PEMBANGUNAN SISTEM MANAJEMEN KEAMANAN PADA SISTEM INFORMASI AKADEMIK (STUDI KASUS PADA STIKOM DINAMIKA BANGSA)

Sharipuddin S.Kom, M.Kom
STIKOM Dinamika Bangsa Jambi
Sharip_udin@yahoo.co.id

ABSTRAK

STIKOM Dinamika Bangsa Jambi merupakan perguruan tinggi swasta di Jambi yang didirikan pada tanggal 13 Mei 2002. Dalam operasional sehari-hari STIKOM Dinamika Bangsa termasuk salah satu pengguna teknologi informasi, khususnya di bidang akademik. STIKOM Dinamika Bangsa Jambi selalu berusaha untuk meningkatkan mutu, kinerja dan pelayanan terhadap para pengguna informasi dan teknologi. Dalam hal pengolahan data-data akademik seperti Kartu Rencana Studi (KRS), Kartu Hasil Studi, daftar absent, daftar ujian, daftar mata kuliah, jadwal mengajar dosen, dan daftar indek prestasi persemester sudah menggunakan sistem informasi akademik (SIAK), namun demikian keamanan sistem informasi akademik ini belum termanajemen dengan baik. Melalui tulisan ini penulis mencoba untuk membangun manajemen keamanan pada sistem informasi akademik yang tujuannya adalah memberikan hak akses kepada para user sesuai dengan fungsi dan jabatanya masing-masing.

Kata Kunci : Sistem, Informasi, Akademik, Sekuriti

ABSTRACT

STIKOM DB Jambi is a privates college in Jambi. STIKOM on Mei, 13 in 2002. In daily operational. STIKOM DB is before to one of information technology by user. In particular academic side. STIKOM DB always tries to increase the quality, ability and serves to user information and technology. In academic data processing. Such as study plan card, study result card, absent list, exam list, lesson list. The schedule of lecturer teaching, and the list of achievement index in each semester has used academic information system, however the security academic information system hasn't menage well yet. Through this writing, writer tries to build security management in academic information system. The goal glues right access for user with their appropriate function (purpose) and each their position.

Keyword : System, Information, Academic, Security

I. PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi adalah suatu teknologi yang digunakan untuk mengolah data, termasuk memproses, mendapatkan, menyusun, menyimpan dan mengolah data dalam berbagai cara untuk menghasilkan informasi yang berkualitas, yaitu informasi yang relevan, akurat dan tepat waktu yang nantinya dapat digunakan baik untuk keperluan pribadi, bisnis, pemerintahan dan pendidikan yang merupakan informasi yang strategis untuk pengambilan keputusan.

Sebagai salah satu perguruan tinggi yang sedang berkembang STIKOM Dinamika Bangsa terus berupaya untuk kualitas pelayanan Informasi Akademik. Salah satu upaya yang dilakukan adalah dengan membangun Sistem Informasi Akademik. Sistem Informasi Akademik yang dibangun berbasis web dan dapat diakses secara on-line melalui internet. Melalui layanan ini diharapkan mampu untuk membantu pihak akademik, calon mahasiswa, mahasiswa dan dosen dalam mendapatkan informasi akademik secara cepat, kapan saja dan terbaru.

Agar Sistem Informasi Akademik ini dapat berjalan dengan baik tentunya harus didukung oleh infrastruktur yang memadai serta memiliki manajemen dan tingkat keamanan yang tinggi. Permasalahannya yang ada saat ini, meskipun Sistem Informasi Akademik Kemahasiswaan di STIKOM telah didukung oleh infrastruktur yang baik namun dari sisi manajemen Sistem Informasi Akademik

STIKOM Dinamika Bangsa belum mempunyai manajemen keamanan yang baik. Untuk itu perlu dilakukan sebuah pembangunan sistem manajemen keamanan pada Sistem Informasi Akademik

1.2 Perumusan Masalah

Agar didapatkan sebuah hasil pembangunan sistem manajemen keamanan pada Sistem Informasi Akademik maka perlu dirumuskan permasalahan sebagai berikut,
Bagaimana pembangunan menajemen keamanan pada pada Sistem Informasi Akademik STIKOM Dinamika Bangsa Jambi dengan menerapkan access control.

1.3 Tujuan Penelitian dan Manfaat Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini adalah :

1 Membangun sistem manajemen keamanan Sistem Informasi Akademik
2 Untuk menghasilkan suatu bentuk pengembangan Sistem Informasi Akedemik dengan menggunakan Pembangunan Sistem Manajemen Keamanan pada Sistem Informasi Akademik
3 Dari hasil pembangunan sistem manajemen keamanan yang dilakukan diharapkan dijadikan acuan dalam meningkatkan keamanan pada Sistem Informasi Akademik tersebut.

1.4 Pembatasan Masalah

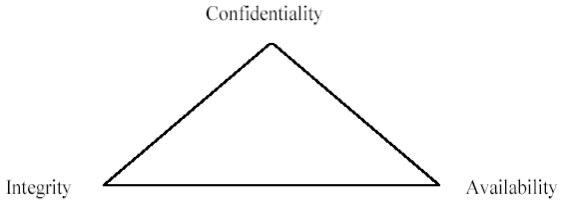
Untuk mendapatkan hasil penelitian yang baik dan terarah perlu dilakukan beberapa pembatasan masalah agar penyusunan tesis ini tidak menyimpang dari tujuan dan sasaran yang hendak dicapai. Batasan yang deberikan oleh peneliti dalam penelitian ini adalah :

Pembangunan Sistem Manajemen Keamanan pada Sistem Informasi Akademik dengan menerapkan akses kontrol dan manajemen keamanan data.

1.5 Aspek-Aspek Keamanan Sistem Informasi

Domain keamanan sistem informasi menggabungkan identifikasi dari aset data dan informasi suatu organisasi dengan pengembangan dan implementasi kebijakan-kebijakan, standar-standar, pedoman-pedoman, dan prosedur-prosedur.

Di dalam domain Keamanan Sistem informasi dikenal tiga buah konsep yakni *Confidentiality*, *Integrity*, dan Availibility (C.I.A.), seperti yang ditunjukkan oleh Gambar 1.5 Ketiga konsep ini mewakili tiga prinsip fundamental dari keamanan informasi. Seluruh kendali-kendali keamanan informasi, dan upaya-upaya perlindungan, serta semua ancaman-ancaman, dan proses keamanan mengacu pada ukuran CIA.



Gambar C.A.I (Irma I. Ibrahim, Wisnu P. Prabowo , Tommy Lukman,2005)

1.5.1 *Confidentiality (* Kerahasiaan)

Inti utama aspek *privacy* atau kerahasiaan adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih kearah data-data yang sifatnya pribadi sedangkan kerahasiaan biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah layanan) dan hanya diperbolehkan untuk keperluan tertentu. Contoh hal yang berhubungan dengan *privacy* adalah e-mail seorang pemakai (*user*) tidak boleh dibaca oleh administrator. Contoh informasi yang bersifat rahasia adalah data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) merupakan data-data yang ingin diproteksi penggunaan dan penyebarannya. Contoh lain dari kerahasiaan adalah daftar pelanggan dari sebuah *Internet Service Provider* (ISP).

Konsep kerahasiaan berupaya untuk mencegah terjadinya penyingkapan yang tidak sah secara disengaja maupun tidak disengaja terhadap isi dari suatu pesan. Hilangnya kerahasiaan dapat terjadi dengan berbagai cara, seperti melalui keluarnya informasi rahasia perusahaan secara sengaja atau melalui penyalahgunaan hak-hak jaringan.

1.5.2 *Integrity* (Keutuhan)

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi. Sebuah e-mail dapat saja "dicegat" (*capture*) di tengah jalan, diubah dan dimodifikasi isinya, kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan *enkripsi* merupakan salah satu cara yang dapat mengatasi masalah ini.

1.5.3 *Availability* (Ketersediaan)

Aspek ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan istilah server tidak dapat memberikan layanan ketika dibutuhkan (*denial of service attack*), dimana server dikirimi permintaan layanan (biasanya palsu) yang bertubi-tubi atau permintaan layanan yang di luar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai terganggu atau mengalami kerusakan.

1.6 Dasar-Dasar Keaman Data

1.6.1 Pengertian Kriptografi

Kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata Crypto dan Graphia yang berarti penulisan rahasia. Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. (Maman Abdurohman, 2002)

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, ciphertext tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali.

Proses tranformasi dari plaintext menjadi ciphertext disebut proses *Encipherment* atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali ciphertext menjadi plaintext disebut proses dekripsi (*decryption*).

Untuk mengenkripsi dan mendekripsi data. Kriptografi menggunakan suatu algoritma (*cipher*) dan kunci *(key*). Cipher adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi data. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data.

Proses tranformasi dari plaintext menjadi ciphertext disebut proses *Encipherment* atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali ciphertext menjadi plaintext disebut proses dekripsi (*decryption*).

Secara umum operasi enkripsi dan dekripsi dapat diterangkan secara matematis sebagai berikut :

$$EK(M) = C \quad \text{(Proses Enkripsi)}$$
$$DK(C) = M \quad \text{(Proses Dekripsi)}$$

Pada saat proses enkripsi kita menyandikan pesan M dengan suatu kunci K lalu dihasilkan pesan C. Sedangkan pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya.

Algoritma Kriptografi

Berdasarkan kunci yang dipakai, algoritma kriptografi dapat dibedakan atas dua golongan, yaitu :

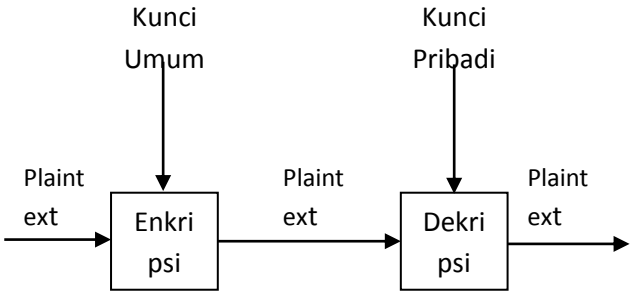
a. Symmetric Algorithms

Algoritma kriptografi simeteris atau disebut juga algoritma kriptografi konvensioanl adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi.

b. Asymmetric Algorithms

Algoritma kriptografi nirsimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma ini disebut juga algoritma kunci umum (*public key)*

algorithm) karena kunci untuk enkripsi dibuat umum (*public key*) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi (*private key*). Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA dan ECC.



Gambar 2.3 Proses Enkripsi/Dekripsi Public Key Cryptography
Sumber**:**(Maman Abdurohman, 2002)

***Access Control* (pengontrolan akses)**

Salah satu cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme otentikasi dan pengaturan akses. Implementasi dari mekanisme ini antara lain dengan menggunakan *"password".* Setelah proses otentikasi pemakai diberikan akses sesuai dengan level yang dimilikinya melalui sebuah pengintrolan akses. Pengontrolan akses ini biasanya dilakukan dengan mengelompokkan pemakai dalam suatu group. Ada group yang berstatus pemakai biasa, ada tamu, dan ada juga administrator atau super uses yang memiliki kemampuan lebih dari group yang lainnya. Pengelompokan ini disesuaikan dengan kebutuhan dari pengguna sistem. Di STIKOM dikelompokkan ke dalam kelompok mahasiswa, dosen/staf dan administrator.

Kontrol akses adalah kumpulan dari metode dan komponen yang dipergunakan untuk melindungi asset informasi (W. Agus Winarta, Auliya Ilman Fadli, Abdul Basith Hijazy, 2005). Meskipun informasi harus dapat diakses oleh setiap orang tetapi diperlukan perlindungan terhadap informasi lainnya. Kontrol akses mendukung baik kerahasiaan dan integritas dari sebuah sistem yang aman.

Kontrol diimplementasikan untuk mengurangi resiko dan potensial kerugian. Kontrol dapat berupa :

1. Preventif : mencegah terjadinya insiden
2. Detektif : mendeteksi terjadinya insiden
3. Korektif : memperbaik terjadinya insiden

***Backup* (Backup)**

Seringkali penyusup (*intruder*) masuk ke dalam sistem dan merusak sistem dengan menghapus berkas-berkas yang dapat ditemui. Jika penyusup ini berhasil menjebol sistem dan masuk sebagai super user (*administrator*), maka ada kemungkinan dia dapat menghapus seluruh berkas. Untuk itu, adanya backup yang dilakukan secara rutin merupakan sebuah hal yang sangat penting. Bayangkan apabila yang dihapus oleh tamu ini adalah berkas penelitian, tugas akhir, skripsi, yang telah dikerjakan bertahun-tahun.

Untuk sistem yang sangat penting, secara berkala perlu dibuat backup yang letaknya berjauhan secara fisik. Hal ini dilakukan untuk menghindari hilangnya data akibat bencana seperti kebakaran, banjir, dan lain sebagainya. Apabila data-data dibackup akan tetapi diletakkan pada lokasi yang sama, kemungkinan data akan hilang jika tempat yang bersangkutan mengalami bencana seperti kebakaran.

Kita tidak pernah tahu apa yang akan terjadi dengan komputer (dalam hal ini disk) kita esok hari. Bisa saja, tiba-tiba terjadi kegagalan yang membuat data yang ada dalam disk berubah, bahkan terhapus. Untuk mengantisipasi ketidakonsistenan data dan terhapusya data dari disk, maka kita perlu melakukan bakup data. Bakup adalah menyalin isi disk kedalam media lain seperti: *floopy disc, magnetic tape*

optical disc, external hardisc, dll. Setelah menyalin disk ke media sementara, maka perlu mengembalikan data tersebut ke dalam disk. Hal inilah yang dinamakan *restore.*

Ada 4 jenis backup data, yaitu:

1. ***Full Backup* (Backup Penuh).**
   Bakup adalah menyalin semua data termasuk *folder* ke media lain. Oleh karena itu, hasil dari backup penuh lebih cepat dan mudah saat operasi *restore*. Kelemahannya adalah: membutuhkan waktu dan ruang yang sangat besar

2. ***Differential Backup* (Backup Turunan).**
   Backup turunan adalah menyalin semua data yang berubah sejak terakhir kali melakukan backup penuh.
   Kelebihan:
   Waktu yang diperlukan untuk *restore* lebih singkat daripada backup peningkatan Jika banyak melakukan bakup turunan, maka data yang di backup semakin kecil ukurannya. Backup turunan lebih cepat daripada backup penuh dan membutuhkan tempat sementara yang lebih kecil daripada yang dibutuhkan oleh backup penuh.

3. ***Incremental Backup* (Backup Peningkatan)**
   Backup peningkatan adalah menyalin semua data yang berubah sejak terakhir kali melakukan backup penuh atau backup turunan.
   Kelebihan:
   a. Membutuhkan waktu yang lebih singkat
   b. Membutuhkan tempat sementara yang lebih kecil ukurannya
   Kekurangan: Waktu untuk *restore* sangat lama

4. ***Mirror Backup* (Backup Cermin)**
   Backup cermin sama dengan backup penuh, tetapi data di padatkan dengan format .tar, .zip, atau yang lain) dan tidak bisa di lindungi dengan *password*. Dapat juga diakses dengan menggunakan *tools* seperti *Windows Explorer*.

II. METODE PENELITIAN

3.1 Kerangka Kerja

Metode penelitian ini dalakukan dengan cara sistematik yang digunakan sebagai pedoman peneliti dalam pelaksanaan penelitian ini agar hasil yang dicapai tidak menyimpang dari tujuan yang telah ditentukan sebelumnya.

Secara umum sistematik yang dimaksud terdapat beberapa langkah – langkah yang harus dilakukan dalam pembuatan tugas akhir ini yaitu :

3.1.1 Perumusan Masalah

Pada tahap ini dilakukan peninjauan ke system yang akan diteliti untuk mengamati serta melakukan eksplorasi lebih dalam dan menggali permasalahan yang ada pada sistem yang berjalan saat ini. Tahap perumusan masalah merupakan langkah awal dari penelitian ini, karena tahap ini diperlukan untuk mendefenisikan keinginan dari sistem yang didak tercapai.

3.1.2 Penentuan Tujuan

Berdasarkan perumusan masalah yang telah dibuat pada tahap sebelumnya, maka tahap penentuan tujuan berguna untuk memperjelas kerangka tentang apa saja yang menjadi sasaran dari penelitian ini. Pada tahap ini ditentukan tujuan dari penelitian ini adalah untuk membangun manajemen keamanan pada sistem informasi akademik yang dapat mendukung semua kegiatan operasional akademik di STIKOM Dinamika Bangsa Jambi.

3.1.3 Studi Pustaka

Studi pustaka dilakukan dengan tujuan untuk mengetahu metode apa yang akan digunakan untuk menyelesaikan permasalahan yang akan diteliti, serta mendapatkan dasar – dasar referensi yang kuat bagi peneliti dalam menerapkan suatu metode yang digunakan.

3.1.4 Pengumpulan Data dan Informasi

Pada tahap ini dilakukan pengumpulan data dan informasi yang untuk lebih mengetahui mengenai sistem yang diteliti. Dari data dan informasi yang dikumpulkan akan dapat diktehui

mengenai sistem yang berjalan saat ini. Data – data dan informasi dapat diperoleh melalui wawancara langsung dengan pihak yang berwenang di STIKOM Dinamika Bangsa Jambi dan pengamatan langsung. Adapun data - data yang diperlukan dalam penelitian ini adalah :

a. Jenis – jenis aktivitas yang terjadi di Bagian Biro Akademik STIKOM Dinamika Bangsa Jambi yang berkenaan dengan bidang akademik.
b. Hak akses apa saja yang dibeikan terhadap mahasiswa, Dosen / Staf, dan Administrator dalam hal pengaksesan terhadap Sistem Informasi Akademik.

3.1.5 Analisa Sistem yang Berjalan

Analisa ini bertujuan untuk mengetahui sistem yang ada saat ini di bagian Akademik STIKOM Dinamika Bangsa Jambi. Analisa sistem yang ada ini perlu dilakukan sebelum melakukan analisa permasalahan, kelemahan – kelemahan sistem, dan kebutuhan – kebutuhan sistem.

3.1.6 Analisa Kebutuhan Sistem

Saat melakukan tahap analisa sistem yang berjalan, secara tidak langsung akan terlihat kelemahan – kelemahan yang ada pada sistem tersebut, sehingga pada saat itu juga bias dilakukan analisa terhadap kebutuhan manajemen keamanan sehingga dapat diidentifikasikan kemungkinan – kemungkianan ancaman yang dapat terjadi pada sistem informasi akademik.

3.1.7 Menentukan Kebutuhan Manajemen Keamanan Data

Pada tahapan ini dilaksanakan proses pendefinisian dan proses dokumentasi terhadap kebutuhan manajemen keamanan sistem informasi akademik berdasarkan hasil analisis yang telah dilakukan.

3.1.8 Menentukan Kebijakan

Pada tahapan ini dirancang prosedur-prosedur, kebijakan dan standar keamanan yang akan digunakan pada sistem informasi akademik

3.1.9 Pembangunan Sistem Manajemen Keamanan

Pada tahapan ini prosedur, standar dan kebijakan dalam bidang keamanan yang telah dirumuskan, kemudian diimplematasikan pada sistem yang berjalan

III. PEMBAHASAN DAN HASIL

3.1 Analisa Masalah

3.1.1 Sistem yang Sedang Berjalan

Salah satu bagian terpenting pada STIKOM Dinamika Bangsa adalah bagian akademik. Bagian akademik ini melingkupi informasi penyedia layanan informasi mahasiswa. Sistem penyedia layanan informasi mahasiswa yang berjalan pada STIKOM Dinamika Bangsa Jambi khususnya informasi penerimaan mahasiswa baru, nilai, administrasi, registrasi (mata kuliah dan jadwal kuliah) dapat diuraikan sebagai berikut:

a. Bagian Penerimaan Mahasiswa Baru

Penerimaan mahasiswa baru pada STIKOM Dinamika Bangsa berlangsung selama beberapa bulan, yang dibagi atas 3 (tiga) gelombang. Calon mahasiswa yang akan mendaftar harus datang langsung ke kampus atau dapat diwakilkan. Bagian penerimaan mahasiswa baru (PMB) menerima setoran biaya pendaftaran dari calon mahasiswa agar calon mahasiswa dapat mendaftar menjadi mahasiswa STIKOM Dinamika Bangsa. Biaya pendaftaran disesuaikan pada gelombang pendaftaran.

b. Bagian Akademik

Proses registrasi dilakukan pada bagian akademik. Bagian akademik menerima bukti setoran uang kuliah dari mahasiswa agar mahasiswa dapat mengisi Kartu Rencana Studi (KRS) yang berguna untuk merencanakan mata kuliah mahasiswa pada semester yang akan datang. KRS yang dikeluarkan bagian akademik terdiri dari 3 rangkap untuk mahasiswa, pembimbing akademik dan bagian akademik. Dalam pengisian KRS tersebut mahasiswa harus mengisi kode mata kuliah, nama mata kuliah yang dipilih, status kontrak, serta sks dan jumlah sks yang diambil. Agar mahasiswa bisa mengisi KRS tersebut, bagian akademik mengeluarkan selebaran informasi yang berisi mata kuliah yang tersedia beserta dosen yang mengajar mata kuliah tersebut. Setelah KRS dikembalikan oleh mahasiswa, KRS diserahkan ke pembimbing akademik untuk dikonsultasikan dan ditandatangani, kemudian KRS dan bukti setoran diserahkan ke bagian administrasi untuk mendapatkan pengecapan

persetujuan KRS. Dari bagian akademik, KRS yang sudah ditandatangani pembimbing akademik dan dicap digunakan untuk dilakukan *entry* data mata kuliah yang diambil mahasiswa. Kemudian bagian akademik memberikan rangkap pertama KRS untuk mahasiswa. Dari KRS tersebut mahasiswa bisa mengetahui mata kuliahnya pada semester yang akan datang.

Dalam mendapatkan informasi nilai Ujian Tengah Semester (UTS) dan Ujian Akhir Semester (UAS), mahasiswa bisa mengetahui dari kertas ujian yang sudah dinilai dosen. Bagian akademik menerima Daftar Nilai Akhir (DNA) yang berisi nilai ujian dari dosen setelah UAS, kemudian bagian akademik melakukan *entry* nilai mahasiswa secara satu persatu berdasarkan nomor induk mahasiswa (NIM) ke dalam *database*. Bagian akademik juga membuat arsip buku informasi mahasiswa yang memuat DNA mahasiswa. Dalam DNA kelas, mahasiswa dapat mengetahui nilai-nilai tatap muka, tugas, *quis*, uts, uas, nilai akhir dan *grade* dari hasil belajar. DNA kelas ini kemudian diproses menjadi Kartu Hasil Studi (KHS) yang diberikan ke pembimbing akademik, yang nantinya akan diberikan kepada mahasiswa.

c. Bagian Administrasi

Bagian Administrasi melakukan verifikasi atas bukti setoran, apakah uang yang disetor sesuai dengan jumlah mata kuliah yang diambil dan memberi cap pada KRS yang sudah ditandatangani pembimbing akademik. Dengan demikian mahasiswa mengetahui status pembayaran uang kuliahnya.

3.2 Otentikasi User

Pengecekan identitas merupakan komponen yang esensial dari sistem keamanan. Hal ini merupakan cara untuk membedakan antara *user* legal dan penyusup. Autentikasi *user* dijaringan merupakan keharusan bagi banyak para *enterprise* yang secara serius melindungi aset informasi yang mereka miliki dan untuk mengetahui siapa dan apa yang akan diakses di jaringan mereka. Sistem autentikasi terdiri atas 3 elemen sebagai berikut:

1. Identifikasi (berupa ID card, sertifikat, dan lain-lain).
2. Informasi (berupa *password*).
3. Atribut (berupa sidik jari, atau informasi *biometric* yang lain).

Dalam jaringan komputer, autentikasi erat kaitannya dengan hak akses seseorang dalam mengakses data yang ada dalam jaringan. Hak akses adalah hak yang diberikan kepada *user* untuk mengakses sistem. Mungkin hak akses merupakan hak yang paling mendasar dalam bidang keamanan. Dalam strategi keamanan, setiap objek dalam sistem (*user*, *administrator*, *software*, sistem itu sendiri, dan sebagainya) harus diberikan hak akses yang berguna untuk menunjang fungsi kerja dari objek tersebut.

Adapun hak akses terhadap administrator adalah sebagai berikut:

1. Administrator dapat melihat data nilai mahasiswa dengan mengklik menu “nilai”. Tampilan data nilai mahasiswa bisa dilihat berdasarkan KHS (kartu hasil studi), transkrip atau secara keseluruhan. Untuk melihat data secara keseluruhan, administrator mengklik “*view*”.

Sedangkan untuk melihat nilai berdasarkan KHS, administrator mengklik menu “khs” yang ada pada menu “*view*”, begitu juga dengan transkrip, hanya dengan mengklik “transkrip”, maka akan muncul layar tampilan yang diinginkan.

2. Administrator berwenang untuk menambah, mengedit dan menghapus data nilai mahasiswa. Untuk menghapus data, tekan tombol “*delete*” pada data yang ingin dihapus. Administrator dapat menambah dan mengedit nilai mahasiswa dengan menekan tombol “*add*” atau “*change*”. Penambahan nilai mahasiswa dilakukan berdasarkan kelas, jadi proses penambahan nilai mahasiswa dilakukan serentak sesuai kelasnya. Gambar 3.2 berikut ini adalah bentuk tampilan layar tambah nilai.
3. Administrator dapat melihat data tugas akhir mahasiswa dengan mengklik menu “tugas akhir”. Tampilan data tugas akhir bisa dilihat perkode tugas akhir, perjurusan, perangkatan serta secara keseluruhan. Untuk melihat data secara keseluruhan, administrator mengklik “*view*”, kemudian akan muncul layar tampilan. Administrator berwenang untuk menambah, mengedit dan menghapus data tugas akhir. Untuk menghapus data, tekan tombol “*delete*” pada data yang ingin dihapus. Administrator dapat menambah dan mengedit jadwal kuliah dengan menekan tombol “*add*” atau “*change*”. Penambahan data tugas akhir hanya bisa apabila mahasiswa telah mengontrak mata kuliah tugas akhir. Administrator dapat melihat data keuangan dengan mengklik menu “keuangan”. Tampilan data keuangan bisa dilihat perdata atau secara periode. Untuk melihat data secara keseluruhan, administrator mengklik “*view*”, kemudian akan muncul layar tampilan. Administrator berwenang untuk menambah, mengedit dan menghapus data keuangan. Untuk menghapus data, tekan tombol “*delete*” pada data yang ingin dihapus. Administrator dapat menambah dan mengedit data keuangan dengan menekan tombol “*add*” atau “*change*”.
4. Administrator dapat melihat data konfirmasi dengan mengklik menu “konfirmasi”. Tampilan data konfirmasi bisa dilihat perdata konfirmasi atau berdasarkan periode tertentu. Untuk melihat data secara keseluruhan, administrator mengklik “*view*”. Administrator berwenang untuk menambah, mengedit dan menghapus data konfirmasi. Untuk menghapus data konfirmasi, tekan tombol “*delete*” pada data yang ingin dihapus. Administrator dapat menambah dan mengedit data konfirmasi dengan menekan tombol “*add*” atau “*change*”. Biasanya penambahan data konfirmasi didasarkan pada tiap transaksi keuangan di bank yang telah dilakukan mahasiswa atau calon mahasiswa, setelah itu baru bisa dilakukan penambahan data konfirmasi oleh administrator.

IV. Kesimpulan

Dari uraian yang telah dikemukakan pada bab sebelumnya dapat diambil beberapa kesimpulan sebagai berikut:

1. Dalam membangun sebuah sistem informasi akademik yang terintegrasi dengan jaringan lokal maupun internet, untuk menghasilkan output informasi yang layak serta sesuai dengan kebutuhan harus didukung dengan sistem manajemen keamanan sarta infrastruktur yang sesuai dengan kebutuhan sistem.
2. Dengan pemanfaatan sistem manajemen keamanan pada sistem informasi akademik yang terintegrasi dengan jaringan lokal dan internet, maka dapat mengefisienkan sumber daya manusia, misalkan untuk memberikan paelayanan informasi nilai kepada mahasiswa.

DAFTAR PUSTAKA

[1] Budi Raharjo, Keamanan Sistem Informasi Berbasis Internet, PT Insan Infonesia – Bandung dan Jakarta, 1998 – 2005

[2] Budi Raharjjo, e – Procurement Security, Institut Teknologi Bandung, 2005

[3] Chris Brenton dan Cameron Huni, "Network Security", Penerbit PT Elex Media Komputindo Kelompok Gramedia, Jakarta, 2005

[4] Jasmir, Analisa dan Perancangan Sistem Informasi Akademik di STIKOM Dinamika Bangsa Jambi, Magister Ilmu Komputer UPI "YPTK", Padang, 2006.

[5] Jogiyanto, HM. "Analisis dan Desain Sistem Informasi : Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis", Penerbit Andi Ofset Yogyakarta, 1995

[6] Malikuswari, Yusron Avivi, Imelda dan Sasongko Budhi, "Proteksi Sistem Informasi Multi Level Marketing", Magister Teknologi Informasi, Universitas Indonesia, 2005

[7] Maman Abdurohman, "Proteksi dan Teknik Keamanan Sistem Informasi", Magister Teknologi Informasi, Universitas Indonesia, 2002

[8] Novita Ariyanti, Perancangan Sistem Administrasi Akademis Online BerbasisnWeb, Program Studi Teknik Informatika, STIKOM Dinamika Bangsa, Jambi,2006

[9] Over Rinel, Perancangan dan Implementasi Sistem Informasi Akademik, Magister Ilmu Komputer UPI "YPTK", Padang, 2007

[10] W. Agus Winarta, Auliya Ilman Fadli dan Abdul Basith Hijazih, "Keamanan Sistem Informasi", Magister Teknologi Informasi, Institut Teknologi Bandung, 2005