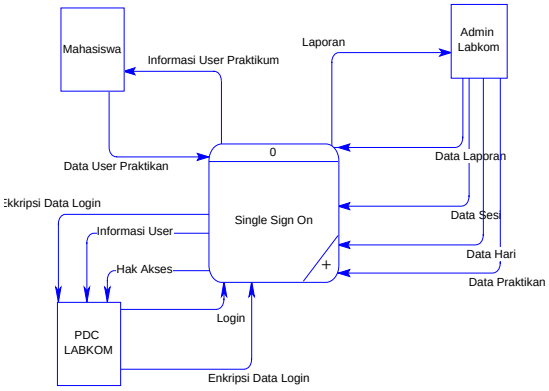
tidak di dalam database praktikan. Jika data ada maka praktikan akan menerima akses dapat masuk kedalam sistem PDC-LABKOM, yang kemudian data praktikan tersebut dimasukkan ke dalam database logging. Jika data login tersebut tidak ada didalam databse praktikan, maka sistem akan menolak data login praktikan tersebut dan sistem PDC-LABKOM tidak memperbolehkan praktikan masuk ke dalam sistem praktikum.Diagram alir membuat laporan terdapat pada Gambar 5.



Gambar 5. Diagram Alir Memelihara Master

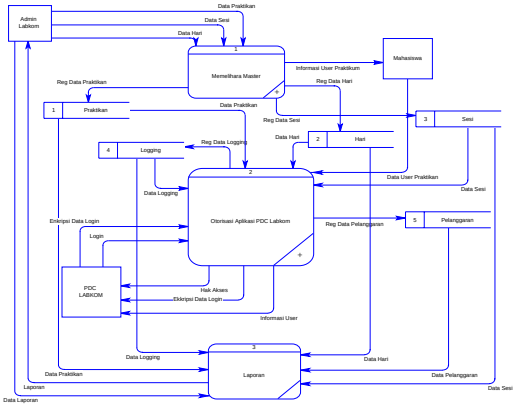
Context Diagram Implementasi Teknologi Single Sign On

Context Diagram ini kemudian didekomposisi ke level yang lebih rendah. *Context Diagram* implementasi teknologi *single sign on* akan dijelaskan pada Gambar 6.



Gambar 6. Context Diagram

Penjelasan lebih lengkap mengenai DFD Level 0 implementasi teknologi single sign on dapat dilihat pada Gambar7.

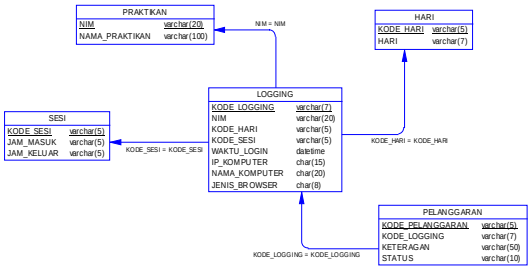


Gambar 7. DFD Level 0

1. Proses memelihara master berguna untuk mengelolah baik menambah ataupun merubah data master
2. Proses otorisasi aplikasi PDC-Labkom berguna untuk proses *single sign on*, dan dapat menentukan praktikan itu melakukan *dual* login atau tidak.
3. Laporan : porses ini berguna untuk menampilkan laporan dari sistem

PDM

Pada PDM *single sign on* ini memiliki 5 tabel (lima) tabel. seperti pada Gambar8.



Gambar 8. PDM Implementasi Teknologi *Single Sign On*.

Hasil dan Pembahasan

Pada saat program PDC-Labkom pertama kali dijalankan, maka web-service single sign on akan aktif dan mengambil data login awal pada windows. Web-service kemudian akan memeriksa data login praktikan tersebut, apakah praktikan dapat akses atau tidak untuk masuk kedalam sistem PDC-Labkom. Jika praktikan tersebut tidak terbukti melakukan kecurangan atau dual login, maka sistem PDC-Labkom akan dapat langsung diakses oleh praktikan Tampilan halaman utama seperti Gambar 9.

Gambar 9 Tampilan halaman utama (Praktikan)

Dan jika praktikan tersebut terbukti melakukan kecurangan atau dual login maka praktikan tidak dapat melakukan proses praktikum. Nim dari praktikan tersebut akan di tutup sampai admin Labkom membuka akses praktikan yang telah melakukan kecurangan. Tampilan praktikan yang tidak dapat akses masuk ke dalam sistem seperti pada Gambar 10.

Gambar 10 Tampilan halaman utama akses ditolak(Praktikan)

Kesimpulan

Kesimpulan yang dapat diambil dari pembuatan Implementasi *Single Sign On* sebagai sarana autentifikasi pada sistem praktikum (studi kasus : Labkom STIKOM Surabaya) adalah sebagai berikut:

1. Implementasi SSO telah mampu menangani kecurangan multi *account* praktikan di Labkom STIKOM Surabaya. Dengan adanya implementasi SSO ini praktikan hanya dapat *login* pada 1 komputer di hari, sesi, dan tanggal yang sama.
2. Sistem yang dibangun telah mampu melakukan pencatatan histori praktikan dan histori pencatatan pelanggaran Labkom STIKOM Surabaya. Admin Labkom dapat melihat laporan-laporan yang dapat

melihat praktikan yang melakukan kecurangan *multi account.*

3. *Web service* SSO telah mampu terintegrasi dengan PDC-Labkom dengan baik. *Web service* SSO akan ditaruh pada server Labkom, sehingga *client* Labkom yang menggunakan aplikasi PDC-Labkom dapat langsung mengakses *login* yang akan divalidasi oleh *web service* SSO.

Saran

Sistem dapat dikembangkan sebagai sarana autentifikasi untuk aplikasi lain yang ada di Labkom Surabaya, seperti aplikasi Hercules yang digunakan Labkom untuk sertifikasi dan aplikasi Poseidon yang digunakan Labkom untuk ujian UTS danUAS.

Daftar Pustaka

Dani, J. (2008). *Pengembangan Kebijakan Keamanan Informasi Pada Perusahaan Jasa Layanan Kurir*. Dipetik Januari 19, 2011, dari http://digilib.ui.ac.id/opac/themes/libri2/detail.jsp?id=126677&lokasi=lokal

Danny, R., & Tommy, R. (2002). *ASP.NET : Your Visual Blueprint for Creating Web Application on the .NET framework.* Inc: Hungry Mind.

Hursti, J. (1997). *Single Sign On.* Department of Computer Science Helsinki University Of Technology.

Malik, J. J. (2009). *Best Tools Hacking & Recovery Password.* Yogyakarta: C.V Andi Offset.

Rafiudin, R. (2005). *Konfigurasi Sekuriti Jaringan Cisco.* Jakarta: PT Elex Media Komputindo.