**LAPORAN AKHIR
PENELITIAN PENGEMBANGAN DOSEN**

**RANCANG BANGUN SISTEM *SINGLE IDENTITY*
INTEGRATION BERBASIS LDAP DI STMIK STIKOM
INDONESIA**

TIM PENELITI

IDA BAGUS ARY INDRA ISWARA, M.KOM. (0824048801)

I DEWA GEDE AGUNG PANDAWANA, S.KOM., M.Si. (0807038701)

PROGRAM STUDI TEKNIK INFORMATIKA
STMIK STIKOM INDONESIA
DENPASAR
DESEMBER 2016

HALAMAN PENGESAHAN

Judul Penelitian : Rancang Bangun Sistem *Single Identity Integration* Berbasis LDAP di STMIK STIKOM Indonesia

Bidang Penelitian : Teknik Informatika

Ketua Peneliti

Nama Lengkap : Ida Bagus Ary Indra Iswara, S.Kom., M.Kom.

NIDN : 0824048801

Program Studi : Teknik Informatika

Anggota Peneliti

Nama Lengkap : I Dewa Gede Agung Pandawana, S.Kom, M.Si.

NIDN : 0807038701

Program Studi : Teknik Informatika

Biaya yang disetujui : Rp. 3.325.000,-

Biaya yang digunakan : Rp. 3.325.000,-

Mengetahui,
Kepala Progam Studi
Teknik Informatika

Denpasar, 5 Desember 2016
Ketua Peneliti,

I Putu Gede Budayasa, SST.Par., M.T.I Ida Bagus Ary Indra Iswara, S.Kom., M.Kom
NIDN: 0820068402 NIDN: 0824048801

Menyetujui,
Kepala Lembaga Penelitian dan Pengabdian Masyarakat

Ida Bagus Ary Indra Iswara, S.Kom, M.Kom
NIDN: 0824048801

RINGKASAN

Teknologi saat ini berkembang seiring dengan cepatnya perkembangan manusia. Begitu juga dengan perkembangan aplikasi yang digunakan untuk menunjang pekerjaan manusia. Sistem maupun aplikasi yang diterapkan pada suatu instansi hampir semuanya menggunakan user dan password. Salah satu contoh aplikasi yang paling sering digunakan dalam interaksi di dunia digital adalah email, hotspot dan untuk menunjang perkuliahan institusi pendidikan juga menggunakan e-learning dalam proses belajar mengajar.

STMIK STIKOM Indonesia merupakan perguruan tinggi swasta yang sedang berkembang seiring dengan bertumbuhnya kesadaran akan pendidikan tinggi di masyarakat. Hal tersebut juga mempengaruhi dalam proses penggunaan user dan password pada setiap aplikasi yang tersedia di STMIK STIKOM Indonesia. Contoh aplikasi yang digunakan oleh mahasiswa, dosen dan karyawan di STMIK STIKOM Indonesia adalah Hotspot sistem, Email serta E-Learning.

Proses penggunaan user dan password secara terpisah memiliki kelemahan dari beberapa sisi salah satunya adalah waktu, untuk melakukan perubahan password dari aplikasi yang digunakan kita harus menghubungi administrator terkait, administrator juga terkadang memiliki pekerjaan yang harus diselesaikan. Maka dari itu hal ini merupakan kelemahan dari penerapan user dan password yang tidak terintegrasi di antara aplikasi yang ada.

Solusi untuk menjawab permasalahan tersebut adalah dengan membangun sebuah sistem yang mampu melakukan integrasi user dan password dari ketiga aplikasi yang ada. Sistem yang dibangun mampu melakukan proses integrasi user dan password untuk ketiga aplikasi yang ada pada STMIK STIKOM Indonesia. Maka dari itu dalam penelitian ini dibuat sebuah sistem *single identity integration* berbasis (*Lightweight Directory Access Protocol*) LDAP.

PRAKATA

Astung wara nugraha penulis panjatkan kehadapan Ida Sang Hyang Widi Wasa. yang telah melimpahkan rahmat-Nya sehingga penulis dapat berkarya untuk berpartisipasi dalam program Hibah Penelitian Pengembangan Dosen STIKI (PPDS) melalui penyusunan karya penelitian yang berjudul “ Rancang Bangun Sistem *Single Identity Integration* Berbasis LDAP di STMIK STIKOM Indonesia”.

Penulis menyadari bahwa proses penelitian ini tidak terlepas dari bantuan berbagai pihak. Oleh karena itu penulis mengucapkan terima kasih kepada:

1. I Dewa Made Krishna Muku, S.T., M.T, selaku Ketua STIKI;
2. I Putu Gede Budayasa, PTT.Par.,M.T.I selaku Kepala Program Studi TI;
3. I Dewa Gede Agung Pandawana, S.Kom., M.Si sebagai anggota tim penulis dalam penelitian ini
4. Para teman sejawat, sahabat dan keluarga yang telah memberikan semangat dan dorongan kepada penulis.

Penulis menyadari bahwa semua ini tidak lepas dari kekurangan, oleh karena itu penulis berharap kritik dan saran yang bersifat membangun dari pembaca guna kesempurnaan karya ini. Semoga karya penelitian ini dapat bermanfaat serta menambah pengetahuan bagi pembaca.

Denpasar, 5 Desember 2016

Penulis

DAFTAR ISI

HALAMAN SAMPUL	i
HALAMAN PENGESAHAN.....	ii
RINGKASAN	iii
PRAKATA.....	iv
DAFTAR ISI.....	v
DAFTAR TABEL.....	vii
DAFTAR GAMBAR	viii
DAFTAR LAMPIRAN.....	ix
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Luaran Penelitian.....	2
BAB 2 TINJAUAN PUSTAKA	3
2.1 Pengertian Sistem	3
2.2 Network Development Life Cycle	3
2.2.1 Analysis.....	4
2.2.2 Design	5
2.2.3 Simulation Prototype.....	6
2.2.4 Implementation	6
2.2.5 Monitoring	6
2.2.6 Management	7
2.3 LDAP (Light Weight Directory Access Protocol)	7
2.3.1 Konsep Dasar LDAP.....	8
2.3.2 Prinsip Kerja LDAP	11

BAB 3 TUJUAN DAN MANFAAT PENELITIAN	13
3.1 Tujuan Penelitian.....	13
3.2 Manfaat Penelitian.....	13
BAB 4 METODE PENELITIAN.....	14
4.1 Lokasi Penelitian	14
4.2 Alur Penelitian.....	14
4.3 Teknik Pengumpulan Data	14
4.3.1 Observasi.....	14
4.3.2 Studi Kepustakaan.....	15
4.4 Analisa dan Perancangan Aplikasi	15
4.4.1 Analisa Kebutuhan	15
4.4.2 Perancangan Sistem	15
4.4.3 Disain Sistem	16
BAB 5 HASIL DAN PEMBAHASAN.....	18
5.1 Implementasi Sistem	18
5.1.1 Implementasi Server LDAP Menggunakan Zimbra	18
5.1.2 Implementasi Server Penghubung dengan Freeradius	22
5.1.3 Implementasi Server Client.....	27
5.2 Pengujian Sistem Single Identity Integration	30
BAB 6 KESIMPULAN DAN SARAN	34
6.1 Kesimpulan.....	34
6.2 Saran	34
DAFTAR PUSTAKA	35

DAFTAR TABEL

Tabel 5.1. Skenario dan Hasil Pengujian Blackbox	30
--	----

DAFTAR GAMBAR

Gambar 2.1 Network Development Life Cycle	4
Gambar 2.2 Konsep Direktori LDAP.....	8
Gambar 2.3 Struktur Pohon Direktori Cara Penamaan Tradisional.....	10
Gambar 2.4 Koneksi dari <i>Client</i> ke <i>Server</i> LDAP Pertama dan Kedua.....	12
Gambar 4.1 Alur Penelitian.....	14
Gambar 4.2 Tahapan Perancangan Sistem.....	16
Gambar 4.3 Gambaran Umum Sistem	17
Gambar 5.1 Script instalasi aplikasi.....	19
Gambar 5.2 Tahap instalasi zimbra.....	19
Gambar 5.3 Konfigurasi Zimbra mail server	20
Gambar 5.4 Akhir Instalasi Zimbra Mail Server	20
Gambar 5.5 Konfigurasi DNS pada mikrotik	21
Gambar 5.7 Spesifikasi Server Freeradius	23
Gambar 5.8 Syntax install freeradius pada terminal	23
Gambar 5.9. Proses Instalasi Freeradius	23
Gambar 5.10. Syntax Install Utility Freradius	24
Gambar 5.11. Proses Instalasi Freeradius	24
Gambar 5.12. Konfigurasi file clients.conf.....	24
Gambar 5.13. Konfigurasi Radiusd.conf.....	25
Gambar 5.14. Konfigurasi module ldap.....	26
Gambar 5.15. Konfigurasi site-available	26
Gambar 5.16. Konfigurasi inner-tunnel	27
Gambar 5.17. Setting Radius Server	28
Gambar 5.18. Konfigurasi Server Hotspot.....	29
Gambar 5.19. Konfigurasi Radius Pada Server Hotspot.....	29
Gambar 5.20. Hasil Pengujian Login User	31
Gambar 5.21. Hasil gagal login user.....	31
Gambar 5.22. Hasil Pengujian radtest.....	32
Gambar 5.23. Hasil Pengujian freeradius -X	33

DAFTAR LAMPIRAN

Lampiran 1. Susunan Organisasi Tim Peneliti dan Pembagian Tugas	36
Lampiran 2. Biodata Ketua Tim Peneliti	37
Lampiran 3. Biodata Anggota Tim Peneliti	41

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Teknologi saat ini berkembang seiring dengan cepatnya perkembangan manusia. Begitu juga dengan perkembangan aplikasi yang digunakan untuk menunjang pekerjaan manusia. Sistem maupun aplikasi yang diterapkan pada suatu instansi hampir semuanya menggunakan user dan password. Salah satu contoh aplikasi yang paling sering digunakan dalam interaksi di dunia digital adalah email, hotspot dan untuk menunjang perkuliahan institusi pendidikan juga menggunakan e-learning dalam proses belajar mengajar.

Aplikasi tersebut sering digunakan oleh para karyawan, dosen dan bahkan mahasiswa. Terkadang dalam penggunaan aplikasi tersebut, sering kali para pengguna aplikasi mengalami kendala dalam hal mengingat user dan password yang digunakan. Hal ini disebabkan oleh berbedanya user dan password yang digunakan pada setiap aplikasi yang ada.

STMIK STIKOM Indonesia merupakan perguruan tinggi swasta yang sedang berkembang seiring dengan bertumbuhnya kesadaran akan pendidikan tinggi di masyarakat. Hal tersebut juga mempengaruhi dalam proses penggunaan user dan password pada setiap aplikasi yang tersedia di STMIK STIKOM Indonesia. Contoh aplikasi yang digunakan oleh mahasiswa, dosen dan karyawan di STMIK STIKOM Indonesia adalah Hotspot sistem, Email serta E-Learning. Ketiga aplikasi tersebut untuk saat ini belum bisa memiliki satu user dan satu password yang sama dan terintegrasi. Dengan kata lain masing-masing aplikasi tersebut mewajibkan kita memiliki user dan password yang hanya bisa di manage pada masing-masing aplikasi. Kemungkinan yang bisa terjadi dengan hal ini adalah lupa password dari salah satu aplikasi yang ada, misal kita melupakan user dan password Hotspot Sistem, maka pengguna harus menghubungi administrator Hotspot Sistem untuk melakukan penggantian user dan password.

Proses tersebut diatas memiliki kelemahan dari beberapa sisi salah satunya adalah waktu, untuk melakukan perubahan password dari aplikasi yang digunakan kita harus menghubungi administrator terkait, administrator juga terkadang

memiliki pekerjaan yang harus diselesaikan. Maka dari itu hal ini merupakan kelemahan dari penerapan user dan password yang tidak terintegrasi di antara aplikasi yang ada.

Solusi untuk menjawab permasalahan tersebut adalah dengan membangun sebuah sistem yang mampu melakukan integrasi user dan password dari ketiga aplikasi yang ada. Sistem yang dibangun mampu melakukan proses integrasi user dan password untuk ketiga aplikasi yang ada pada STIMIK STIKOM Indonesia. Maka dari itu dalam penelitian ini dibuat sebuah sistem *single identity integration* berbasis (*Lightweight Directory Access Protocol*) LDAP.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah pada penelitian ini adalah Bagaimana merancang dan membangun Sistem *Single Identity Integration* berbasis (*Lightweight Directory Access Protocol*) LDAP di STMIK STIKOM Indonesia?

1.3 Luaran Penelitian

Hasil penelitian ini akan dipublikasikan dalam bentuk publikasi ilmiah hasil penelitian yaitu pada Jurnal Ilmiah Teknik Informatika atau Sistem Informasi ber-ISSN. Dengan dipublikasikannya dalam suatu jurnal ilmiah, diharapkan hasil dari penelitian akan semakin valid dan reliable karena akan melalui suatu mekanisme assesment dari mitra bestari pada Jurnal Ilmiah yang bersangkutan. Diharapkan juga dalam publikasi tersebut akan menimbulkan dampak manfaat yang lebih luas karena pengetahuan (hasil penelitian) dapat diacu dan dimanfaatkan oleh masyarakat luas...

BAB 2

TINJAUAN PUSTAKA

2.1 Pengertian Sistem

Menurut (Hall, 2001) sebuah sistem adalah sekelompok dua atau lebih komponen yang saling berkaitan (*inter-related*) atau subsistem-subsistem yang bersatu untuk mencapai tujuan sama (*common purpose*). Menurut (O'Brien, 2005) sistem adalah sekelompok komponen yang saling berhubungan dan bekerja sama untuk mencapai tujuan bersama dengan menerima input serta menghasilkan output dalam proses transformasi yang teratur. Dalam bukunya (Jogiyanto, 2005) membagi definisi sistem menjadi dua pendekatan, yaitu pendekatan yang menekankan pada prosedurnya dan menekankan pada komponen atau elemennya. Pendekatan yang menekankan pada prosedur mendefinisikan sistem sebagai suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan, berkumpul bersama-sama melakukan kegiatan atau untuk menyelesaikan suatu sasaran tertentu. Pengertian sistem yang menekankan pada pendekatan elemen atau komponen, adalah kumpulan dari elemen-elemen yang berinteraksi untuk mencapai suatu tujuan tertentu.

Beberapa pengertian sistem tersebut dapat disimpulkan bahwa sistem adalah suatu prosedur dan atau komponen yang saling berkaitan melakukan kegiatan tertentu untuk mencapai tujuan atau sasaran tertentu.

2.2 Network Development Life Cycle

Model kunci di balik proses desain jaringan dikenal sebagai *Network Development Life Cycle* (NDLC) seperti digambarkan pada Gambar 2.1. Kata "cycle" adalah istilah deskriptif kunci dari siklus hidup pengembangan jaringan sebagai itu jelas menggambarkan sifat kontinyu pembangunan jaringan. Sebuah jaringan dirancang "dari awal" jelas harus dimulai di suatu tempat, yaitu dengan tahap analisis. Bagaimanapun, jaringan yang ada, terus mengalami kemajuan dari satu tahap ke tahap lainnya dalam NDLC (Bill, 2005).

Gambar 2.1 Network Development Life Cycle

2.2.1 Analysis

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan user, dan analisa topologi / jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya ;

- a. Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah / operator agar mendapatkan data yang konkrit dan lengkap. pada kasus di Computer Engineering biasanya juga melakukan brainstorming juga dari pihak vendor untuk solusi yang ditawarkan dari vendor tersebut karena setiap mempunyai karakteristik yang berbeda.
- b. survey langsung kelapangan, pada tahap analisis juga biasanya dilakukan survey langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap design, survey biasa dilengkapi dengan alat ukur seperti GPS dan alat lain sesuai kebutuhan untuk mengetahui detail yang dilakukan.
- c. membaca manual atau blueprint dokumentasi, pada analysis awal ini juga dilakukan dengan mencari informasi dari manual-manual atau blueprint dokumentasi yang mungkin pernah dibuat sebelumnya. Sudah menjadi keharusan dalam setiap pengembangan suatu sistem dokumentasi menjadi pendukung akhir dari pengembangan tersebut,

begitu juga pada project network, dokumentasi menjadi syarat mutlak setelah sistem selesai dibangun.

- d. Menelaah setiap data yang didapat dari data-data sebelumnya, maka perlu dilakukan analisa data tersebut untuk masuk ke tahap berikutnya. Adapun yang bisa menjadi pedoman dalam mencari data pada tahap analysis ini adalah ;
 - User / people : jumlah user, kegiatan yang sering dilakukan, peta politik yang ada, level teknis user
 - Media H/W & S/W : peralatan yang ada, status jaringan, ketersediaan data yang dapat diakses dari peralatan, aplikasi s/w yang digunakan
 - Data : jumlah pelanggan, jumlah inventaris sistem, sistem keamanan yang sudah ada dalam mengamankan data.
 - Network : konfigurasi jaringan, volume trafik jaringan, protocol, monitoring network yang ada saat ini, harapan dan rencana pengembangan kedepan.
 - Perencanaan fisik : masalah listrik, tata letak, ruang khusus, sistem keamanan yang ada, dan kemungkinan akan pengembangan kedepan.

2.2.2 Design

Dari data-data yang didapatkan sebelumnya, tahap Design ini akan membuat gambar design topology jaringan interkoneksi yang akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Design bisa berupa design struktur topology, design akses data, design tata layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang project yang akan dibangun.

Biasanya hasil dari design berupa ;

- a. Gambar-gambar topology (server farm, firewall, datacenter, storages, lastmiles, perkabelan, titik akses dan sebagainya)
- b. Gambar-gambar detailed estimasi kebutuhan yang ada

2.2.3 Simulation Prototype

Beberapa networker's akan membuat dalam bentuk simulasi dengan bantuan Tools khusus di bidang network seperti BOSON, PACKET TRACERT, NETSIM, dan sebagainya, hal ini dimaksudkan untuk melihat kinerja awal dari network yang akan dibangun dan sebagai bahan presentasi dan sharing dengan team work lainnya. Namun karena keterbatasan perangkat lunak simulasi ini, banyak para networker's yang hanya menggunakan alat Bantu tools VISIO untuk membangun topology yang didesign.

2.2.4 Implementation

Tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi networker's akan menerapkan semua yang telah direncanakan dan di design sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil / gagalnya project yang akan dibangun dan ditahap inilah Team Work akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis.

Ada beberapa Masalah-masalah yang sering muncul pada tahapan ini, diantaranya ;

- a. jadwal yang tidak tepat karena faktor-faktor penghambat,
- b. masalah dana / anggaran dan perubahan kebijakan
- c. team work yang tidak solid
- d. peralatan pendukung dari vendor

makanya dibutuhkan manajemen project dan manajemen resiko untuk meminimalkan sekecil

mungkin hambatan-hambatan yang ada.

2.2.5 Monitoring

Setelah implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan monitoring. Monitoring bisa berupa melakukan pengamatan pada ;

- a. Infrastruktur hardware : dengan mengamati kondisi reliability / kehandalan sistem yang telah dibangun (reliability = performance + availability + security),
- b. Memperhatikan jalannya packet data di jaringan (pewaktuan, latency, peektime,throughput)
- c. Metode yang digunakan untuk mengamati ”kesehatan” jaringan dan komunikasi secara umum secara terpusat atau tersebar

Pendekatan yang paling sering dilakukan adalah pendekatan Network Management, dengan pendekatan ini banyak perangkat baik yang lokal dan tersebar dapat di monitor secara utuh.

2.2.6 Management

Manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah Policy, kebijakan perlu dibuat untuk membuat / mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur Reliability terjaga. Policy akan sangat tergantung dengan kebijakan level management dan strategi bisnis perusahaan tersebut. IT sebisa mungkin harus dapat mendukung atau alignment dengan strategi bisnis perusahaan.

2.3 LDAP (Light Weight Directory Access Protocol)

LDAP (*Light Weight Directory Access Protocol*) adalah sebuah protokol yang mengatur mekanisme pengaksesan layanan direktori (*Directory Service*), yang dapat digunakan untuk mendeskripsikan banyak informasi seperti informasi tentang *people, organizations, roles, services* dan banyak entitas lainnya. LDAP menggunakan model *client-server*, dimana *client* mengirimkan identifier data kepada server menggunakan protokol TCP/IP dan server mencoba mencarinya pada DIT (*Directory Information Tree*) yang tersimpan di *server* (Carter, 2003). Bila ditemukan maka hasilnya akan dikirimkan ke *client* tersebut, namun bila tidak ditemukan maka hasilnya berupa pointer ke *server* lain yang menyimpan data yang dicari.

Terdapat dua layanan utama pada LDAP yaitu *slapd* yang merupakan LDAP *daemon* dan *slurpd* yang merupakan *replication daemon*. *Slapd* melayani

permintaan dari pengguna, *query* dan berkomunikasi dengan *database backend* sedangkan *slurpd* melayani replikasi data agar terus terjadi sinkronisasi data antara *client* dan *server*, dan untuk memfasilitasi pengisian dan perubahan informasi data dalam direktori digunakanlah LDIF (*LDAP Data Interchange Format*).

2.3.1 Konsep Dasar LDAP

Untuk mempelajari LDAP, sangatlah penting untuk memahami maksud dari direktori dan apa fungsinya. Direktori dapat berupa *personal address book*, *phone book*, *yellow pages* bahkan *web direktori* seperti Yahoo. Direktori dapat membantu untuk menemukan informasi yang dibutuhkan, sebagai contoh *yellow pages*. Di dalam *yellow pages* dapat dicari alamat lengkap, nomor telepon, alamat *website* dan *email* dari suatu perusahaan hanya dengan mencarinya berdasarkan ‘nama’ dari perusahaan yang telah disusun secara alfabetis pada direktori *yellow pages*. Dalam terminologi komputer, *directory service* bisa dikatakan sebagai suatu *database* tempat penyimpanan data, yang dapat digunakan untuk memberikan informasi-informasi yang berkaitan dengan objeknya. Bagian direktori mungkin dapat berisi kumpulan informasi tentang pengguna seperti *sure name*, *first name*, *phone number*, *User ID*, *mail address* dan lain sebagainya. Untuk memudahkan pemahaman tentang konsep direktori ini, dijelaskan melalui model seperti Gambar 2.2.

Gambar 2.2 Konsep Direktori LDAP

Secara prinsip struktur *database* pada suatu *directory service* adalah hierarki seperti yang ditunjukkan pada Gambar 2.2. Suatu *directory service* akan memiliki item yang dijadikan sebagai *root*. Untuk sebuah titik *root*, secara umum ditunjukkan dengan suatu atribut *dc* (*Domain Component*) atau *o* (*Organization*) mungkin juga *ou* (*Organization Unit*). Kemudian pada titik daun (*leaf*) biasanya akan berisi item dengan atribut *uid* (*User ID*) ataupun *cn* (*Common Name*). *Directory service* biasanya menyimpan informasi dalam bentuk struktur *tree* yang dinamakan *Directory Information Tree* (DIT). Setiap titik pada DIT diberi suatu alamat, baik secara relatif maupun secara absolut. Untuk suatu alamat relatif sering disebut sebagai RDN (*Relative Distinguish Name*) sedangkan alamat yang absolut disebut sebagai DN (*Distinguish Name*). Jadi apabila ingin mendapatkan informasi tentang pengguna rsukmana seperti contoh pada Gambar 2.2 diatas, dapat dituliskan hasil pencariannya dengan “dn=uid=rsukmana,ou=people,dc=smartbee,dc=com”. Konsep seperti inilah yang digunakan oleh direktori LDAP.

Ada tiga hal yang sebaiknya diketahui dalam membangun sebuah *server* LDAP (Arkills, 2003), yaitu:

1. **Schema** mendefinisikan seperangkat aturan yang mendeskripsikan jenis data apa saja yang akan disimpan, *schema* sangat membantu untuk menjaga konsistensi dan kualitas data sehingga mengurangi terjadinya duplikasi data.
2. **ObjectClass** merupakan sekumpulan entri yang menginformasikan jenis *group*, dan membutuhkan atribut yang biasanya terdiri atas *attribute names*, *attribute type* dan *attribute syntax* yang semuanya terkumpul dalam suatu data *valid* pada setiap kelasnya.
3. **Attribute** merupakan entri yang bersifat unik seperti *uid*, *cn*, *sn*, *ou*, *o*, *dc* dan lain sebagainya, attribute sendiri dapat merupakan *single value* maupun *multiple value*.

Model informasi LDAP adalah berdasarkan entri. Sebuah entri adalah koleksi atribut yang mempunyai nama yang terbedakan (*Distinguished Name/DN*) secara global. DN ini digunakan sebagai referensi ke entri yang secara unik berbeda dengan nilai DN yang lainnya. Setiap atribut entri mempunyai sebuah tipe dengan satu nilai atau lebih. Tipe biasanya string singkatan khusus, seperti “cn” untuk

common name, atau “*mail*” untuk alamat *e-mail*. Sintaks dari nilai bergantung kepada tipe atribut. Contoh, atribut *cn* mungkin berisi kata-kata “repo”. Atribut *mail* mungkin berisi alamat *email* “repo@server.com”.

Dalam LDAP entri direktori disusun dalam sebuah hirarki struktur seperti pohon (*tree*). Struktur pohon LDAP saat ini pada umumnya berdasarkan nama *domain* internet. Pendekatan penamaan layanan direktori mirip dengan penamaan pada DNS. Gambar 2.2 menunjukkan sebuah contoh pohon direktori LDAP menggunakan penamaan berdasarkan *domain*. Selain secara struktur pohon dengan penamaan internet, terdapat juga struktur pohon dengan cara penamaan tradisional seperti Gambar 2.3. Struktur ini merefleksikan geografis atau lingkup organisasi. Entri-entri mewakili negara-negara, terlihat di atas dari pohon (*tree*). Dibawahnya adalah entri yang menyatakan provinsi dan organisasi nasional. Dibawahnya lagi mungkin entri yang menyatakan unit organisasi, orang, printer, dokumen, dan lain-lain.

Gambar 2.3 Struktur Pohon Direktori Cara Penamaan Tradisional

LDAP dapat mengontrol atribut-atribut yang diperlukan dan diizinkan dalam sebuah entri, melalui penggunaan atribut spesial yang dinamakan *objectClass*. Angka-angka dari atribut *objectClass* menyatakan aturan (*rule*) skema yang ditaati oleh entri. Sebuah entri direferensi oleh nama yang berbeda dari yang lain, yang dibentuk dari nama entri itu sendiri. Nama ini disebut nama relatif yang membedakan (*Relative Distinguished Name/RDN*) dengan menggabungkan nama-nama dari entri-entri di atasnya atau sebelumnya. Operasi *update* yang ada, seperti

untuk menambah dan menghapus sebuah entri dari direktori, adalah mengubah entri yang ada dengan mengubah nama dari entri tersebut. Sebagian besar waktu LDAP digunakan untuk operasi mencari informasi dalam direktori (*query*). Operasi pencarian LDAP memungkinkan beberapa bagian dari direktori untuk mencari entri-entri yang sama dengan beberapa kriteria yang dispesifikasikan oleh *filter search*.

2.3.2 Prinsip Kerja LDAP

Secara teknis, LDAP adalah sebuah protokol untuk mengakses ke layanan direktori X.500, yang merupakan layanan direktori yang diatur oleh OSI. Awalnya, pengguna LDAP mengakses *gateway* ke layanan direktori X.500. *Gateway* ini menjalankan LDAP di antara *client* dan *gateway*, dan menjalankan Protokol Akses Direktori (*Directory Access Protocol/DAP*) X.500 antara *gateway* dan X.500 *server*. DAP adalah sebuah protokol kelas berat yang beroperasi melalui tumpukan protocol OSI secara penuh dan memerlukan pemrosesan yang sangat signifikan dari sumber daya komputasi. LDAP didesain untuk beroperasi melalui TCP/IP dan menyediakan sebagian besar dari fungsi DAP dengan biaya yang sangat lebih rendah.

LDAP adalah protokol yang digunakan untuk mengakses direktori X.500 *directory service* (OSI-nya layanan direktori). Inisialisasi LDAP *server* merupakan *gateway* antara LDAP dengan X.500 Directory Access Protokol (DAP), sedangkan DAP merupakan protokol *heavy-weight* yang mengoperasikan *stack* protokol OSI secara penuh, konsekuensinya tentu saja sangat menyedot *resource*. LDAP hadir dirancang menggunakan pendekatan protokol TCP/IP dikawinkan dengan fungsi-fungsi DAP sehingga fungsi DAP dapat dijalankan dengan lebih murah.

Dengan adanya fungsi-fungsi DAP pada LDAP, tentu saja sangat meringankan pengaksesan X.500, tetapi tetap saja diperlukan pemakaian layanan X.500 secara penuh untuk dapat membuat banyak data LDAP pada *client*. Sehingga tetap diperlukan *resource* yang besar untuk memenuhi keperluan tersebut. Service direktori LDAP berdasarkan model *client-server*. Satu atau lebih *server* LDAP membentuk pohon (*tree*) direktori informasi. *Client* terkoneksi ke *server* dan mengajukan pertanyaan. *Server* merespon dengan jawaban dan / atau dengan *pointer*, ke arah mana *client* dapat mendapat tambahan informasi (khususnya

keserver LDAP yang lain). Gambar 2.4 berikut menunjukkan proses koneksi dari *client* ke *server* LDAP pertama dan *server* LDAP kedua yang ditunjuk oleh *server* LDAP pertama.

Gambar 2.4 Koneksi dari *Client* ke *Server* LDAP Pertama dan Kedua

Tidak menjadi masalah pada *server* LDAP yang mana *client* akan terkoneksi. *Client* tersebut akan mendapat informasi yang sama dari *server* direktori berupa sebuah nama yang direpresentasikan ke satu LDAP *server* sebagai entri referensi yang akan menunjuk ke *server* LDAP lainnya. Ini ciri khas penting bagi layanan direktori global seperti LDAP.

Layanan direktori LDAP menyediakan proteksi keamanan yang dapat diatur pada saat pengguna akan melihat suatu informasi. Ketika pengguna melewati proses otentikasi atau *login*, pengguna yang tidak terotentikasi identitasnya, tidak memiliki izin untuk melihat informasi (tidak terotorisasi), sedangkan pengguna yang telah terotentikasi dapat melihat informasi sesuai dengan tingkatan otorisasi yang dimilikinya.

BAB 3

TUJUAN DAN MANFAAT PENELITIAN

3.1 Tujuan Penelitian

Tujuan yang ingin dicapai pada penelitian ini adalah merancang dan membangun Sistem *Single Identity Integration* berbasis (*Lightweight Directory Access Protocol*) LDAP di STMIK STIKOM Indonesia untuk menunjang kegiatan kampus.

3.2 Manfaat Penelitian

Manfaat penelitian ini terbagi menjadi dua yaitu manfaat akademis dan praktis sebagai berikut.

1. Manfaat Akademis

Metodologi yang digunakan dan hasil penelitian ini diharapkan memberikan suatu pemahaman tentang pemanfaatan *Network Development Life Cycle* dalam menganalisa dan merancang sebuah sistem yang berbasiskan jaringan komputer.

2. Manfaat Praktis

Hasil penelitian ini diharapkan dapat digunakan bagi pengelola perguruan tinggi beserta stakeholder untuk menjalankan proses bisnis yang terdapat pada sistem *single identity integration*. Agar penggunaan *user* dan *password* pada aplikasi yang diterapkan di STMIK STIKOM Indonesia terkelola dengan baik dalam satu wadah yang terstruktur.

BAB 4

METODE PENELITIAN

4.1 Lokasi Penelitian

Penelitian dilakukan di Kampus STMIK STIKOM Indonesia yang beralamat di Jalan Tukad Pakerisan No. 97 Denpasar Bali. Penelitian ini akan dilakukan selama 4 bulan.

4.2 Alur Penelitian

Penelitian dilakukan dengan merancang dan membangun aplikasi pengelolaan surat. Penelitian terbagi ke dalam beberapa langkah yang ditunjukkan seperti pada gambar 4.1

Gambar 4.1 Alur Penelitian

4.3 Teknik Pengumpulan Data

4.3.1 Observasi

Pengumpulan data dengan melakukan pengamatan langsung yang diawali dengan observasi deskriptif yaitu mengamati secara umum obyek penelitian terkait dengan sistem yang telah dijalankan, kemudian dengan observasi terfokus yaitu pengamatan dengan memfokuskan pada pokok-pokok permasalahan yang diteliti mengenai kendala yang dihadapi pada sistem, dan terakhir dengan observasi terseleksi yaitu menggabungkan kembali pokok-pokok permasalahan terhadap

obyek yang diteliti sehingga memperoleh gambaran yang jelas. Pada tahap ini dibantu pula dengan teknik pencatatan dan dokumentasi.

4.3.2 Studi Kepustakaan

Pengumpulan data dengan menggunakan beberapa buku atau literatur yang menjadi acuan atau landasan teori yang relevan dengan pembahasan masalah.

4.4 Analisa dan Perancangan Aplikasi

4.4.1 Analisa Kebutuhan

Dalam pembuatan Sistem *Single Identity Integration* diperlukan beberapa proses yang saling berhubungan. Sistem ini membutuhkan server, client dan penghubung dalam proses integrasinya. Adapun kebutuhan sistem yang dimaksud adalah sebagai berikut

- a. Server LDAP, kebutuhan server adalah untuk menampung database user dari Sistem *Single Identity Integration*. Server ini memiliki kemampuan untuk menjalankan LDAP dimana LDAP ini akan digunakan sebagai database user yang nantinya akan didistribusikan ke client melalui penghubung.
- b. Server Penghubung, Server ini bertugas sebagai perantara antara server LDAP dengan client. Server ini merupakan penerjemah atau protocol perantara yang mampu menyesuaikan protocol yang digunakan dari LDAP menuju ke jenis authentication client lainnya.
- c. Client, Client ini merupakan node terakhir dari sistem *single identity integration*, client yang dimaksud adalah sebuah server atau aplikasi yang memiliki proses *authentication*, pada penelitian ini penulis menggunakan mikrotik hotspot sebagai client yang menggunakan user yang ada pada LDAP Server.

4.4.2 Perancangan Sistem

Perancangan Sistem pada penelitian ini menggunakan *Network Life Cycle Development* (NDLC).

Gambar 4.2 Tahapan Perancangan Sistem

Seperti terlihat pada Gambar 4.2, pada tahapan perancangan ini, peneliti melakukan beberapa tahapan sebagai berikut :

1. Analisis
2. Disain
3. Simulasi
4. Implementasi
5. Monitoring
6. Manajemen

Tahapan perancangan yang diterapkan pada penelitian ini tidak menggunakan semua langkah-langkah dari NDLC, melainkan hanya menggunakan beberapa tahapan saja. Tahapan yang dilakukan dalam penelitian ini adalah Analisis, Disain, Implementasi. Hal ini dilakukan mengingat keterbatasan waktu dalam proses penelitian.

4.4.3 Disain Sistem

Disain Sistem yang dimaksud dalam implementasi sistem *single identity integration* adalah gambaran secara umum yang memperlihatkan cara kerja sistem secara keseluruhan. Gambaran umum ini diharapkan mampu memberikan bayangan dalam proses implementasi sistem. Adapun gambaran umum sistem *Single Identity Integration* bisa dilihat pada Gambar 4.3. Pada Gambar 4.3 menunjukkan bahwa sistem ini memiliki tiga node utama yaitu server LDAP, Server Penghubung dan Client.

Gambar 4.3 Gambaran Umum Sistem

Client yang terlihat pada Gambar 4.3 adalah client yang mempunyai proses authentication. Dalam hal ini client bias dalam bentuk aplikasi yang memiliki end user atau sebuah sistem yang memiliki beberapa jenis user. Penelitian ini menggunakan mikotik untuk dijadikan sebagai client. Mikrotik disini berfungsi sebagai penyuplay user untuk hotspot. Dimana user yang disebarkan ke hotspot adalah hasil dari user yang ada di LDAP Server. Jadi dengan kata lain user dan password yang ada pada LDAP Server akan sama dengan User yang digunakan untuk login di hotspot.

BAB 5

HASIL DAN PEMBAHASAN

Pada Bab ini diuraikan tahapan-tahapan penelitian yang dilakukan. Selain itu, juga dipaparkan penerapan skenario pengujian dan melakukan evaluasi dengan menganalisis hasil pengujian yang telah dilakukan. Hasil analisis disajikan pada bagian akhir dari Bab ini.

5.1 Implementasi Sistem

Tahapan implementasi sistem merupakan tahapan yang dilakukan untuk menguraikan tahap-tahap dalam implementasi masing-masing server yang digunakan pada gambaran umum sistem.

5.1.1 Implementasi Server LDAP Menggunakan Zimbra

Zimbra mail server diimplementasikan pada sebuah server yang menggunakan sistem operasi Ubuntu 16.04. Server tersebut memiliki arsitektur sesuai dengan gambar yang ditunjukkan.

Spesifikasi server yang digunakan:

- 1 X vCPU
- 1 GB VRAM
- 20 GB HDD - kontroler SCSI - thin provisioning
- CentOS sistem operasi 4/5/6
- VNIC E1000

Tahapan implementasi zimbra mail server secara terperinci disampaikan sebagai berikut:

5.1.1.1 Instalasi dan konfigurasi sistem operasi Ubuntu 16.04 pada server

Sebelum melakukan instalasi Zimbra mail server, terlebih dahulu dilakukan instalasi Ubuntu 16.04 pada server. Server yang digunakan merupakan server khusus (dedicated server) yang tidak diperuntukkan untuk sistem yang lainnya. Hasil dari tahap ini adalah sebuah sistem operasi Ubuntu 16.04 yang sudah terpasang pada server.

Setelah dilakukan instalasi dilanjutkan dengan konfigurasi Ubuntu 16.04server. Konfigurasi yang dilakukan meliputi pengaturan IP Address agar server dapat terkoneksi ke internet, pengarahan ke repository local untuk melakukan update dan instalasi software, dan melakukan instalasi tools remote sistem SSH agar bekerja pada server dapat dilakukan secara jarak jauh.

5.1.1.2 Instalasi dan konfigurasi Zimbra Mail Server

Pada tahap ini dilakukan instalasi dan konfigurasi Zimbra Mail server pada sistem operasi Ubuntu 16.04 yang telah berhasil diinstalasi pada server. Pada tahap pertama dilakukan instalasi aplikasi-aplikasi yang dibutuhkan oleh Zimbra mail server.

```
[Root @ zimbra ~] # apt-get install wget nano nc sudo  
sysstat libtool-ltdl glibc perl ntp
```

Gambar 5.1 Script instalasi aplikasi

```
Select the packages to install  
Install zimbra-ldap [Y]  
Install zimbra-logger [Y]  
Install zimbra-mta [Y]  
Install zimbra-snmp [Y]  
Install zimbra-store [Y]  
Install zimbra-apache [Y]  
Install zimbra-spell [Y]  
Install zimbra-memcached [N]  
Install zimbra-proxy [N]  
Checking required space for zimbra-core  
checking space for zimbra-store  
Installing:  
  zimbra-core  
  zimbra-ldap  
  zimbra-logger  
  zimbra-mta  
  zimbra-snmp  
  zimbra-store  
  zimbra-apache  
  zimbra-spell  
You appear to be installing packages on a platform different  
than the platform for which they were built.  
This platform is CentOS6_64  
Packages found: RHEL6_64  
This may or may not work.  
Using packages for a platform in which they were not designed for  
may result in an installation that is NOT usable. Your support  
options may be limited if you choose to continue.  
Install anyway? [N] y
```

Gambar 5.2 Tahap instalasi zimbra

Apabila semua aplikasi-aplikasi pendukung telah dilakukan instalasi maka zimbra mail server yang telah di-download kemudian dilakukan ekstrak untuk dapat dilakukan instalasi. Gambar 5.2 merupakan tahap instalasi zimbra yang dilakukan dan paket-paket software yang diinstalasi.

```

Main menu
1) Common Configuration:
2) zimbra-ldap:
3) zimbra-store:
   +Create Admin User:
   +Admin user to create:
   +Admin Password
   +Anti-virus quarantine user:
   +Enable automated spam training:
   +Spam training user:
   +Non-spam(Ham) training user:
   +SMTP host:
   +web server HTTP port:
   +web server HTTPS port:
   +web server mode:
   +IMAP server port:
   +IMAP server SSL port:
   +POP server port:
   +POP server SSL port:
   +Use spell check server:
   +Spell server URL:
   +Configure for use with mail proxy:
   +Configure for use with web proxy:
   +Enable version update checks:
   +Enable version update notifications:
   +Version update notification email:
   +Version update source email:
4) zimbra-mta:
5) zimbra-smtp:
6) zimbra-logger:
7) zimbra-spell:
8) Default Class of Service Configuration:
r) Start servers after configuration
s) Save config to file
x) Expand menu
q) Quit
Address unconfigured (**) items (? - help)

```

Gambar 5.3 Konfigurasi Zimbra mail server

Konfigurasi Zimbra mail server dilakukan pada saat proses instalasi berlangsung. Gambar 5.3 merupakan bagian konfigurasi zimbra mail server. Pada bagian tersebut menu-menu pada mail server dapat dilakukan konfigurasi menggunakan keyboard untuk melakukan pemilihan.

```

Moving /tmp/zmsetup.09202012-020042.log to /opt/zimbra/log
Configuration complete - press return to exit

```

Gambar 5.4 Akhir Instalasi Zimbra Mail Server

Pada akhir instalasi zimbra mail server, apabila instalasi berjalan sukses maka akan diperoleh tampilan seperti Gambar 5.4. Seluruh log yang berkaitan dengan Zimbra tercatat pada direktori /opt/zimbra/log.

5.1.1.3 Konfigurasi DNS (Domain Name System)

DNS merupakan sistem penamaan domain yang memungkinkan untuk mengarahkan nama domain ke sebuah IP Address. Hal ini bertujuan untuk memudahkan mengingat, karena manusia lebih mudah mengingat nama-nama daripada angka-angka. Domain yang digunakan untuk Zimbra Mail Server STIKI Indonesia adalah www.mail.stiki-indonesia.ac.id. Setiap akun akan memiliki alamat email dengan domain stiki-indonesia.ac.id, sebagai contoh : lppm@stiki-indonesia.ac.id

Gambar 5.5 Konfigurasi DNS pada mikrotik

Konfigurasi DNS dilakukan menggunakan mikrotik yang merupakan sebuah router yang digunakan pada Kampus STIKI Indonesia Denpasar. Pada Gambar 5.5 dapat dilihat domain www.mail.stiki-indonesia.ac.id diarahkan ke IP Address 172.16.80.8, IP Address 172.16.80.8 merupakan IP Address server yang digunakan sebagai mail server. Ketika terdapat user yang melakukan akses domain www.mail.stiki-indonesia.ac.id maka akan diarahkan ke IP Address Zimbra mail server yaitu 172.16.80.8. Karena sudah dilakukan instalasi Zimbra pada server

tersebut maka ketika akses dilakukan muncul halaman login dari Zimbra Mail Server STIKI Indonesia.

5.1.1.4 Hasil instalasi dan konfigurasi Zimbra Mail Server

Setelah dilakukan tahapan instalasi dan konfigurasi Zimbra Mail Server yang berjalan secara lancar, maka untuk menguji sistem yang dibuat kemudian dilakukan akses terhadap Zimbra Mail Server STIKI Indonesia melalui web browser. Gambar 5.6 merupakan tampilan awal zimbra mail server STIKI Indonesia. Pada tampilan ini user diminta memasukkan username dan password untuk bisa menggunakan email STIKI Indonesia.

Gambar 5.6 Tampilan Awal Zimbra Mail Server STIKI Indonesia

5.1.2 Implementasi Server Penghubung dengan Freeradius

Freeradius digunakan untuk melakukan proses penjembaran antara LDAP server dengan Client. Server Penghubung dengan menggunakan freeradius ini membutuhkan spesifikasi server seperti pada Gambar 5.7

Memory	1.00GB
Swap	512MB
CPU limit	2
CPU units	1024
Root Disk	local:103/vm-103-disk-1.raw,size=10G

Gambar 5.7 Spesifikasi Server Freeradius

Tahap-tahap instalasi secara detail akan dijelaskan pada langkah-langkah di sebagai berikut

5.1.2.1 Instalasi dan Konfigurasi Server Penghubung

Pada tahapan ini dilakukan proses instalasi dan konfigurasi freeradius. Instalasi freeradius dilakukan untuk membuat server penghubung antara LDAP Server dengan Client. Tahap pertama yang dilakukan ada instalasi freeradius dengan menjalankan perintah seperti pada Gambar 5.8.

```
[Root @ freeradius ~] # apt-get install freeradius
```

Gambar 5.8 Syntax install freeradius pada terminal

Setelah menjalankan perintah pada Gambar 5.8. selanjutnya akan muncul proses seperti pada Gambar 5.9.

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
freeradius-common freeradius-utils libfreeradius2 ssl-cert
Suggested packages:
freeradius-ldap freeradius-postgresql freeradius-mysql freeradius-krb5
The following NEW packages will be installed:
freeradius freeradius-common freeradius-utils libfreeradius2 ssl-cert
0 upgraded, 5 newly installed, 0 to remove and 70 not upgraded.
Need to get 1,069kB of archives.
After this operation, 4,235kB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

Gambar 5.9. Proses Instalasi Freeradius

Untuk mendukung koneksi antara freeradius dengan LDAP server diperlukan aplikasi penghubung atau aplikasi yang bisa menyamakan protocol antara LDAP dengan server Penghubung. Syntax untuk proses instalasi bisa dilihat pada Gambar 5.10 dan Gambar 5.11.


```
[Root @ freeradius ~] # apt-get install freeradius-ldap
```

Gambar 5.10. Syntax Install Utility Freradius

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
freeradius-ldap
0 upgraded, 1 newly installed, 0 to remove and 70 not upgraded.
```

Gambar 5.11. Proses Installasi Freeradius

Setelah melakukan installasi freeradius maka selanjutnya dilakukan tahapan konfigurasi freeradius agar bisa melakukan koneksi user antara LDAP server dengan server penghubung ini.

5.1.2.2 Konfigurasi Freeradius client

Freeradius merupakan aplikasi yang memiliki beberapa file konfigurasi yang digunakan untuk melakukan koneksi antara LDAP server dengan server penghubung. Dalam kasus ini akan dilakukan konfigurasi beberapa file yang terkait dengan koneksi LDAP Server. File yang perlu dikonfigurasi adalah client.conf, radius.conf, module ldap, dan site-available default.

```
[Root @ freeradius ~] # vim /etc/freeradius/clients.conf

client localhost {
    ipaddr = 127.0.0.1
    secret = secretkey
    nastype = other
}

client 172.16.80.0/24 {
    secret = secretkey
    nastype = other
}

client 188.8.88.0/21 {
    secret = secretkey
    nastype = other
}
```

Gambar 5.12. Konfigurasi file clients.conf

Konfigurasi yang paling pertama dilakukan adalah memastikan IP Client yang akan mengakses server penghubung. Dalam hal ini ip client yang akan melakukan koneksi dengan server penghubung adalah pada blok ip 172.16.80.0/24. Seperti terlihat pada Gambar 5.12, untuk mendaftarkan client yang bisa mengakses LDAP Server melalui server penghubung maka perlu dilakukan konfigurasi pada file *client.conf* yang terdapat pada */etc/freeradius/clients.conf*. Client yang didaftarkan adalah client yang berpeluang bisa menggunakan user yang ada di LDAP server.

```
[Root @ freeradius ~] # vim /etc/freeradius/radiusd.conf

prefix = /usr
exec_prefix = /usr
sysconfdir = /etc
localstatedir = /var
sbindir = ${exec_prefix}/sbin
logdir = /var/log/freeradius
raddbdir = /etc/freeradius
radacctdir = ${logdir}/radacct

name = freeradius

confdir = ${raddbdir}
run_dir = ${localstatedir}/run/${name}

db_dir = ${raddbdir}

libdir = /usr/lib/freeradius
pidfile = ${run_dir}/${name}.pid

user = freerad
group = freerad

max_request_time = 30
cleanup_delay = 5
```

Gambar 5.13. Konfigurasi Radiusd.conf

Tahap berikutnya adalah melakukan konfigurasi pada file *radius.conf*, konfigurasi file ini bertujuan untuk mendaftarkan service apa saja yang akan digunakan untuk melakukan koneksi ke LDAP server. Dalam penelitian ini service yang digunakan adalah service *ldap* yang berfungsi untuk memanggil data user yang ada pada LDAP server atau *zimbra* email server yang sudah di konfigurasi di

atas. Konfigurasi yang terlihat pada Gambar 5.13 adalah potongan konfigurasi dari radius.conf.

```
[Root @ freeradius ~] # vim /etc/freeradius/modules/ldap

1  ldap {
2    server = "mail.stiki-indonesia.ac.id"
3    port = "389"
4    basedn = "dc=mail,dc=stiki-indonesia, dc=ac,dc=id"
5    filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}}) "
6    ldap_connections_number = 5
7    timeout = 4
8    timelimit = 3
9    net_timeout = 1
10   dictionary_mapping = ${confdir}/ldap.attrmap
11   edir_account_policy_check = no
12   set_auth_type = yes
13 }
```

Gambar 5.14. Konfigurasi module ldap

Pada tahapan konfigurasi freeradius, file yang paling berperan adalah file dari module ldap yang ada pada /etc/freeradius/modules/ldap. Seperti yang terlihat pada Gambar 5.14. Konfigurasi yang harus diketahui adalah host dari server zimbra

```
[Root @ freeradius ~] # vim /etc/freeradius/sites-available/default

1  authorize {
2    ldap
3  }
4  authenticate {
5    Auth-Type LDAP {
6      ldap
7    }
8  }
9  preacct {
10 }
11 accounting {
12 }
13 session {
14   radutmp
15 }
16 post-auth {
17   exec
18   Post-Auth-Type REJECT {
19     attr_filter.access_reject
20   }
21 }
22 pre-proxy {
23 }
24 post-proxy {
25 }
```

Gambar 5.15. Konfigurasi site-available

yang merupakan server LDAP. Pada Gambar 5.14 dijelaskan host servernya adalah mail.stiki-indonesia.ac.id, dengan menggunakan port 389 yang merupakan default port dari LDAP server zimbra. Selain itu perlu juga di setting adalah basedn yang dimana basedn ini merupakan domain yang digunakan pada server zimbra. Selain konfigurasi tersebut setting juga set_auth_type = yes.

File yang dikonfigurasi selain site-available pada Gambar 5.15 dan inner-tunnel pada Gambar 5.16. pada kedua konfigurasi tersebut, yang perlu dilakukan adalah memastikan ldap sudah ada pada konfigurasi tersebut. Setting default dari kedua file ini tidak mengaktifkan service ldap. Service ldap yang perlu di aktifkan adalah authenticate type, authorise. Kedua service tersebut ada pada kedua file yang ada pada Gambar 5.15 dan Gambar 5.16.

```
[Root @ freeradius ~] # vim /etc/freeradius/sites-available/inner-tunnel

1  server inner-tunnel {
2  authorize {
3  ldap
4  }
5  authenticate {
6  Auth-Type LDAP {
7  ldap
8  }
9  }
10 session {
11 radutmp
12 }
13 post-auth {
14 Post-Auth-Type REJECT {
15 attr_filter.access_reject
16 }
17 }
18 pre-proxy {
19 }
20 post-proxy {
21 }
22 }
```

Gambar 5.16. Konfigurasi inner-tunnel

5.1.3 Implementasi Server Client

Tahap selanjutnya adalah tahapan konfigurasi pada Client. Pada kasus ini client yang digunakan adalah Mikrotik. Mikrotik merupakan alat yang serbaguna, mikrotik bisa difungsikan sebagai router, bandwidth management, firewall serta

hotspot authentication. Pada penelitian ini, fitur yang akan digunakan adalah hotspot authentication, yaitu management user yang digunakan untuk hotspot.

Konfigurasi yang dilakukan agar mikrotik bisa melakukan koneksi ke LDAP server kemudian menggunakan user yang ada pada LDAP server untuk koneksi ke hotspot, maka harus dilakukan beberapa tahapan konfigurasi sebagai berikut.

5.1.3.1 Konfigurasi Radius Server

Konfigurasi radius server pada mikrotik dilakukan dengan cara menyiapkan radius server yang ada pada mikrotik. Terlihat pada Gambar 5.17 konfigurasi yang dilakukan pada Gambar tersebut adalah konfigurasi untuk menentukan address dari radius server serta menentukan service yang bisa menggunakan radius server. Dalam penelitian ini radius server yang akan digunakan memiliki IP 172.16.80.9, dengan menggunakan secretkey. Maka yang perlu dilakukan adalah memastikan konfigurasi radius server pada mikrotik sudah sesuai dengan server freeradius yang sudah di setup sebelumnya.

Gambar 5.17. Setting Radius Server

Setelah melakukan konfigurasi seperti pada Gambar 5.17, selanjutnya adalah melakukan konfigurasi pada hotspot server profile di mikrotik yang ada pada *ip → Hotspot → Server Profile*. Konfigurasi yang perlu dilakukan adalah memilih

“login by” service, dalam hal ini karena kita menggunakan service CHAP dan PAP, maka centang *HTTP CHAP* dan *HTTP PAP*, serta centang *HTTPS* untuk mengaktifkan fitur keamanan. Konfigurasi tersebut bisa dilihat pada Gambar 5.18. setelah melakukan konfigurasi seperti pada Gambar 5.18 selanjutnya lakukan konfigurasi pada tab *RADIUS*, dan sesuaikan konfigurasi seperti pada Gambar 5.19. pada gambar tersebut terlihat “use RADIUS” diberikan tanda centang yang menandakan bahwa server hotspot akan menggunakan Radius dari server Penghubung untuk penggunaan user dari LDAP server.

Gambar 5.18. Konfigurasi Server Hotspot

Gambar 5.19. Konfigurasi Radius Pada Server Hotspot

5.2 Pengujian Sistem Single Identity Integration

Skenario pengujian pada penelitian ini menggunakan metode pengujian *blackbox testing*. Skenario pengujian dapat dilihat pada Tabel 5.1.

Tabel 5.1. Skenario dan Hasil Pengujian Blackbox

No.	Skenario Pengujian	Hasil Yang Diinginkan	Hasil Sistem	Keterangan Gambar
1.	Melakukan Login menggunakan User dan Password LDAP	Berhasil Login dengan munculnya status login	Valid	Gambar 5.20
		Tidak Berhasil Login dan Muncul Pesan Error	Valid	Gambar 5.20
2	Melakukan Pengujian Koneksi antara LDAP Server dan Server Penghubung dengan radtest	Berhasil menerima akses server	Valid	Gambar 5.22
3	Melakukan Pengujian LDAP Server dengan menggunakan freeradius -X	Berhasil menerima tes dengan memberikan status accept	Valid	Gambar 5.23

Pengujian yang dilakukan merujuk pada table 5.1, tahap pertama dalam pengujian sistem ini adalah melakukan pengujian pada end user, dimana pada pengujian ini dibuatkan satu user untuk pengujian yaitu user aryindraiswara@stiki-indonesia.ac.id pada server LDAP. User tersebut akan digunakan untuk login pada hotspot server pada mikrotik. Dengan server penghubung yang sudah dibuat diatas maka user yang di inputkan pada saat login di hotspot tidak perlu menggunakan @stiki-indonesia.ac.id, melainkan hanya menggunakan nama sebelum @ yaitu aryindraiswara. Seperti terlihat pada Gambar 5.20 user yang digunakan adalah aryindraiswara dan terlihat pada statusnya berhasil login dan bisa menggunakan layanan internet. Dengan kata lain hanya dengan membuat satu akun email @stiki-

indonesia.ac.id maka email tersebut langsung bisa digunakan untuk melakukan login pada hotspot sistem.

Gambar 5.20. Hasil Pengujian Login User

Gambar 5.21. Hasil gagal login user

Sedangkan untuk Gambar 5.21. muncul pesan error dikarenakan tidak ada respon dari RADIUS server atau server penghubung. Hal ini dikarenakan ada beberapa faktor, salah satu faktornya adalah usernya benar dan passwordnya salah, atau user tersebut belum terdaftar pada email server atau LDAP server. Selain itu penyebab error ini bisa juga diakibatkan karena terputusnya koneksi antara server

penghubung dengan LDAP server, yang mana akan menyebabkan request user dari client tidak terlayani dengan baik. Terputusnya koneksi ini biasanya disebabkan oleh gangguan teknis, seperti kabel putus, cuaca dll.

Setelah melakukan pengujian end user, selanjutnya dilakukan pengujian antara server penghubung dengan server LDAP. Pengujian pertama dilakukan dengan menggunakan aplikasi radtest. Seperti terlihat pada Gambar 5.22 radtest digunakan untuk melakukan pengujian ke server LDAP dengan mengirimkan beberapa parameter agar bisa diterima oleh server LDAP. Terlihat pada Gambar 5.22 pengujian menggunakan radtest berhasil, yang ditandai dari diterimanya parameter yang dikirimkan. Terlihat pada baris ke 7 Gambar 5.22.

```
1  [Root @ freeradius ~] # radtest porter ldap-password ps160
   secretkey
2  Sending Access-Request of id 37 to 172.16.80.8 port 1812
3  User-Name = "porter"
4  User-Password = "ldap-password"
5  NAS-IP-Address = 172.16.80.8
6  NAS-Port = 1812
7  rad_recv: Access-Accept packet from host 172.16.80.8 port
   length=20
```

Gambar 5.22. Hasil Pengujian radtest

Pengujian selanjutnya adalah pengujian untuk mengecek konfigurasi freeradius sekaligus juga mengecek koneksi dari server penghubung ke server LDAP. Pada Gambar 5.23 dilakukan pengujian dengan aplikasi freeradius dengan memberikan parameter -X. Hal ini digunakan untuk mengecek konfigurasi apakah sudah benar atau masih ada masalah. Pada Gambar 5.23 terlihat konfigurasi yang sudah dilakukan terlihat tidak ada masalah hal ini ditandai dari tidak adanya pesan error yang muncul pada hasil pengujian yang ditunjukkan Gambar 5.23. Selain mengecek hasil konfigurasi dari freeradius, pengujian ini juga bisa memperlihatkan koneksi yang dibuat apakah sudah nyambung dengan server LDAP atau belum. Terlihat pada Gambar 5.23 baris 5 dan baris 47, hasil dari output pengujian tersebut menunjukkan bahwa koneksi diterima dengan baik dan bisa digunakan untuk server penghubung dengan ip 172.16.80.8.

Ketika pengujian ini berhasil maka sistem sudah bisa digunakan dengan baik dan dapat digunakan pada client-client lainnya, seperti pada moodle atau aplikasi yang support dengan LDAP.

```
[Root @ freeradius ~] # freeradius -X

1      Listening on authentication address * port 1812
2      Listening on accounting address * port 1813
3      Listening on proxy address * port 1814
4      Ready to process requests.
5      rad_recv: Access-Request packet from host 172.16.80.8 port 55230, id=110, length=58
6      User-Name = "porter"
7      User-Password = "ldap-password"
8      NAS-IP-Address = 172.16.80.8
9      NAS-Port = 1812
10     +- entering group authorize {...}
11     ++[preprocess] returns ok
12     [ldap] performing user authorization for porter
13     [ldap]     expand: %{Stripped-User-Name} ->
14     [ldap]     ... expanding second conditional
15     [ldap]     expand: %{User-Name} -> porter
16     [ldap]     expand: (uid=%{Stripped-User-Name}:-%{User-Name}}) -> (uid=porter)
17     [ldap]     expand: dc=domain,dc=com -> dc=domain,dc=com
18     [ldap] ldap_get_conn: Checking Id: 0
19     [ldap] ldap_get_conn: Got Id: 0
20     [ldap] attempting LDAP reconnection
21     [ldap] (re)connect to ldap.domain.com:636, authentication 0
22     [ldap] setting TLS mode to 1
23     [ldap] bind as / to ldap.domain.com:636
24     [ldap] waiting for bind result ...
25     [ldap] Bind was successful
26     [ldap] performing search in dc=domain,dc=com, with filter (uid=porter)
27     [ldap] No default NMAS login sequence
28     [ldap] looking for check items in directory...
29     [ldap] looking for reply items in directory...
30     WARNING: No "known good" password was found in LDAP.  Are you sure that the user is conf
31     [ldap] Setting Auth-Type = LDAP
32     [ldap] user porter authorized to use remote access
33     [ldap] ldap_release_conn: Release Id: 0
34     ++[ldap] returns ok
35     Found Auth-Type = LDAP
36     +- entering group LDAP {...}
37     [ldap] login attempt by "porter" with password "ldap-password"
38     [ldap] user DN: uid=porter,ou=people,dc=domain,dc=com
39     [ldap] (re)connect to ldap.domain.com:636, authentication 1
40     [ldap] setting TLS mode to 1
41     [ldap] bind as uid=porter,ou=people,dc=domain,dc=com/ldap-password to ldap.domain.com:63
42     [ldap] waiting for bind result ...
43     [ldap] Bind was successful
44     [ldap] user porter authenticated successfully
45     ++[ldap] returns ok
46     +- entering group post-auth {...}
47     Sending Access-Accept of id 110 to 172.16.80.8 port 55230
48     Finished request 0.
49     Going to the next request
50     Waking up in 4.9 seconds.
```

Gambar 5.23. Hasil Pengujian freeradius -X

BAB 6

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Adapun yang bisa disimpulkan pada penelitian ini adalah sebagai berikut

1. Perancangan sistem *single identity integration* sudah berhasil dilakukan dengan menggunakan metode perancangan NDLC
2. Implementasi sistem *single identity integration* telah berhasil dengan menggunakan client mikrotik hotspot sistem.
3. Berdasarkan hasil pengujian, koneksi antara server LDAP, server Penghubung dan Client sudah berjalan dengan baik.

6.2 Saran

Saran yang dapat diberikan untuk pengembangan penelitian ini selanjutnya adalah sebagai berikut:

1. Pada penelitian berikutnya dapat dikembangkan ke sistem yang lebih besar seperti penggunaan login SISKAD.
2. Karena keterbatasan waktu penulis tidak bisa melakukan pengujian untuk sistem single sign on, maka hal ini menjadi peluang untuk bisa diteliti untuk penelitian berikutnya.

DAFTAR PUSTAKA

- Arkills, B., 2003. *LDAP Directories Explained: An Introduction and Analysis*. USA: Addison Wesley.
- Bill, B., 2005. The Network Development Life Cycle. In: s.l.:CSIS.
- Carter, G., 2003. *LDAP System Administration*. California, USA: O'Reily & Associates Inc.
- Hall, J. A., 2001. *Sistem Informasi Akuntansi*. Edisi Ketiga ed. s.l.:Salemba Empat.
- Jogiyanto, H., 2005. *Analisis dan Desain Sistem Informasi : Pendekatan Terstruktur Teori dan Praktik Aplikasi Bisnis*. Yogyakarta: Andi.
- O'Brien, J. A., 2005. *Pengantar Sistem Informasi*. Edisi Keduabelas ed. Jakarta: Salemba Empat.

Lampiran 1. Susunan Organisasi Tim Peneliti dan Pembagian Tugas

No.	Nama Lengkap / NIDN	Instansi Asal	Bidang Ilmu	Alokasi Waktu (Jam/Minggu)	Uraian Tugas
1.	Ida Bagus Ary Indra Iswara, S.Kom., M.Kom	STMIK STIKOM Indonesia	Teknik Informatika	16 Jam / minggu	Mendefinisikan masalah, menganalisis data dan melakukan pengujian sistem serta penyusunan laporan
2.	I Dewa Gede Agung Pandawana, S.Kom., M.Si.	STMIK STIKOM Indonesia	Sistem Informasi dan Komputer	16 Jam / minggu	Mendesain database, mendesain antarmuka dan programming serta penyusunan laporan

Lampiran 2. Biodata Ketua Tim Peneliti

A. Identitas Diri

1.	Nama Lengkap	Ida Bagus Ary Indra Iswara, S.Kom., M.Kom
2.	Jenis Kelamin	Laki-laki
3.	Jabatan Fungsional	Tenaga Pengajar
4.	NIK	1403210
5.	NIDN	0824048801
6.	Tempat dan Tanggal Lahir	Bangli, 24 April 1988
7.	E-Mail	aryindraiswara@gmail.com
8.	Nomor HP	081 805 468 408
9.	Alamat Kantor	Jl. Tukad Pakerisan 97 Denpasar, Bali
10.	Nomor Telepon/Faks	0361 - 256 995/ 0361 - 246 875
11.	Lulusan yang Telah Dihasilkan	30
12. Mata Kuliah yg Diampu	1. Struktur Data	
	2. Sistem Operasi	
	3. Jaringan Komputer	
	4. Komunikasi Data	
	5. Pengantar Teknologi Informasi	

B. Riwayat Pendidikan

	S-1	S-2
Nama Perguruan Tinggi	Universitas Udayana (UNUD)	Institut Teknologi Sepuluh Nopember (ITS)
Bidang Ilmu	Ilmu Komputer	Teknik Informatika
Tahun Masuk-Lulus	2006-2010	2011-2013
Judul Tugas Akhir/Tesis	Disain dan implementasi Internet Protocol Private Branch Exchange (IPPBX) dengan Menggunakan	Perbaikan Kinerja Zone Routing Protocol (ZRP) Pada MANET Dengan Menggunakan Metode

	Teknologi Voice over Internet Protocol (VoIP)	Signal Strength Based Link-Stability Sensing
Nama Pembimbing	1. Cokorda Rai Adi Pramartha, ST, MMSI 2. Drs. I Wayan Santiyasa, M.Si.	1. Wasktho Wibisono, S.Kom, M.Eng, Ph.D.

C. Pengalaman Penelitian Dalam 5 Tahun Terakhir

No.	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jml (juta Rp)
1	2014	Analisis Dan Implementasi Mail Server Berbasis Open Source Software Di Stmik Stikom Indonesia	Penelitian Pengembangan Dosen STIKI (PPDS)	Rp. 3.900.000,-
2	2015	Analisis Dan Desain Infrastruktur Jaringan Komputer Di Stmik Stikom Indonesia	Penelitian Pengembangan Dosen STIKI (PPDS)	Rp. 4.980.000,-

D. Pengalaman Pengabdian Kepada Masyarakat dalam 5 Tahun Terakhir

No.	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jml (juta Rp)
1.	2014	Website Pemasaran Kerajinan Akar Bambu	Institusi	Rp. 3.300.000,-

		untuk UKM Akah Bali di Kabupaten Bangli		
2.	2015	Pelatihan Microsoft Office & Jaringan Bagi Pegawai Negeri Sipil di Lingkungan Dinas Perhubungan Informasi dan Komunikasi Provinsi Bali	Institusi	Rp. 2.200.000,-
3.	2015	Pelatihan 40 Wanita Pelaku Home Industri Rumah Tangga Dalam Teknologi Informasi dan Komunikasi di Denpasar	Institusi	Rp. 5.000.000,-

E. Publikasi Artikel Ilmiah Dalam Jurnal dalam 5 Tahun Terakhir

No.	Judul Artikel Ilmiah	Nama Jurnal	Volume/Nomor/Tahun
1.	Pemilihan Node Tetangga yang Handal dengan Memperhitungkan Signal Strength dan Link Quality pada Zone Routing Protocol di Lingkungan MANET	Jurnal Ilmu Komputer Universitas Udayana	Volume VI No 2 tahun 2013

F. Pemakalah Seminar Ilmiah (*Oral Presentation*) dalam 5 Tahun Terakhir

No.	Nama Pertemuan Ilmiah/Seminar	Judul Artikel Ilmiah	Waktu dan Tempat

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggung jawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidak-sesuaian dengan kenyataan, saya sanggup menerima sanksi

Denpasar, 14 April 2016

Hormat saya,

A handwritten signature in black ink, appearing to read 'Ida Bagus Ary Indra Iswara', written over a horizontal line.

(Ida Bagus Ary Indra Iswara, M.Kom)

Lampiran 3. Biodata Anggota Tim Peneliti

A. Identitas Diri

1.	Nama Lengkap	I Dewa Gede Agung Pandawana, S.Kom., M.Si
2.	Jenis Kelamin	L
3.	Jabatan Fungsional	Asisten Ahli
4.	NIK	1002146
5.	NIDN	0807038701
6.	Tempat dan Tanggal Lahir	Denpasar, 7 Maret 1987
7.	E-Mail	vandawaa@yahoo.com
8.	Nomor HP	081805635519
9.	Alamat Kantor	Jl. Tukad Pakerisan 97 Denpasar, Bali
10.	Nomor Telepon/Faks	0361 - 256 995/ 0361 - 246 875
11.	Lulusan yang Telah Dihasilkan	S1 = 20 Orang
12. Mata Kuliah yg Diampu		a. Algoritma dan Pemrograman
		b. Struktur Data
		c. Sistem Informasi Geografi
		d. Pemrograman Dasar

B. Riwayat Pendidikan

	S-1	S-2
Nama Perguruan Tinggi	STMIK AKAKOM Yogyakarta	Universitas Udayanan Bali
Bidang Ilmu	Teknik Informatika	<i>Environmental Remote Sensing</i>
Tahun Masuk-Lulus	2005-2009	2010-2012

Judul Skripsi/Thesis	Aplikasi <i>Global Positioning System</i> Pada <i>Handphone</i> Menggunakan Java J2ME	Rainfall Diurnal Analysis Using Satellite Data : Case Study On Java Island and Surrounding
Nama Pembimbing	Sri Rejeki, S.Kom., M.Kom.	Prof. Ir. I Made Sudiana Mahendra, M.App,Sc., Ph.D

C. Pengalaman Penelitian Dalam 5 Tahun Terakhir

No.	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jml (juta Rp)
1.	2012	Sistem Pakar Diagnosa Awal Penyakit THT Dengan Metode <i>Certainy Factor</i> .	Institusi	1.500.000
2.	2013	<i>Rainfall Diurnal Analysis Using Satellite Data : Case Study On Java Island and Surrounding</i>	Institusi	2.000.000

D. Pengalaman Pengabdian Kepada Masyarakat dalam 5 Tahun Terakhir

No.	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jml (juta Rp)
1	2010	Pemberdayaan Masyarakat di Kelurahan Beng- Kabupaten Gianyar	Institusi	3.000.000
2.	2012	Pelatihan Microsoft Office dan Pemanfaatan Internet	Institusi	3.500.000
3.	2013	Rekapitulasi Hasil Pemilihan Umum Kepala Daerah Bali 2013 untuk Kabupaten Badung	Institusi	2.000.000

E. Publikasi Artikel Ilmiah Dalam Jurnal dalam 5 Tahun Terakhir

No.	Judul Artikel Ilmiah	Nama Jurnal	Volume/Nomor/Tahun
1.	Sistem Pakar Diagnosa Awal Penyakit THT Dengan Metode <i>Certainy Factor</i> .	Jurnal S@CIES	Vol:4, No. 1, April 2013,
2.	<i>Rainfall Diurnal Analysis Using Satellite Data : Case Study On Java Island and Surrounding</i>	<i>Proceedings of the 34th ACRS</i>	Vol. 1, No. 1, Oktober 2013

F. Pemakalah Seminar Ilmiah (Oral Presentation) dalam 5 Tahun Terakhir

No.	Nama Pertemuan Ilmiah/Seminar	Judul Artikel Ilmiah	Waktu dan Tempat
1.	34 th Asian Conference on Remote Sensing 2013	<i>Rainfall Diurnal Analysis Using Satellite Data : Case Study On Java Island and Surrounding</i>	Selasa, 22 Oktober 2013 di Hotel Kartika Plaza Nusa Dua - Bali

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidak-sesuaian dengan kenyataan, saya sanggup menerima sanksi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan Hibah Penelitian Dosen Pemula

Denpasar, 11-12-2016

Hormat Saya,

(I Dewa Gede Agung Pandawana, S.Kom., M.Si)