UNIVERSITAS INDONESIA

PERANCANGAN DAN IMPLEMENTASI MODUL KONTROL AKSES BERBASIS MIKROKONTROLLER AVR ATMEGA32 UNTUK PROTEKSI LOGIN APLIKASI WEB DATABASE

SKRIPSI

MUHAMAD TAUFIK YUSUF
0806366112

FAKULTAS TEKNIK
PROGRAM SARJANA EKSTENSI
DEPOK
JUNI 2011

UNIVERSITAS INDONESIA

PERANCANGAN DAN IMPLEMENTASI MODUL KONTROL AKSES BERBASIS MIKROKONTROLLER AVR ATMEGA32 UNTUK PROTEKSI LOGIN APLIKASI WEB DATABASE

SKRIPSI

Diajukan sebagai syarat untuk memperoleh gelar Sarjana Teknik

MUHAMAD TAUFIK YUSUF
0806366112

FAKULTAS TEKNIK
PROGRAM SARJANA EKSTENSI
DEPOK
JUNI 2011

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan
semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama : MUHAMAD TAUFIK YUSUF
NPM : 0806366112

Tanda Tangan : .....
Tanggal : 23 Juni 2011

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :

Nama : MUHAMAD TAUFIK YUSUF

NPM : 0806366112

Program Studi : TEKNIK ELEKTRO

Judul Skripsi : Perancangan dan Implementasi Modul Kontrol Akses Berbasis Mikrokontroller AVR ATmega32 untuk Proteksi Login Aplikasi Web Database

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Indonesia

DEWAN PENGUJI

Pembimbing : Ir. A. Endang Sriningsih, M.T, Si ( )

Penguji : Dr. Ir. A.A.P Ratna, M.Eng ( )

Penguji : Prima Dewi Purnamasari, S.T, M.T, M.Sc ( )

Ditetapkan di : Depok

Tanggal : 23 Juni 2011

KATA PENGANTAR

Puji syukur saya panjatkan kepada Allah SWT, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan Skripsi ini. Penulisan Skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Jurusan Teknik Elektro pada Fakultas Teknik Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan Skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan Skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

(1) Ir. A. Endang Sriningsih, M.T, Si, selaku dosen pembimbing yang telah menyediakan waktu, tenaga dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini;
(2) Rekan-rekan staf Deputi I Lembaga Sandi Negara yang telah banyak membantu dalam usaha memperoleh data yang saya perlukan;
(3) Istri saya tercinta Ratri Nur Rohmah dan anak saya Zahra Nur Azizah Yusuf yang selalu memberikan dukungan moral; dan
(4) Sahabat yang telah banyak membantu saya dalam menyelesaikan skripsi ini.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 23 Juni 2011

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama	: Muhamad Taufik Yusuf
NPM	: 0806366112
ProgramStudi	: Teknik Elektro
Departemen	: Teknik
Fakultas	: Teknik
Jenis karya	: Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia Hak Bebas Royalti Noneksklusif (Non-exclusive Royalty-Free Right) atas karya ilmiah saya yang berjudul :

PERANCANGAN DAN IMPLEMENTASI MODUL KONTROL AKSES BERBASIS MIKROKONTROLLER AVR ATMEGA32 UNTUK PROTEKSI LOGIN APLIKASI WEB DATABASE

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (database), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 23 Juni 2011
Yang menyatakan

(Muhamad Taufik Yusuf)

ABSTRAK

Nama : Muhamad Taufik Yusuf
Program Studi : Teknik Elektro
Judul : Perancangan dan Implementasi Modul Kontrol Akses Berbasis Mikrokontroller AVR ATmega32 untuk Proteksi Login Aplikasi Web Database

Teknik yang telah banyak digunakan untuk melindungi suatu pangkalan data adalah penggunaan *username* dan *password*. Untuk mengurangi tingkat keberhasilan penyusupan ke dalam pangkalan data, biasanya ditambahkan *salt* yaitu string yang ditambahkan pada *password* pada saat login. Pada tingkatan informasi tertentu, perlindungan terhadap pangkalan data tidak cukup hanya dengan menggunakan *username*, *salt* dan *password* saja. Perlu ada mekanisme lain yang dapat menyulitkan penyusup agar tidak mudah masuk ke dalam pangkalan data. Penulisan skripsi ini bertujuan untuk melakukan perancangan dan implementasi teori sekuriti pada aplikasi pangkalan data berbasis web di jaringan intranet dengan menambahkan modul kontrol akses yang diharapkan dapat memberikan perlindungan lebih terhadap aplikasi pangkalan data dari penyusup. Pengujian pada sistem menyatakan bahwa modul kontrol akses dapat berjalan baik dengan tingkat keberhasilan mencapai 100%. *Delay* yang terjadi akibat proses otentikasi yang lebih panjang membuat waktu respon bertambah menjadi 2.14 detik dari sebelumnya 0.004 detik, namun masih dalam batas yang diperkenankan.

Kata kunci:
sekuriti, kontrol akses, pangkalan data berbasis web

ABSTRACT

Name : Muhamad Taufik Yusuf
Study Program : Electrical Engineering
Title : Access Control Modul Design and Implementation Based on AVR ATmega32 Microcontroller for Web Database Application Login Protection

The technique has been widely used to protect a data base is the use of username and password. To reduce the success rate of infiltration into the database, namely strings usually added salt is added to the password at login. At a certain level of information, protection of databases is not enough just to use username, salt and password. There should be other mechanisms that would prevent easy entry into the database for an intruder. This writing aims to do the design and implementation of the theory of security in web-based database applications on intranets by adding network access control module that is expected to provide greater protection against database application from intruders. Tests on the system states that the access control module can be run either with a success rate reached 100%. Delay caused by a longer authentication process makes the response time increases about 2.14 seconds from about 0.004 seconds, but still within the permitted limits.

Key words:
security, access control, web database

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Informasi adalah aset yang mempunyai nilai bagi organisasi dan memerlukan perlindungan yang memadai. Perlindungan tersebut meliputi beberapa diantaranya: kerahasiaan, yaitu memastikan informasi hanya bisa diakses oleh otoritas pemegang akses; integritas, yaitu menjaga keakuratan dan keutuhan informasi serta metode pemrosesannya; dan ketersediaan, yaitu memastikan pengguna yang diberikan otoritas mendapatkan akses informasi serta aset terkait bila diperlukan. Informasi tersebut dapat berupa data-data tentang pegawai, data peralatan pendukung, informasi gaji dan tunjangan, usulan kenaikan pangkat, rencana mutasi pegawai, jaring komunikasi, dan lain sebagainya. Informasi-informasi ini pada umumnya dikumpulkan dan dikelola pada satu berkas elektronik berbentuk pangkalan data.

Teknik yang telah banyak digunakan untuk melindungi suatu pangkalan data adalah penggunaan *username* dan *password*. Untuk mengurangi tingkat keberhasilan penyusupan ke dalam pangkalan data, biasanya ditambahkan *salt* yaitu string tertentu yang ditambahkan pada *password* pada saat login. Pada tingkatan informasi tertentu, perlindungan terhadap pangkalan data tidak cukup hanya dengan menggunakan *username*, *password* dan *salt* saja. Perlu ada mekanisme lain yang dapat menyulitkan penyusup agar tidak mudah masuk ke dalam pangkalan data.

Dalam perkembangan dunia elektronika dan komputer saat ini, dimungkinkan untuk menambahkan suatu sistem kontrol akses berbentuk modul terhadap pangkalan data berbasis web guna memberikan perlindungan lebih terhadap informasi sensitif yang ada di dalamnya.

1.2. Tujuan Penulisan

Penulisan skripsi ini bertujuan untuk melakukan perancangan dan implementasi teori sekuriti pada aplikasi pangkalan data berbasis web di jaringan intranet dengan menambahkan modul kontrol akses yang diharapkan dengan implementasi ini, dapat memberikan perlindungan lebih terhadap aplikasi pangkalan data dari pengguna yang tidak memiliki hak akses. Disamping itu, data yang dilindungi juga harus memiliki tingkat akurasi yang baik.

1.3. Batasan Masalah

Penulisan skripsi ini dibatasi pada implementasi mekanisme otentikasi untuk masuk ke dalam sistem pangkalan data pada jaringan intranet. Tidak dibahas perancangan aplikasi pangkalan data berbasis web dengan asumsi aplikasi web tersebut dapat berubah sesuai kebutuhan pengguna. Otentikasi dilakukan antara pengguna yang memiliki hak akses, modul kontrol akses dan server pangkalan data. Pada mekanisme otentikasi digunakan teknik kriptografi dan skema protokol *secret splitting*.

1.4. Metode Penulisan

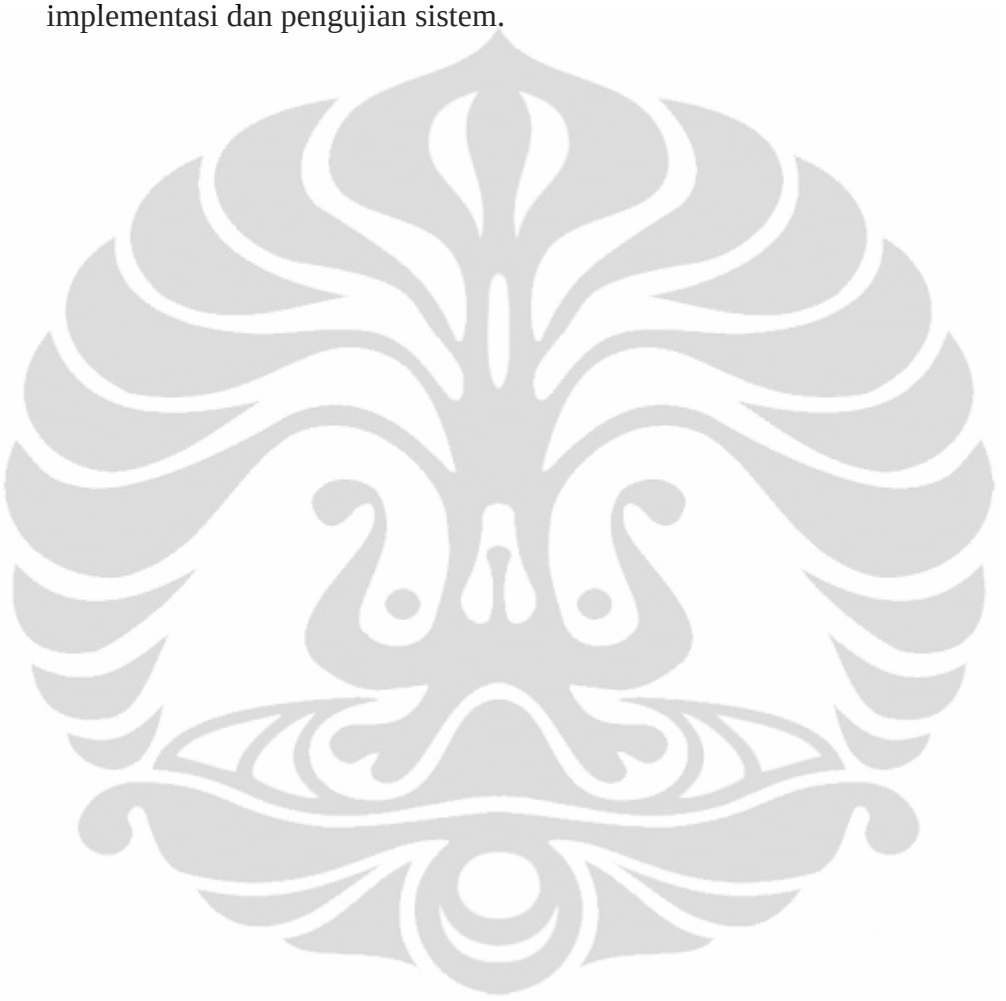
Penulisan skripsi ini dilakukan melalui beberapa tahapan, yaitu studi literatur, identifikasi kebutuhan alat pengembangan, perancangan sistem, implementasi sistem, pengujian dan analisis sistem.

1.5. Sistematika Penulisan

Sistematika penulisan skripsi ini dibagi atas beberapa bab dan masing-masing bab terbagi menjadi beberapa sub bab. Dibawah ini uraian singkat isi dari tiap-tiap bab untuk memberikan gambaran secara keseluruhan mengenai isi dari materi ini.

Bab pendahuluan menguraikan tentang latar belakang, tujuan, batasan masalah, metode penulisan, dan sistematika penulisan. Bab modul kontrol akses menjelaskan tentang teori yang berhubungan dengan kontrol akses, sistem manajemen pangkalan data, kriptografi, mikrokontroller AVR ATmega32, modul

ethernet, konsep dasar TCP/IP dan alat pengembangan. Bab perancangan sistem menjelaskan tentang deskripsi perancangan sistem, spesifikasi dan fungsi sistem, cara kerja sistem, arsitektur sistem dan perancangan *layout*. Bab implementasi dan pengujian sistem berisi tentang deskripsi implementasi dan pengujian sistem, hasil pengambilan data dan analisis. Bab kesimpulan berisi kesimpulan tentang implementasi dan pengujian sistem.



BAB 2
MODUL KONTROL AKSES

2.1. Kontrol Akses

Kontrol akses adalah sebuah sistem yang mengatur bagaimana seseorang yang memiliki hak akses dapat melakukan akses terhadap suatu fasilitas fisik dan sumber daya didalamnya atau akses terhadap sistem informasi komputer [1]. Dalam kehidupan sehari-hari, kontrol akses sudah biasa digunakan. Kunci pada pintu mobil adalah salah satu bentuk dari kontrol akses. Penggunaan PIN pada sistem ATM sebuah bank juga bentuk lain dari kontrol akses. Satpam yang berjaga di depan pintu parkir juga adalah bentuk lain dari kontrol akses yang sifatnya lebih tradisional. Penggunaan kontrol akses menjadi penting ketika seseorang membutuhkan pengamanan terhadap peralatan dan informasi yang penting, rahasia, atau sensitif.

Kontrol akses juga berkenaan dengan pengendalian akses terhadap sumber daya pada sebuah komputer atau sistem jaringan. Tanpa pengendalian tersebut, setiap orang dapat mengakses apa saja didalamnya. Karyawan dapat melihat informasi gaji milik manajernya, membaca e-mail milik karyawan lain, dan orang-orang tak dikenal atau pesaing bisnis dapat mengakses ke dalam server secara *remote* dan mengetahui rencana strategis perusahaan untuk beberapa tahun kedepan. Dengan adanya kontrol akses, para pengguna harus teridentifikasi, terbukti benar dan memiliki hak akses sebelum mereka dapat mengakses sumber daya ataupun menjalankan operasi pada sebuah sistem [2].

Pada setiap model kontrol akses, entitas yang dapat melakukan tindakan dalam sistem disebut subjek, dan entitas yang melambangkan sumber daya dimana akses kepadanya perlu dikontrol disebut objek.

2.1.1. Teknik Kontrol Akses

Teknik control akses pada umumnya dikategorikan menjadi *discretionary* dan *non-discretionary*. Kategori *discretionary* berarti kebijakan akses ditentukan oleh pemilik objek, sedangkan kategori *non-discretionary* ditentukan oleh sistem.

Tiga model yang paling dikenal adalah *Discretionary Access Control* (DAC), *Mandatory Access Control* (MAC), dan *Role Based Access Control* (RBAC). MAC and RBAC keduanya adalah *non-discretionary[3]*. Model-model tersebut dapat dijelaskan sebagai berikut:

a. DAC adalah kebijakan akses yang ditentukan oleh pemilik objek. Pemilik menentukan siapa saja yang dibolehkan untuk mengakses objek dan apa kewenangannya terhadap objek tersebut. Setiap pengguna memiliki hak akses berbeda-beda (dikenal dengan nama *privileges*) pada objek yang berbeda-beda pula.
b. MAC adalah kebijakan akses yang ditentukan oleh sistem dan digunakan pada sistem bertingkat yang mengolah data-data super sensitif seperti informasi terbatas pemerintah dan militer. Sistem bertingkat dimaksud adalah sistem komputer tunggal yang menangani level klasifikasi bertingkat antara subjek dan objek. Setiap objek diberi label dengan tingkat klasifikasi tertentu, dan setiap pengguna diberikan tingkat *clearance* tertentu. Setiap objek data tertentu hanya dapat diakses oleh pengguna dengan level *clearance* yang sesuai.
c. RBAC adalah kebijakan akses yang ditentukan oleh sistem dan digunakan pada aplikasi komersial atau juga pada sistem militer dimana keamanan bertingkat dibutuhkan. Berbeda dengan DAC yang membolehkan pengguna mengendalikan akses ke sumber dayanya, pada RBAC hak akses dikendalikan pada level sistem dan tidak dengan kontrol dari pengguna. RBAC mengendalikan kumpulan *permission* yang berisi operasi kompleks seperti transaksi *e-commerce*.

2.1.2. Layanan Kontrol Akses

Layanan pada kontrol akses menyediakan layanan pokok yang mencakup otentikasi, otorisasi, dan akuntabilitas yang dapat dijelaskan sebagai berikut:

a. Otentikasi menentukan siapa yang dapat masuk ke dalam sistem. Otentikasi adalah proses verifikasi yang membuktikan bahwa sebuah identitas terikat dengan entitas yang membuat pernyataan atau klaim identitas tersebut. Proses ini mensyaratkan ada validasi awal identitas yang

disebut pembuktian identitas. Mekanisme otentikasi pada umumnya didasarkan pada paling tidak satu dari empat faktor berikut ini:

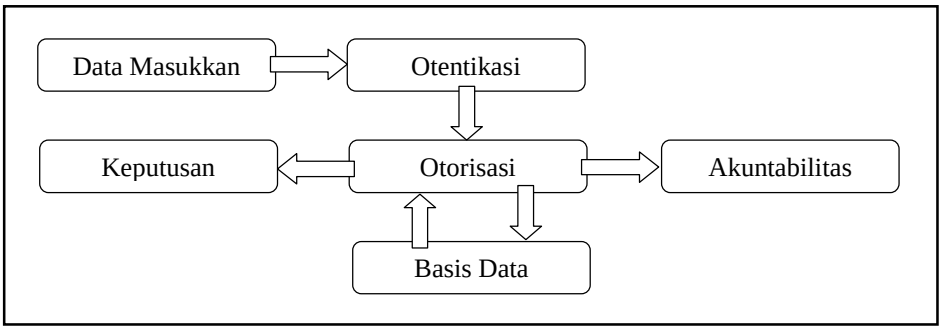
1) Sesuatu yang diketahui, seperti *password* atau PIN;
2) Sesuatu yang dimiliki, seperti *smart card* atau token;
3) Sesuatu yang ada di diri sendiri, seperti sidik jari, suara, retina atau karakteristik iris;
4) Posisi dimana berada, misal di dalam atau di luar jaringan perusahaan.

b. Otorisasi menentukan apa yang bisa dilakukan oleh subjek. Sebagian besar sistem operasi modern mendefinisikan himpunan hak akses yang merupakan pengembangan atau variasi dari tiga tipe dasar akses berikut ini:

1) *Read* (R), Subjek hanya dapat melihat;
2) *Write* (W), Subjek dapat mengubah isi berkas atau direktori dengan operasi *add*, *create*, *delete, rename*;
3) *Execute* (X), Jika berkas berupa program maka subjek dapat menjalankan program tersebut.

c. Akuntabilitas mengidentifikasi apa yang dilakukan subjek. Layanan ini menggunakan komponen sistem seperti *record* dan *log* untuk menghubungkan subjek dengan tindakannya. Komponen-komponen tersebut sangat membantu administrator sistem untuk mengidentifikasi usaha-usaha yang mungkin dilakukan subjek dalam menerobos sistem.

Layanan kontrol akses memiliki proses seperti yang ditunjukkan pada Gambar 2.1 di bawah ini:



Gambar 2.1. Layanan kontrol akses

Data masukan merupakan data yang diberikan oleh subjek kepada sistem. Data masukan ini berisi informasi mengenai identitas subjek yang dapat dikenali oleh sistem. Data dapat berupa sesuatu yang diketahui subjek, sesuatu yang dimiliki subjek, sesuatu yang melambangkan subjek atau posisi subjek. Sistem mengolah data masukan yang berisi identitas subjek dengan teknik pengolahan tertentu dan membandingkannya dengan pola yang telah tersimpan di dalam pangkalan data sistem. Jika polanya sesuai, sistem memberikan akses kepada subjek sesuai dengan hak akses yang menempel padanya. Sistem mencatat tindakan-tindakan subjek terhadap objek sebelum subjek tersebut keluar sistem.

2.2. Sistem Manajemen Pangkalan Data

Pangkalan data didefinisikan sebagai himpunan kelompok data yang saling berhubungan yang diorganisasi sedemikian rupa agar kelak dapat dimanfaatkan kembali dengan cepat dan mudah. Kumpulan data tersebut juga diatur sedemikian rupa sehingga tidak terjadi perulangan data yang tidak perlu dan disimpan dalam media penyimpanan elektronis untuk memenuhi berbagai kebutuhan. Tidak semua bentuk penyimpanan data secara elektronis bisa disebut pangkalan data. Dokumen-dokumen elektronis seperti berkas teks, *spreadsheet*, musik dan lain-lain dapat disimpan dalam media penyimpanan elektronis. Namun karena tidak ada pemilahan dan pengelompokan data sesuai jenis atau fungsi data dan akan menyulitkan pencarian data kelak, maka hal itu tidak termasuk dalam pangkalan data [4].

Pengelolaan pangkalan data secara fisik tidak dilakukan oleh pemakai secara langsung, tetapi ditangani oleh sebuah perangkat lunak khusus yang disebut *Database Management System* atau DBMS. Perangkat lunak inilah yang menentukan bagaimana data diorganisasi, disimpan, diubah dan diambil kembali. DBMS juga menerapkan mekanisme pengamanan data, pemakaian data secara bersama, pengecekan konsistensi data dan sebagainya. Perangkat lunak yang termasuk sebagai DBMS diantaranya adalah dBase III+, dBase IV, FoxBase, Rbase, MS-Access, MS-SQLServer, Oracle, Sybase dan MySQL.

2.2.1 MySQL

MySQL adalah sebuah DBMS terbuka yang sangat terkenal di kalangan pengembang sistem pangkalan data dunia yang digunakan untuk berbagai aplikasi terutama untuk aplikasi berbasis *web*. MySQL mempunyai fungsi sebagai *Structured Query Language* (SQL) yang dimiliki sendiri dan telah diperluas. MySQL umumnya digunakan bersamaan dengan PHP untuk membuat aplikasi yang dinamis dan powerful [5].

2.2.2 Keunggulan MySQL

Ada beberapa keunggulan dari MySQL, diantaranya adalah:

a. MySQL merupakan program yang *multi-threaded*, sehingga dapat dipasang pada *server* yang memiliki multi-CPU.
b. Didukung program-program umum seperti C, C++, Java, Perl, PHP, Python, TCL API.
c. Bekerja pada berbagai *platform*. Tersedia berbagai versi untuk berbagai sistem operasi.
d. Memiliki jenis kolom yang cukup banyak sehingga memudahkan konfigurasi sistem pangkalan data.
e. Memiliki sistem sekuriti yang cukup baik dengan verifikasi *host*.
f. Mendukung *record* yang memiliki kolom dengan panjang tetap atau panjang bervariasi.

2.2.3 Sistem Server Pangkalan Data MySQL

Sistem pangkalan data MySQL memiliki sistem keamanan dengan tiga verifikasi yaitu *username*, *password* dan *host*. Verifikasi *host* memungkinkan untuk membuka keamanan di *localhost*, tetapi tertutup bagi *host* lain (bekerja di lokal komputer). Sistem keamanan ini ada di dalam pangkalan data *mysql* dan pada tabel *user*. Proteksi juga dapat dilakukan terhadap pangkalan data, tabel, hingga kolom secara terpisah.

2.2.4 Fungsi-fungsi SQL

MySQL memiliki fungsi-fungsi standar SQL dan beberapa kemampuan tambahan. Secara lengkap dokumentasi ini terdapat pada manual MySQL. Namun demikian pada bagian ini perlu disajikan beberapa fungsi SQL yang sering digunakan dalam aplikasi *Web*.

a. SELECT <column,...> FROM <table_name,...> WHERE <where_definition> ORDER BY <column, ...> [ASC|DESC]. Fungsi ini berfungsi untuk memilih atau mengambil data dari sebuah tabel dengan kolom yang telah ditentukan kemudian dipanggil dari kolom yang diinginkan.
b. INSERT INTO <table_name> VALUES (<list_of_data>). Fungsi ini berfungsi untuk memasukkan data kedalam sebuah tabel dengan nilai atau data yang diinginkan.
c. UPDATE <table_name> SET column=<expression> WHERE <where_definition>. Fungsi ini berfungsi untuk mengganti data pada sebuah tabel dengan data yang diinginkan berdasarkan syarat yang ditentukan.
d. DELETE FROM <table_name> WHERE <where_definition>. Fungsi ini berfungsi untuk menghapus data pada sebuah tabel berdasarkan syarat yang ditentukan.

2.3. Kriptografi

Sebelum tahun 1980-an kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandinya kedalam bentuk yang tidak dapat dimengerti lagi maknanya. Namun saat ini kriptografi berkembang lebih dari sekedar untuk kepentingan *privacy*, tetapi juga memberikan layanan *data integrity*, *authentication*, dan *non-repudiation*. Selanjutnya kriptografi didefinisikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas, serta otentikasi [6].

2.3.1. Peran Kriptografi

Kriptografi dapat diartikan sebagai studi dari teknik–teknik matematika yang berhubungan dengan keamanan informasi seperti *confidentiality*, *data integrity*, *entity authentication* serta *data origin authentication*. Dari pengertian di atas dapat diketahui bahwa kriptografi memiliki peranan yang sangat penting dalam hal pengamanan informasi terutama pada beberapa hal yang sangat penting bagi suatu informasi, yang dapat dijelaskan sebagai berikut:

a. *Confidentiality*, dapat diartikan juga sebagai *secrecy* yaitu cara yang digunakan untuk menjaga isi dari suatu informasi agar hanya dapat diketahui oleh orang yang berhak untuk mengetahuinya.
b. *Data integrity*, adalah cara yang digunakan untuk mencegah adanya perubahan terhadap isi informasi yang dilakukan oleh orang yang tidak berhak, misalnya menghilangkan sebagian isi informasi, penambahan ataupun penggantian.
c. *Authentication*, merupakan cara yang digunakan untuk mengetahui siapa yang berhak terhadap suatu isi informasi.
d. *Non-repudiation*, merupakan cara yang digunakan untuk mencegah adanya penyangkalan bahwa seseorang adalah pembuat dari suatu informasi ataupun penolakan terhadap suatu perjanjian tertentu.

Keempat hal di atas merupakan tujuan utama dari kriptografi yang diterapkan dalam teori dan praktek. Kriptografi merupakan hal–hal yang berhubungan dengan pencegahan dan pendeteksian adanya kecurangan dan aktifitas–aktifitas membahayakan lainnya.

2.3.2. Protokol Kriptografi

Protokol didefinisikan sebagai aturan yang berisi rangkaian langkah-langkah yang melibatkan dua pihak atau lebih dan dibuat untuk menyelesaikan suatu pekerjaan [7]. “Rangkaian langkah-langkah” berarti bahwa sebuah protokol memiliki urutan eksekusi, dari awal sampai akhir. Setiap langkah harus dieksekusi sesuai urutannya dan tidak ada langkah baru yang dikerjakan jika langkah sebelumnya masih berjalan. “Melibatkan dua pihak atau lebih” artinya untuk menyelesaikan protokol dibutuhkan paling sedikit dua pihak. “Dibuat untuk

menyelesaikan suatu pekerjaan" berarti sebuah protokol harus menghasilkan sesuatu. Berikut ini adalah karakteristik lain dari protokol:

a. Setiap pihak yang terlibat dalam protokol harus memahami protokol serta semua langkah-langkahnya;
b. Setiap pihak yang terlibat dalam protokol harus setuju untuk mengikutinya;
c. Protokol harus jelas dan tidak boleh menimbulkan makna ganda atau ambigu; dan
d. Protokol harus lengkap, dimana terdapat langkah-langkah tertentu yang diambil untuk setiap kemungkinan permasalahan.

Protokol kriptografi adalah protokol yang menggunakan kriptografi. Protokol kriptografi melibatkkan beberapa algoritma kriptografi tetapi tujuannya lebih dari sekedar keamanan sederhana. Protokol kriptografi sangat diperlukan, misalnya untuk berbagi komponen rahasia untuk menghitung sebuah nilai, membangkitkan rangkaian bilangan acak, meyakinkan identitas pengguna yang lain (otentikasi), dan lain sebagainya. Tujuan utama penggunaan kriptografi dalam protokol adalah untuk mencegah atau mendeteksi penyadapan atau kecurangan lainnya.

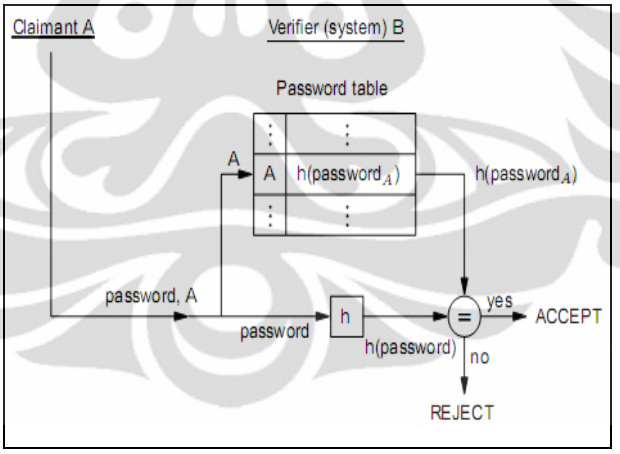
2.3.3. Protokol Kriptografi untuk Otentikasi

Agar pengguna dapat mengotentikasi dirinya ke sistem, demikian pula sistem dapat mengotentikasi pengguna maka digunakan *user ID* dan *password*. *Password* adalah string rahasia dengan panjang 6 sampai 10 karakter atau lebih yang berhubungan dengan pengguna atau entitas yang digunakan oleh pengguna untuk otentikasi ke suatu sistem. *User ID* digunakan untuk identifikasi sedangkan *password* digunakan untuk mendapatkan klaim suatu *user account*. Sistem akan mengecek kecocokan pola hasil pengolahan *password* dan *user ID* dan memberi kewenangan untuk mengakses sistem. Berikut ini adalah aturan umum penggunaan *password*:

a. Panjang minimal 8 atau 12 karakter yang terdiri dari *uppercase*, *numeric*, *non-alphanumeric*.

b. Mempunyai periode *password* yang kecil, jadi periode penggantian *password* tidak boleh terlalu lama.
c. *Password* haruslah menggunakan kata-kata yang tidak umum dipakai.
d. *Password* tidak berhubungan dengan biodata pengguna.

Pertama kali pengguna memasukkan *password* ke sistem, *password* dienkripsi dengan menggunakan fungsi kompresi satu arah, nilai kompresi tersebut kemudian disimpan dalam berkas *password*. Ketika pengguna akan mengakses kembali sistem tersebut maka ia harus memasukkan *password*. Kemudian sistem akan mengenkripsi *password* yang baru saja dimasukkan dengan fungsi kompresi satu arah (fungsi yang sama dengan ketika *password* pertama kali dimasukkan) sehingga diperoleh nilai kompresi. Sistem kemudian membandingkan nilai kompresi *password* yang baru dimasukkan dengan nilai kompresi pada berkas *password*. Apabila sesuai maka pengguna dapat mengakses sistem. Sebaliknya apabila tidak sama maka pengguna tidak diperkenankan mengakses sistem. Dapat digambarkan seperti pada Gambar 2.2. Sebagai berikut:



Gambar 2.2. Protokol otentikasi [6]

Salt adalah string tambahan pada *password* yang diberikan oleh suatu sistem sebelum dienkripsi menggunakan fungsi kompresi satu arah. Nilai *salt* dan hasil fungsi kompresi disimpan dalam pangkalan data *administrator*. Jika jumlah nilai *salt* yang digunakan cukup besar, maka *dictionary attack* dapat dihindari karena penyusup harus membangkitkan nilai kompresi untuk masing-masing *salt*

yang mungkin. Pemberian *salt* pada umumnya digunakan untuk hal-hal sebagai berikut:

a. Mencegah *dictionary attacks*.
b. Mencegah duplikasi *password*. Jika 2 pengguna memilih *password* yang sama, *password* tersebut akan ditandai dengan string yang berbeda sehingga diperoleh *password* yang berbeda pada tabel.
c. Meningkatkan panjang *password* tanpa meminta pengguna untuk mengingat tambahan karakter.

2.3.4. *Secret Splitting*

Secret splitting adalah suatu metode untuk membagi angka, teks maupun data komputer menjadi dua bagian atau lebih. Semua bagian dibutuhkan untuk mendapatkan informasi asli. Ketika salah satu bagian saja tidak ada, secara perhitungan akan mustahil untuk mendapatkan informasi asli [7]. Secara matematis *secret splitting* memberikan kerahasiaan yang mutlak selama informasi dibagi secara terpisah. Masalah yang muncul adalah informasi tidak bisa begitu saja dibagi menjadi dua, karena hal ini akan mengungkapkan setengah dari informasi asli ataupun dapat memudahkan untuk mendapatkan kembali informasi asli.

Prinsip kerja dari *secret splitting* mengacu pada *one-time-pad encryption* yang sangat sederhana tetapi efektif. Satu bagian merupakan *random key* dan satu bagian lagi adalah hasil pengurangan *random key* tersebut dengan informasi asli. *Secret splitting* dapat dijelaskan dengan contoh sebagai berikut:

a. X membagi nomor kunci kombinasi brankas, yaitu 51 42 03 18. Misal *Random key* yang dipilih adalah 22 01 35 17 dimana panjangnya sama dengan panjang nomor kombinasi. Untuk menghasilkan bagian yang kedua, kunci kombinasi brankas dikurangi *random key* digit demi digit dengan *carry*. (contoh: 1 – 2 = 11 – 2 = 9).
b. Y dan Z masing-masing menerima salah satu bagian informasi dari X. Untuk mendapatkan kembali kunci kombinasi brankas dilakukan dengan menambahkan dua bagian yang ada pada Y maupun Z tanpa menggunakan *carry* (contoh: 2 + 9 = 1 bukan 11).

Contoh perhitungan menggunakan metode *secret splitting* dapat dilihat pada Tabel 2.1. berikut:

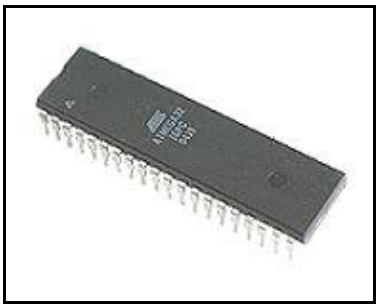
Tabel 2.1. Contoh perhitungan metode *secret splitting*

Kunci kombinasi X	51	42	03	18
Random key (bagian pertama)	-22	-01	-35	-17
Hasil (bagian kedua)	39	41	78	01

Dari tabel diatas, Nilai yang diterima oleh Y adalah 22 01 35 17, sedangkan nilai yang diterima oleh Z adalah 39 41 78 01.

2.4. Mikrokontroler AVR ATmega32

Perkembangan teknologi AVR (*Alf and Vegard Rics Processor*) memberikan suatu teknologi yang memiliki kapabilitas yang amat maju, tetapi dengan biaya yang sangat minimalis. Mikrokontroler AVR memiliki arsitektur RICS 8 bit dan sebagian besar instruksi dieksekusi dalam satu siklus *clock*. Mikrokontroler AVR merupakan *low-power* CMOS 8-bit, yang merupakan pengembangan arsitektur RISC (*Reduce Instruction Structure Chip*). Dengan mengeksekusi instruksi dalam *single clock cycle*, AVR dapat mencapai 1 MIPS per MHz sehingga desain sistemnya dapat mengoptimalkan konsumsi daya dan kecepatan proses. Secara umum AVR dapat dikelompokkan menjadi 4 kelas yaitu, keluarga ATtiny, keluarga AT90Sxx, keluarga ATmega dan AT86RFxx. Pada dasarnya yang membedakan masing-masing kelas adalah memori, kelengkapan dan fungsinya. Dari segi arsitektur dan instruksi yang digunakan, dapat dikatakan hampir sama. Gambar 2.3. berikut ini adalah bentuk fisik mikrokontroler AVR ATmega32.



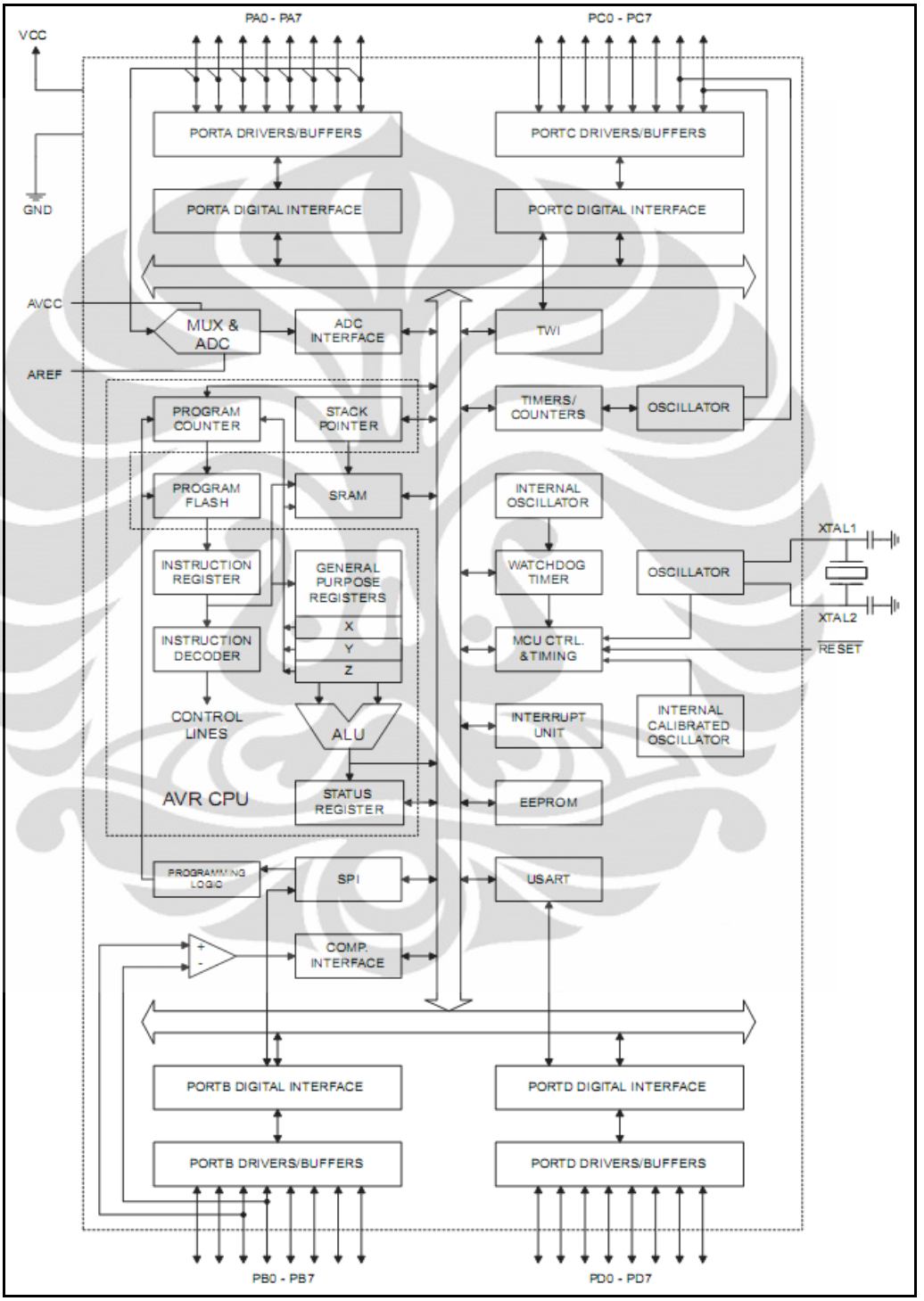
Gambar 2.3. AVR ATmega32 [8]

2.4.1. Diagram Blok AVR ATmega32

Inti mikrokontroler AVR mengkombinasikan semua instruksi dengan 32 *general purpose working register*. Seluruh register tersebut terhubung langsung dengan *Arithmetic Logic Unit* (ALU), yang memungkinkan 2 register secara bebas untuk diakses pada 1 instruksi yang dieksekusi dalam 1 siklus clock. Hal ini menghasilkan arsitektur yang lebih efisien dan lebih cepat bila dibandingkan dengan mikrokontroler CISC konvensional. ATmega32 memiliki fitur-fitur sebagai berikut: 32K bytes *In-System Programmable Flash* dengan kemampuan *Read-While-Write,* 1024 bytes EEPROM, 2K byte SRAM, 32 fungsi umum I/O, 32 *general purpose working registers*, 3 buah *Timer/Counters*, *interrupt* internal dan eksternal, *serial programmable* USART, 1 byte *oriented Two-wire Serial Interface*, 10-bit ADC, *Watchdog Timer* yang dapat diprogram dengan *Internal Oscillator*, SPI *serial port,* serta memiliki 6 pilihan *power saving mode*.

Mikrokontroler AVR diproduksi menggunakan teknologi *high density non-volatile memory on-chip ISP flash* yang memungkinkan program yang ada di dalam memori dapat di program ulang secara langsung di dalam sistem melalui antarmuka serial SPI dengan menggunakan konvensional *non-volatile memory programmer* atau *on-chip boot program* yang berjalan pada inti AVR. *Boot program* dapat menggunakan antarmuka apa saja untuk men-download program pada memori *flash*. Perangkat lunak pada *boot sistem* akan tetap bekerja ketika memori *flash* aplikasi ini sedang di perbaharui, hal ini merupakan operasi "*read-while-write*". Kombinasi antara CPU 8-bit RISC dengan *in system self programmable flash* pada *chip monolithic,* membuat AVR ATmega32 dan AT90S2313 merupakan mikrokontroler powerful yang fleksibel dan merupakan solusi efektif untuk berbagai aplikasi pengontrolan.

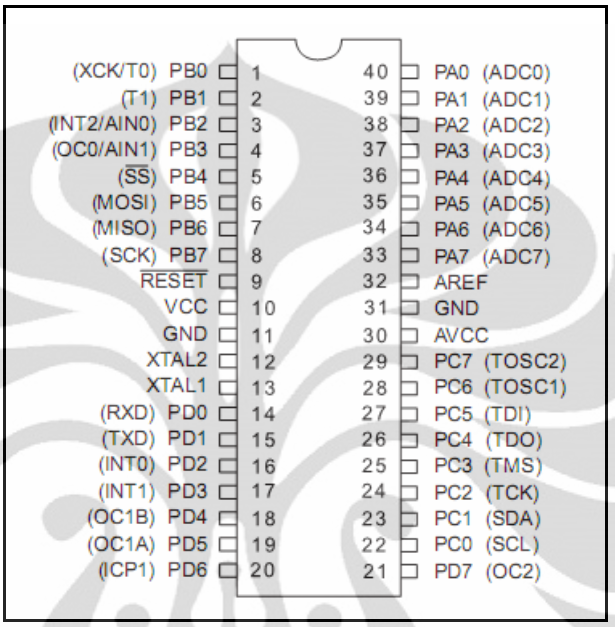
Diagram blok mikrokontroler AVR ATmega32 dapat digambarkan seperti pada Gambar 2.4. berikut ini:



Gambar 2.4. Diagram blok mikrokontroler AVR ATmega32 [8]

2.4.2. Konfigurasi Pin Mikrokontroler AVR ATmega32

Konfigurasi Pin pada mikrokontroler AVR ATmega32 dapat dilihat seperti pada Gambar 2.5. berikut ini:



Gambar 2.5. Konfigurasi pin mikrokontroler AVR ATmega32 [8]

a. *Port* A (PA0-PA7)

Port A merupakan *port* I/O 8-bit bi-directional. Disamping itu *port* A juga dapat berfungsi sebagai analog input untuk ADC. Pin-pin pada *port* ini dapat diberi resistor *pull-up* internal secara invidual. *Buffer port* dapat mencatu arus hingga 200 mA dan dapat secara langsung mengatur LED. Jika semua pin digunakan sebagai input dan eksternal pull-nya *low*, maka semua pin akan menghasilkan sumber arus jika internal pull-up resistor diaktifkan. Pin *port* A merupakan *tree-state* jika kondisi reset dalam keadaan aktif dan jika *clock*-nya tidak berjalan.

Fungsi alternatif pin-pin pada *port* A dapat dilihat pada Tabel 2.2. berikut ini:

Tabel 2.2. Fungsi alternatif pin-pin pada *port* A [8]

Port Pin	Alternate Function
PA7	ADC7 (ADC input channel 7)
PA6	ADC6 (ADC input channel 6)
PA5	ADC5 (ADC input channel 5)
PA4	ADC4 (ADC input channel 4)
PA3	ADC3 (ADC input channel 3)
PA2	ADC2 (ADC input channel 2)
PA1	ADC1 (ADC input channel 1)
PA0	ADC0 (ADC input channel 0)

b. *Port* B (PB0-PB7)

Sama seperti halnya dengan *port* A. *Port* B merupakan *port* I/O 8-bit bi-directional, selain itu *port* B mempunyai fungsi selain sebagai I/O. Fungsi alternatif pin-pin pada *port* B dapat dilihat pada Tabel 2.3. berikut ini:

Tabel 2.3. Fungsi alternatif pin-pin pada *port* B [8]

Port Pin	Alternate Functions
PB7	SCK (SPI Bus Serial Clock)
PB6	MISO (SPI Bus Master Input/Slave Output)
PB5	MOSI (SPI Bus Master Output/Slave Input)
PB4	$\overline{SS}$ (SPI Slave Select Input)
PB3	AIN1 (Analog Comparator Negative Input) OC0 (Timer/Counter0 Output Compare Match Output)
PB2	AIN0 (Analog Comparator Positive Input) INT2 (External Interrupt 2 Input)
PB1	T1 (Timer/Counter1 External Counter Input)
PB0	T0 (Timer/Counter0 External Counter Input) XCK (USART External Clock Input/Output)

c. *Port* C (PC0-PC7)

Port C merupakan *port* I/O 8-bit bi-directional, selain itu *port* C mempunyai fungsi selain sebagai I/O. Fungsi alternatif pin-pin pada *port* C dapat dilihat pada Tabel 2.4. berikut ini:

Tabel 2.4. Fungsi alternatif pin-pin pada *port* C [8]

Port Pin	Alternate Function
PC7	TOSC2 (Timer Oscillator Pin 2)
PC6	TOSC1 (Timer Oscillator Pin 1)
PC5	TDI (JTAG Test Data In)
PC4	TDO (JTAG Test Data Out)
PC3	TMS (JTAG Test Mode Select)
PC2	TCK (JTAG Test Clock)
PC1	SDA (Two-wire Serial Bus Data Input/Output Line)
PC0	SCL (Two-wire Serial Bus Clock Line)

d. *Port* D (PD0-PD7)

Port D merupakan *port* I/O 8-bit bi-directional, selain itu *port* D mempunyai fungsi selain sebagai I/O. Fungsi alternatif pin-pin pada *port* D dapat dilihat pada Tabel 2.5. berikut ini:

Tabel 2.5. Fungsi alternatif pin-pin pada *port* D [8]

Port Pin	Alternate Function
PD7	OC2 (Timer/Counter2 Output Compare Match Output)
PD6	ICP1 (Timer/Counter1 Input Capture Pin)
PD5	OC1A (Timer/Counter1 Output Compare A Match Output)
PD4	OC1B (Timer/Counter1 Output Compare B Match Output)
PD3	INT1 (External Interrupt 1 Input)
PD2	INT0 (External Interrupt 0 Input)
PD1	TXD (USART Output Pin)
PD0	RXD (USART Input Pin)

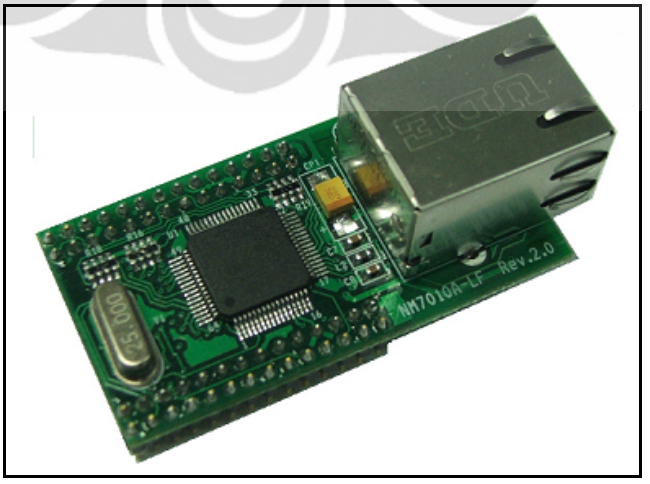
e. VCC : *Power supply*

f. GND : *Ground*

g. RESET : Reset inputan. Kondisi logika *low* "0" lebih dari 50ns pada pin ini akan membuat mikrokontroler masuk ke dalam kondisi reset.
h. XTAL1 : Merupakan input bagi *inverting oscillator amplifier* dan input bagi *clock* internal.
i. XTAL2 : *output inverting oscillator amplifier*.
j. AVCC : Pin *power supply* untuk *port* A dan A/D *converter*. AVCC harus dihubungkan dengan VCC eksternal jika tidak digunakan sebagai ADC. Namun jika digunakan sebagai ADC, maka harus dihubungkan dengan VCC yang dilewati oleh filter *low-pass*.
k. AGND : *Ground* analog (ADC)
l. AREF : Referensi analog untuk ADC.

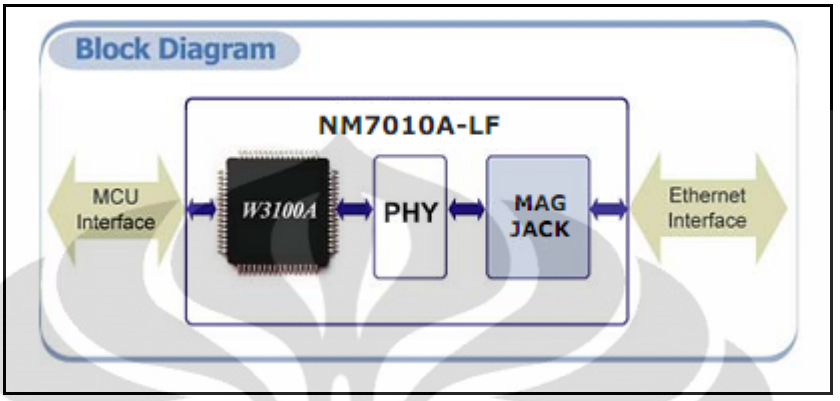
2.5. Modul Ethernet NM7010A-LF

NM7010A-LF merupakan suatu *network module* yang terdiri dari W3100A-LF (TCP/IP *hardwired chip*), Ethernet PHY (RTL8201BL), MAG-JACK (RJ45 dengan X'FMR) dan dengan *glue logics* yang lainnya. Modul tersebut dapat digunakan sebagai komponen untuk menerapkan koneksi internet ke dalam sistem yang dibuat. Pada versi terbaru, untuk menunjang operasi yang lebih stabil penggunaan RTL8201BL sudah digantikan oleh IP101A-LF. Bentuk fisik Modul Ethernet NM7010A-LF dapat dilihat pada Gambar 2.6. sebagai berikut:



Gambar 2.6. Bentuk fisik modul ethernet NM7010A-LF [9]

Diagram blok yang menggambarkan hubungan antara W3100A-LF, Ethernet PHY dan MAG-JACK dapat digambarkan seperti pada Gambar 2.7. sebagai berikut:



Gambar 2.7. Blok diagram modul ethernet NM7010A-LF [9]

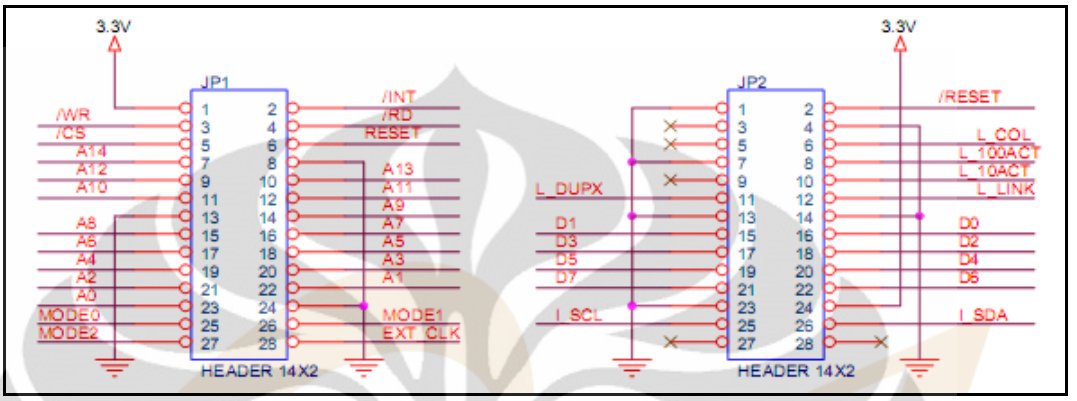
2.5.1. Fitur-fitur Modul NM7010A-LF

Fitur-fitur yang terdapat pada modul NM7010A-LF antara lain sebagai berikut:

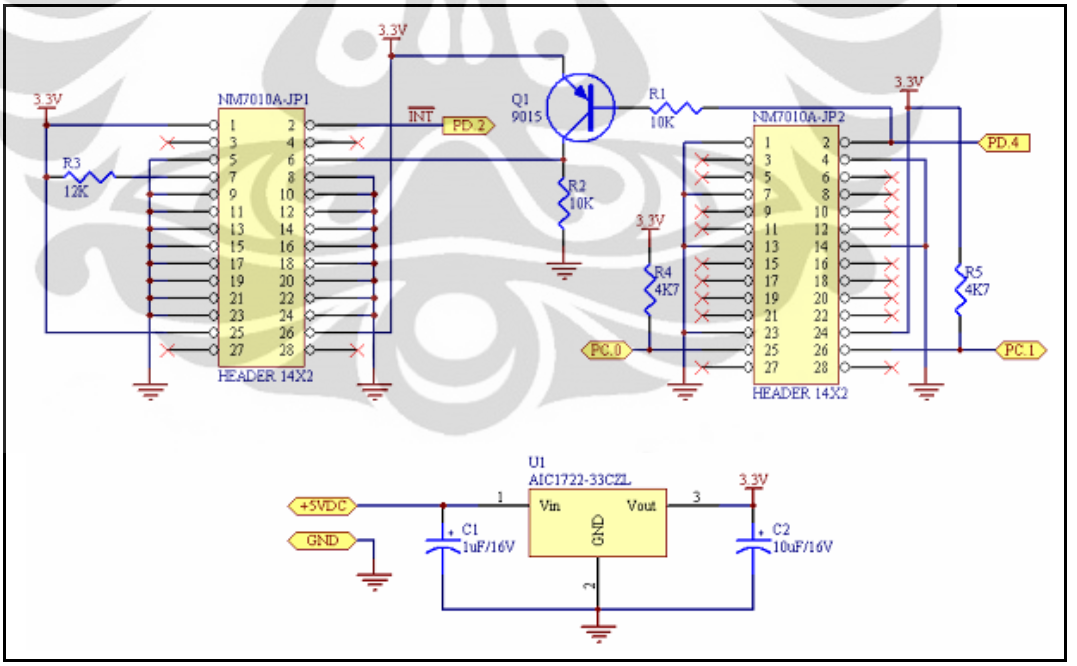
a. Mendukung 10/100 *base* Tx, *half/full duplex*, dan *auto-negotiation*.
b. Sesuai standar IEEE 802.3/802.3u.
c. Catu daya 3,3V dengan toleransi I/O 5V.
d. Tersedia sinyal status jaringan untuk indikator LED.
e. Protokol internet (TCP, IP Ver.4, UDP, ICMP, ARP) dan ethernet (DLC, MAC).
f. Mendukung 4 buah koneksi independen (*socket*) secara simultan.
g. Antarmuka I2C dan bus Intel/Motorola dengan akses *direct*/*indirect*.
h. Mendukung mode *clocked, non-clocked, external clocked*.
i. Mendukung *socket* API untuk memudahkan pemrograman aplikasi.

2.5.2. Pin dan Skema Rangkaian pada Modul NM7010A-LF

Letak pin pada modul NM7010A-LF dan skema rangkaian modul NM7010A-LF dapat dilihat seperti pada Gambar 2.8. dan Gambar 2.9. berikut ini:



Gambar 2.8. Lokasi pin pada modul NM7010A-LF [9]



Gambar 2.9. Skema rangkaian modul NM7010A-LF [9]

Untuk dapat memahami fungsi dari tiap-tiap pin pada modul NM7010A-LF, berikut ini dideskripsikan konfigurasi pin-pin tersebut dalam bentuk tabel. Kode dari tipe tiap-tiap pin, yaitu: I untuk Input, I/O untuk *Bi-directional Input* dan Output, O untuk Output dan P untuk Power.

a. *Power* dan *Ground*

Tabel konfigurasi pin untuk power dan ground dapat dilihat pada Tabel 2.6. berikut ini:

Tabel 2.6. Konfigurasi pin untuk *power* dan *ground* [9]

Symbol	Type	Pin No.	Description
VCC	P	JP1 : 1 , JP2 : 24	**Power** : 3.3 V power supply
GND	P	JP1 : 8, JP1 : 13, JP1 : 24, JP2 : 1, JP2 : 4, JP2 : 7, JP2 : 13, JP2 : 14, JP2 : 23	**Ground**

b. *Network status & LED*

Tabel konfigurasi pin untuk *network status & LED* dapat dilihat pada Tabel 2.7. berikut ini:

Tabel 2.7. Konfigurasi pin untuk *network status & LED* [9]

Symbol	Type	Pin No.	Description
L_COL	O	JP2 : 6	**Collision LED** : Active low when collisions occur.
L_100ACT	O	JP2 : 8	**Link 100/ACT LED** : Active low when linked by 100 Base TX, and blinking when transmitting or receiving data.
L_10ACT	O	JP2 : 10	**Link 10/ACT LED** : Active low when linked by 10 Base T, and blinking when transmitting or receiving data.
L_DUPX	O	JP2 : 11	**Full Duplex LED** : Active low when in full duplex operation. Active high when in half duplex operation.
L_LINK	O	JP2 : 12	**Link LED** : Active low when linked

c. MCU Interfaces

Tabel konfigurasi pin untuk *MCU interfaces* dapat dilihat pada Tabel 2.8. berikut ini:

Tabel 2.8. Konfigurasi pin untuk *MCU interfaces* [9]

Symbol	Type	Pin No.	Description
A14~A8	I	JP1 : 7, JP1 : 10 JP1 : 9, JP1 : 12 JP1 : 11, JP1 : 14 JP1 : 15	**Address / Device Address** :In Bus access mode is used as Address[14-8] pin In I^2C interface mode is used as device address[6-0] pin
A7~A0	I	JP1 : 16 ~ JP1 : 23	**Address :** In Bus access mode is used as Address[7-0] pin In I^2C interface mode, these pins are not used, so leave them NC or ground them.
D7~D0	I/O	JP2 : 21, JP2 : 22, JP2 : 19, JP2 : 20, JP2 : 17, JP2 : 18 JP2 : 15, JP2 : 16	**Data** : 8 bit-wide data bus
/CS	I	JP1 : 5	**Module Select** : Active low. /CS of W3100A-LF
/RD	I	JP1 : 4	**Read Enable** : Active low. /RD of W3100A-LF
/WR	I	JP1 : 3	**Write Enable** : Active low /WR of W3100A-LF
/INT	O	JP1 : 2	**Interrupt** : Active low After reception or transmission it indicates that the W3100A-LF requires MCU attention. By writing values to the Interrupt Status Register of W3100A-LF the interrupt will be cleared. All interrupts can be masked by writing values to the IMR of W3100A-LF(Interrupt Mask Register). For more details refer to the W3100A-LF Datasheet
I_SCL	I	JP2 : 25	**SCL** : Used as clock by I^2C interface mode. Internally pull-down
I_SDA	I/O	JP2 : 26	**SDA** : Used as data by I^2C interface mode. Internally pull-down

d. Miscellaneous Signals

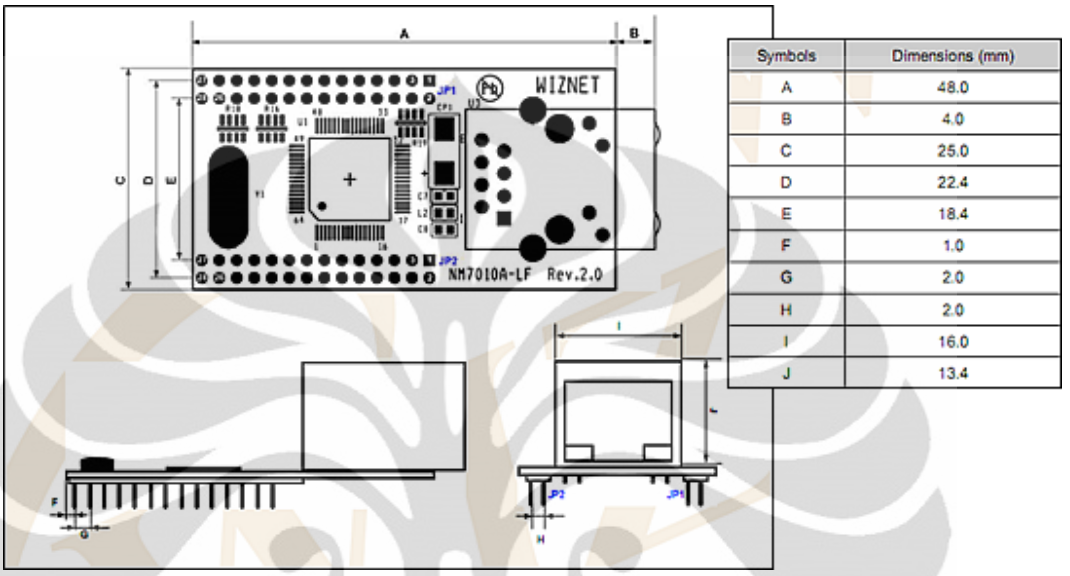
Tabel konfigurasi pin untuk *miscellaneous signals* dapat dilihat pada Tabel 2.9. berikut ini:

Tabel 2.9. Konfigurasi pin untuk *miscellaneous signals* [9]

<table>
<tr><th>Symbol</th><th>Type</th><th>Pin No.</th><th>Description</th></tr>
<tr><td>RESET</td><td>I</td><td>JP1 : 6</td><td>Reset : Active high
Initializes or Reinitializes the W3100A-LF. Asserting this pin will force a reset process to occur, which will result in all internal registers reinitializing to their default and all strapping options are reinitialized.
For complete reset function, this pin must be asserted low for at least 10us. Refer to W3100A-LF datasheet for further detail regarding reset.</td></tr>
<tr><td>/RESET</td><td>I</td><td>JP2 : 2</td><td>Reset : Active low
Reset RTL8201BL chip. For complete reset function this pin must be asserted low for at least 10ms.</td></tr>
<tr><td>MODE1~0</td><td>I</td><td>JP1 : 26 ,
JP1 : 25</td><td>Mode Select : These pins select MCU interface and operating mode. Since each pin is pull-down internally, clocked mode (the default mode) is selected when these pins are not connected.
<table>
<tr><th>M1 M0</th><th>Mode</th></tr>
<tr><td>0 0</td><td>Clocked</td></tr>
<tr><td>0 1</td><td>External clocked</td></tr>
<tr><td>1 0</td><td>Non-clocked</td></tr>
<tr><td>1 1</td><td>I^2C interface</td></tr>
</table>
Refer to W3100A-LF datasheet for further detail regarding mode select</td></tr>
<tr><td>EXT_CLK</td><td>I</td><td>JP1 : 28</td><td>External clock : supplementary clock used for external clocked mode.
In external clocked mode, W3100A-LF uses this clock to interface with MCU.
Refer to W3100A-LF datasheet for further detail regarding external clock.</td></tr>
<tr><td>NC</td><td>-</td><td>JP1 : 27, JP2 : 3
JP2 : 5, JP2 : 9
JP2 : 27, JP2 : 28</td><td>Not Connect</td></tr>
</table>

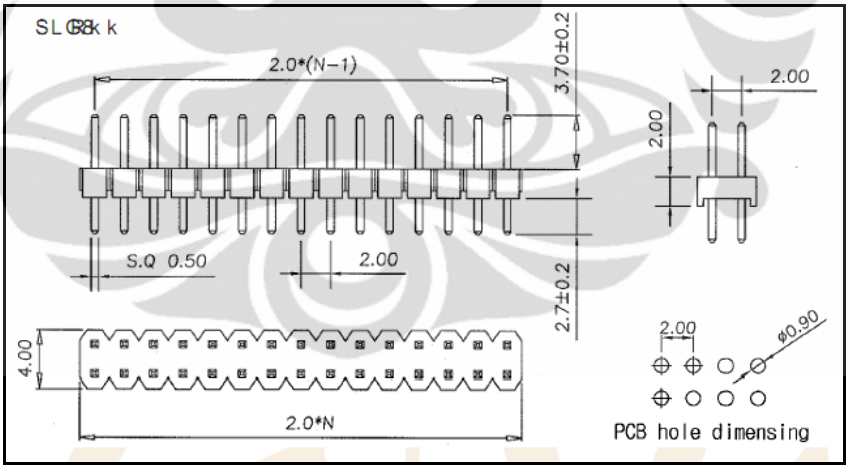
2.5.3. Dimensi dan Spesifikasi Konektor pada Modul NM7010A-LF

Dimensi modul NM7010A-LF dan spesifikasi konektor modul NM7010A-LF dapat dilihat pada Gambar 2.10. dan 2.11. berikut ini:



Symbols	Dimensions (mm)
A	48.0
B	4.0
C	25.0
D	22.4
E	18.4
F	1.0
G	2.0
H	2.0
I	16.0
J	13.4

Gambar 2.10. Dimensi modul NM7010A-LF [9]

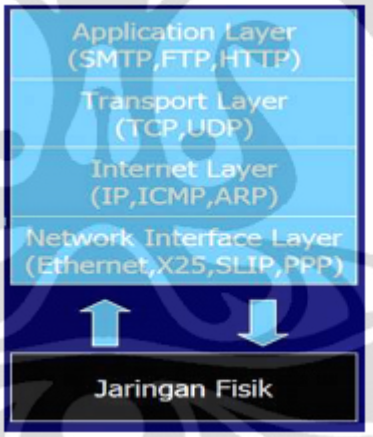


Gambar 2.11. Spesifikasi konektor modul NM7010A-LF [9]

2.6. Konsep Dasar TCP/IP

Komunikasi data merupakan proses pengiriman data dari satu komputer ke komputer yang lain. Untuk dapat mengirimkan data, pada komputer harus ditambahkan alat khusus, yang dikenal sebagai *network interface* (antarmuka jaringan). Jenis antarmuka jaringan ini bermacam-macam, bergantung pada media

fisik yang digunakan untuk mentransfer data tersebut. Dalam proses pengiriman data ini terdapat beberapa masalah yang harus dipecahkan. Pertama, data harus dapat dikirimkan ke komputer yang tepat sesuai tujuan, dan data harus dalam keadaan utuh tanpa kerusakan (kerusakan data dapat terjadi jika ada interferensi sinyal dari luar atau komputer tujuan berada jauh secara jaringan). Karenanya perlu ada mekanisme yang dapat mencegah rusaknya data, dengan membuat beberapa aturan yang saling bekerja sama satu sama lainnya. Sekumpulan aturan untuk mengatur proses pengiriman data ini disebut sebagai protokol komunikasi data. Protokol ini diimplementasikan dalam bentuk program komputer yang terdapat pada komputer dan peralatan komunikasi lainnya. TCP/IP adalah salah satu protokol yang didesain untuk melakukan fungsi-fungsi komunikasi data tersebut. Protokol TCP/IP dimodelkan dengan empat layer TCP/IP, dengan susunan seperti terlihat pada Gambar 2.12. berikut:



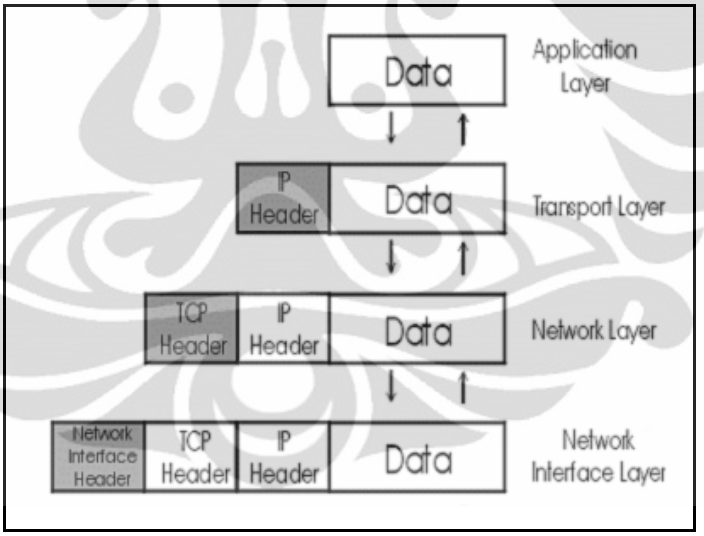
Gambar 2.12. Susunan layer pada protokol TCP/IP

TCP/IP terdiri atas empat layer protokol yang bertingkat. Keempat layer tersebut adalah:

a. *Network Interface Layer*, bertanggungjawab mengirim dan menerima data ke dan dari media fisik.
b. *Internet Layer*, bertanggungjawab dalam proses pengiriman paket ke alamat yang tepat.
c. *Transport Layer*, bertanggungjawab untuk mengadakan komunikasi antara dua host/komputer.

d. *Application Layer*, pada layer inilah terletak semua aplikasi yang menggunakan protokol TCP/IP ini.

Dalam TCP/IP, terjadi penyampaian data dari protokol yang berada di satu layer ke protokol yang berada pada layer dibawahnya. Setiap protokol memperlakukan informasi yang diterimanya dari protokol lain sebagai data. Jika suatu protokol menerima data dari protokol lain di layer atasnya, akan ditambahkan informasi tambahan miliknya yang disebut *header* ke data tersebut. Informasi ini memiliki fungsi yang sesuai dengan fungsi protokol. Setelah itu data diteruskan lagi ke protokol pada layer dibawahnya. Hal yang sebaliknya terjadi disisi penerima jika suatu protokol menerima data dari protokol lain yang berada pada layer di bawahnya. Jika data ini dianggap valid, protokol akan melepas *header* tersebut, untuk kemudian meneruskan data itu ke protokol yang berada pada layer diatasnya. Penambahan *header* umumnya disebut dengan enkapsulasi yang dapat digambarkan seperti pada Gambar 2.13. berikut ini:



Gambar 2.13. Enkapsulasi pada protokol TCP/IP

2.7. Alat Pengembangan

Setelah memasuki tahapan pembangunan sistem, maka diperlukan penggunaan alat pengembangan agar proses pengerjaan sistem ini berjalan dengan efektif dan efisien. Terdapat berbagai macam alat pengembangan yang dapat digunakan untuk membangun sebuah pangkalan data berbasis web. Pada sistem ini akan digunakan bahasa scripting PHP, DBMS MySQL, TCP/IP Starter kit dan

web server XAMPP (*basic package*) versi 1.6.3a. IDE/alat lainnya yang digunakan adalah Macromedia Dreamweaver MX dan Mozilla Firefox/3.5.18. Alat pengembangan untuk untuk pemrograman modul kontrol akses menggunakan KR-125R USB ISP, Bascom AVR Compiler 1.11.9.2 dan Avr-Osp II.

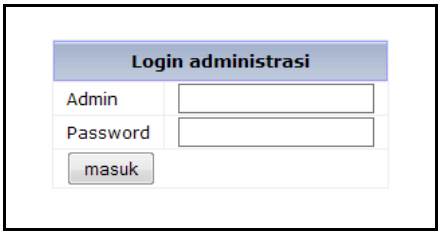
BAB 3
PERANCANGAN SISTEM

3.1. Deskripsi Sistem

Modul kontrol akses digunakan untuk mengendalikan akses suatu subjek terhadap objek. Sebelum masuk ke dalam sistem, pengguna diharuskan untuk login melalui halaman login pada aplikasi pangkalan data berbasis web. Selain *username* dan *password* yang melambangkan identitas subjek, sistem juga mengidentifikasi entitas lain berupa alamat IP dan serial number. Dengan demikian layanan kontrol akses yang diterapkan adalah 3 dari 4 faktor yaitu: Sesuatu yang diketahui, seperti password; Sesuatu yang dimiliki, seperti modul kontrol akses dan *random key*; dan Posisi dimana berada, yakni di dalam jaringan yang diketahui alamat IP-nya.

3.2. Spesifikasi dan Fungsi Sistem

Perancangan merupakan tahapan yang penting dalam pembuatan suatu sistem, sehingga dengan perancangan yang baik diharapkan akan dihasilkan suatu sistem yang sesuai dengan fungsi dan tujuan dari pembuatan sistem tersebut. Pada perancangan ini terdiri dari beberapa tahapan seperti menentukan spesifikasi dan fungsi dari sistem, menentukan cara kerja sistem, mengidentifikasi hal-hal yang dibutuhkan sistem dan menentukan alat bantu yang digunakan untuk pembuatan sistem. Sistem yang dirancang merupakan sistem berbasis mikrokontroler AVR ATmega32 yang berfungsi untuk mensimulasikan kontrol akses pada proses login ke dalam pangkalan data. Sistem menampilkan hasil identifikasi subjek dengan menggunakan suatu antarmuka pemakai yang berbentuk halaman web. Antarmuka pada saat penguna login dapat dilihat seperti pada Gambar 3.1. berikut:



Gambar 3.1. Antarmuka login pangkalan data berbasis web

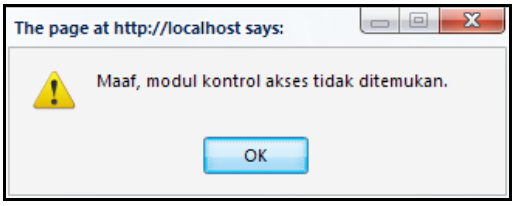
3.3. Cara Kerja Sistem

Sistem bekerja dengan meminta masukan identitas subjek berupa *username* dan *password* dengan menampilkan form seperti Gambar 3.1. diatas. Kemudian web server meminta keterangan pada modul kontrol akses tentang keabsahan subjek dan posisi subjek saat login. Jika modul kontrol akses ditemukan, web server mengirimkan sinyal tanda koneksi dapat dilanjutkan. Pengecekan modul dilakukan dengan perintah kode program seperti pada Gambar 3.2. berikut ini:

```
Function isModulConnected()) {
$ip="192.168.1.8";
$fp=fsockopen($ip, 80, $errno, $errstr, 3);
      if (!$fp){
            $result = false;
      } else {
            $result = true;
            fclose ($fp);
      }
      return $result;
}
```

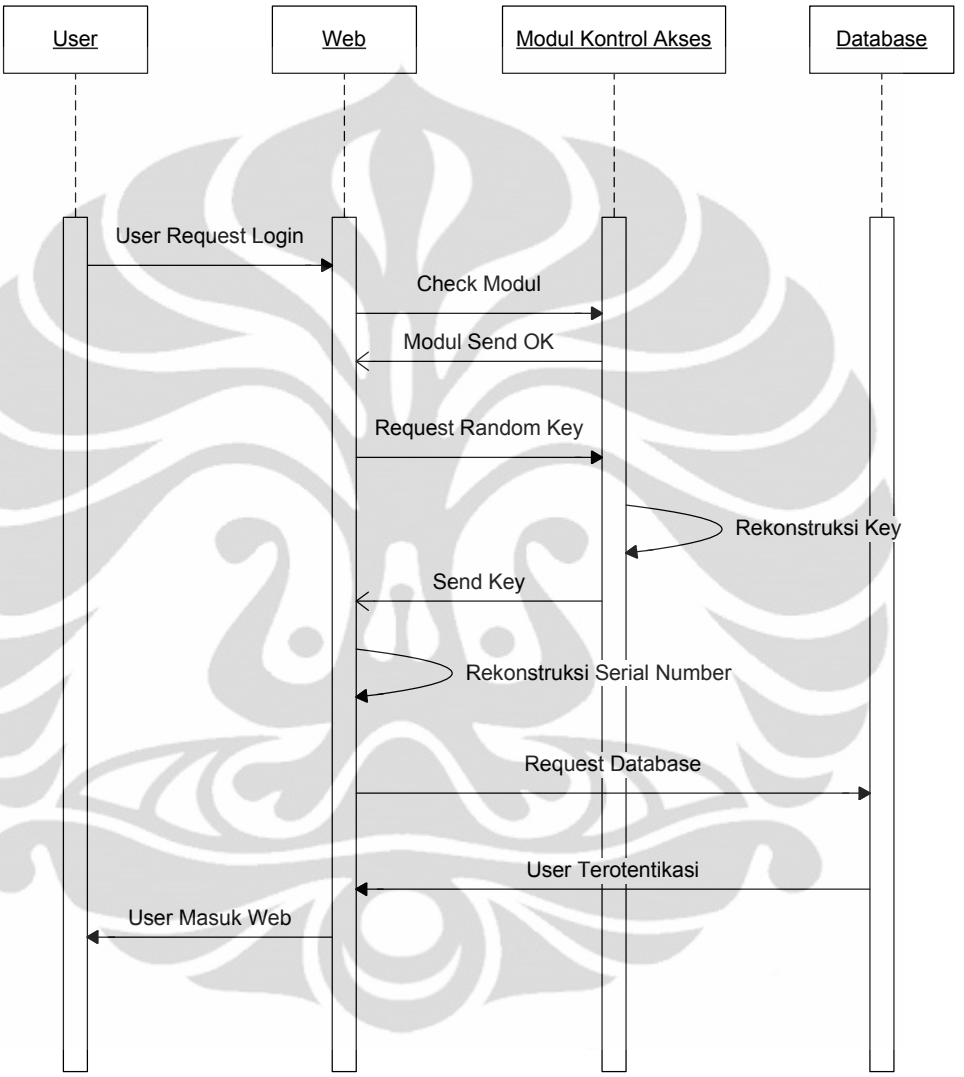
Gambar 3.2. Kode program untuk pengecekan modul terpasang

Web server kemudian meminta *random key* kepada modul untuk subjek sesuai *username* dan *password* yang dimasukkan. Sebelum memberikan random key yang dibutuhkan, modul kontrol akses melakukan pengecekan format data yang dikirimkan oleh *web server*. Setelah format di terima, *Random key* tersebut kemudian di rekonstruksi oleh sistem dengan protokol kriptografi *secret splitting*. Rekonstruksi menghasilkan serial number yang akan dicocokkan dengan pola pada pangkalan data. Jika hasilnya sesuai dengan pola pada pangkalan data milik admin, subjek dibolehkan mengakses pangkalan data sesuai dengan kewenangannya. Ketika *web server* tidak menemukan modul kontrol akses karena diluar jaringan atau tidak terpasang, maka sistem menampilkan pesan kesalahan seperti pada Gambar 3.3. berikut ini:



Gambar 3.3. Pesan kesalahan karena modul tidak ditemukan

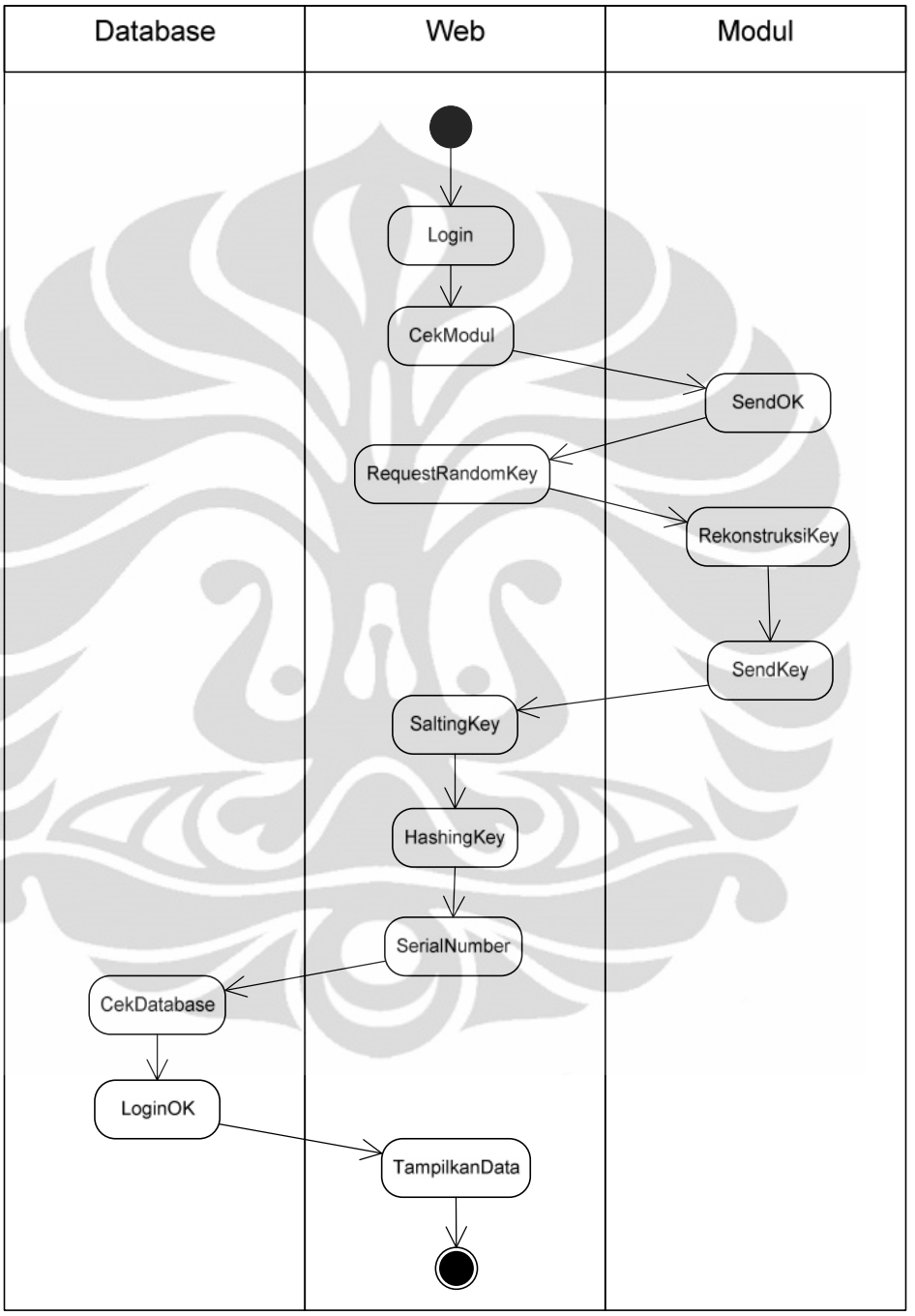
Urutan komunikasi yang terjadi antara komponen yang satu dengan yang lainnya pada sistem dapat digambarkan seperti terlihat pada Gambar 3.4. berikut ini:



Gambar 3.4. Komunikasi antar komponen sistem

Langkah-langkah atau alur kerja dari keseluruhan sistem yang akan dibuat, termasuk untuk mengetahui operasi-operasi yang akan dilakukan oleh masing-masing komponen pada sistem. Digambarkan dengan menggunakan salah satu diagram yang ada pada UML, yaitu dengan menggunakan suatu *activity diagram.*

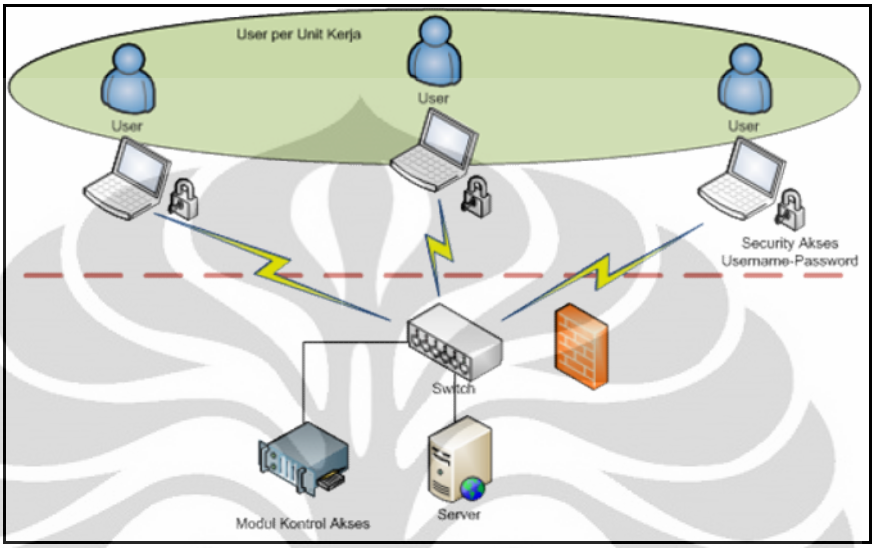
Activity diagram untuk operasi-operasi yang dilakukan oleh masing-masing komponen pada sistem, dapat digambarkan seperti terlihat pada Gambar 3.5. berikut ini:



Gambar 3.5. Activity diagram dari sistem kontrol akses

3.4. Arsitektur Sistem

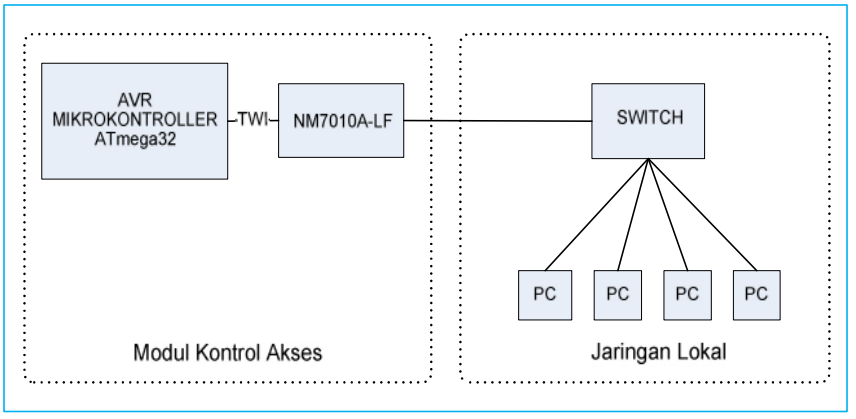
Secara umum sistem yang dirancang dapat dilihat seperti pada Gambar 3.6. berikut ini:



Gambar 3.6. Arsitektur sistem secara umum

3.4.1. Perancangan Perangkat Keras

Perancangan perangkat keras dapat digambarkan dengan diagram blok seperti yang ditunjukkan oleh Gambar 3.7. Dari gambar tersebut terlihat bahwa modul kontrol akses terdiri dari blok mikrokontroler dan modul jaringan NM7010A-LF yang berfungsi sebagai jembatan antara mikrokontroler dengan jaringan lokal. Protokol komunikasi antara mikrokontroler dengan NM7010A-LF menggunakan *Two Wire Interface* (TWI).



Gambar 3.7. Diagram blok perangkat keras sistem

Dari diagram blok pada Gambar 3.7. di atas, akan dijelaskan masing-masing bagian, yaitu sebagai berikut:

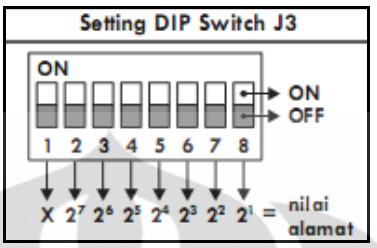
a. Mikrokontroler

Sebagai pusat pengolahan data digunakan mikrokontroler ATmega32. ATmega32 memiliki kapasitas memori SRAM dan *flash* yang cukup besar, yaitu masing-masing sebesar 1024 byte dan 32 KB. Selain itu, ATmega32 juga dilengkapi dengan beberapa fitur antara lain adanya pin TWI data (SDA) dan TWI clock (SCL) yang merupakan pin *Two Wire Interface* yang akan digunakan sebagai antarmuka dengan modul jaringan NM7010A-LF. Pada pin SDA (*Port* C1) dan SCL (*Port* C0) dipasang resistor *pull-up* sebesar 4.7 kΩ. Untuk memudahkan proses penanaman program dalam mikrokontroler ATmega32, digunakan sistem minimum DT-AVR *Low Cost Micro System* dari Innovative Electronics yang sudah dilengkapi dengan *In-Sistem Programming* (ISP) *downloader*.

b. Modul jaringan NM7010A-LF

Modul jaringan NM7010A-LF ini digunakan sebagai jembatan antara mikrokontroler dengan jaringan lokal. Fungsinya adalah mengubah format data yang dikirim dari mikrokontroler menjadi format data TCP/IP, dan sebaliknya. Pada perancangan NM7010A-LF dikonfigurasi dengan mode I2C. Untuk pemilihan mode ini diatur oleh pin MODE0 dan MODE1. Pin MODE0 dan MODE1 harus diberi logika 1 untuk konfigurasi I2C. Untuk itu, pin-pin ini dihubungkan dengan Vcc. Untuk pemilihan alamat I2C-nya, dapat diatur dengan memilih alamat sesuai dengan yang dikehendaki melalui saklar DIP *Switch* 8. Pada mode I2C, pin SDA, SCL, INT, dan RST inilah yang akan dihubungkan dengan mikrokontroler.

Posisi DIP *Switch* untuk melakukan pengaturan alamat dapat dilihat pada Gambar 3.8. dibawah ini:

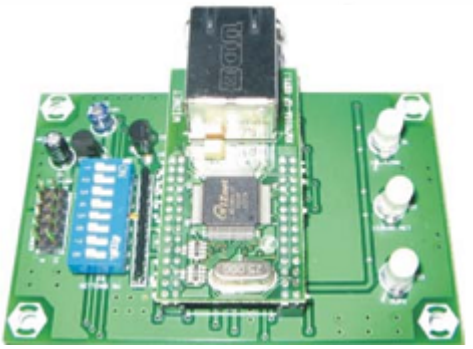


Gambar 3.8. DIP *Switch* alamat I2C [9]

Alamat I2C ditentukan oleh posisi saklar nomor 2 s.d. saklar nomor 8, sedangkan saklar nomor 1 tidak digunakan. Nilai alamat didapatkan dengan menjumlahkan nilai saklar yang berada pada posisi OFF. Misalnya saklar 2, 3, 6, 8 pada posisi OFF dan saklar 4, 5, 7 pada posisi ON maka alamat modul adalah: $2^7 + 2^6 + 2^3 + 2^1 = 202$ (desimal) atau CA (heksadesimal).

c. TWI

Two Wire Interface (TWI) digunakan sebagai protokol komunikasi antara mikrokontroler dengan modul jaringan NM7010A-LF. Untuk memudahkan dalam evaluasi TWI pada modul jaringan NM7010A-LF, digunakan TCP/IP *Starter Kit*. Perangkat tersebut dapat dilihat seperti pada Gambar 3.9. berikut ini:



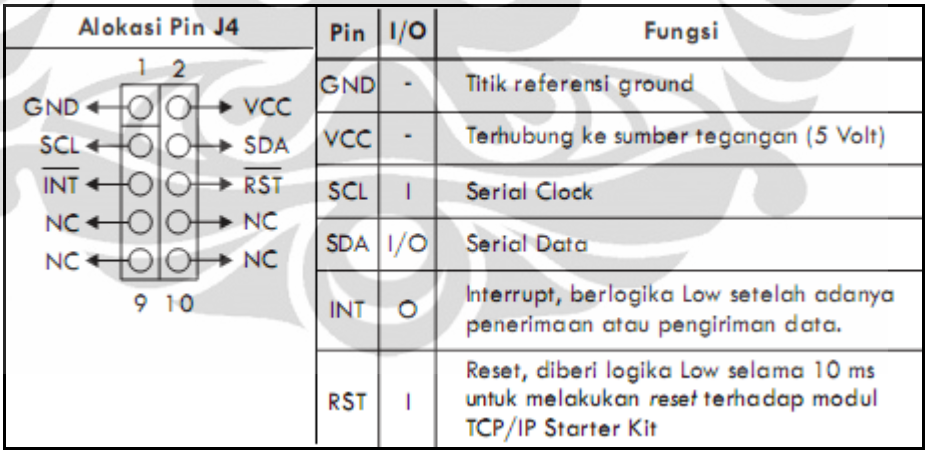
Gambar 3.9. TCP/IP *Starter Kit* [9]

TCP/IP *Starter Kit* sudah dilengkapi dengan LED (COL/LINK, 10/100 ACT, dan DUPX) yang dapat memperlihatkan kondisi konektivitas jaringan. Jika modul TCP/IP *Starter Kit* berfungsi dengan baik, LED akan menyala hijau semua. Kondisi tersebut dapat dilihat seperti pada Tabel 3.1. sebagai berikut:

Tabel 3.1. LED penanda konektivitas jaringan [9]

Kondisi / LED	Menyala		Padam
	Oranye	Hijau	
COL/LINK	Collision	Link	-
10/100 ACT	10Mbps	100Mbps	No activity
DUPX	-	Full duplex	Half duplex

Untuk menghubungkan mikrokontroler AVR ATmega32 dengan NM7010A-LF perlu diketahui terlebih dahulu fungsi dari tiap-tiap pin pada modul TCP/IP *Starter Kit*. Alokasi pin pada TCP/IP *Starter Kit* beserta fungsinya dapat dilihat pada Gambar 3.10. berikut ini:



Pin	I/O	Fungsi
GND	-	Titik referensi ground
VCC	-	Terhubung ke sumber tegangan (5 Volt)
SCL	I	Serial Clock
SDA	I/O	Serial Data
INT	O	Interrupt, berlogika Low setelah adanya penerimaan atau pengiriman data.
RST	I	Reset, diberi logika Low selama 10 ms untuk melakukan *reset* terhadap modul TCP/IP Starter Kit

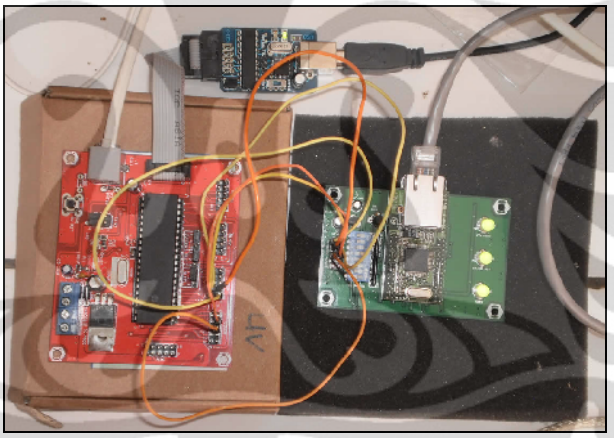
Gambar 3.10. Alokasi pin pada TCP/IP *Starter Kit* [9]

Hubungan antara mikrokontroler AVR ATmega32 dengan NM7010A-LF melalui TCP/IP *Starter Kit dapat* dilihat pada Tabel 3.2. berikut ini:

Tabel 3.2. Hubungan AVR dengan NM7010A-LF [9]

TCP/IP Starter Kit J4	DT-AVR Low Cost Micro System
GND (pin 1)	GND (PORTC pin 1)
VCC (pin 2)	VCC (PORTC pin 2)
SCL (pin 3)	PC.0 (PORTC pin 3)
SDA (pin 4)	PC.1 (PORTC pin 4)
INT (pin 5)	PD.2 (PORTD pin 5)
RST (pin 6)	PD.4 (PORTD pin 7)

Rangkaian perangkat keras sistem secara lengkap dapat dilihat seperti pada Gambar 3.11. berikut ini:



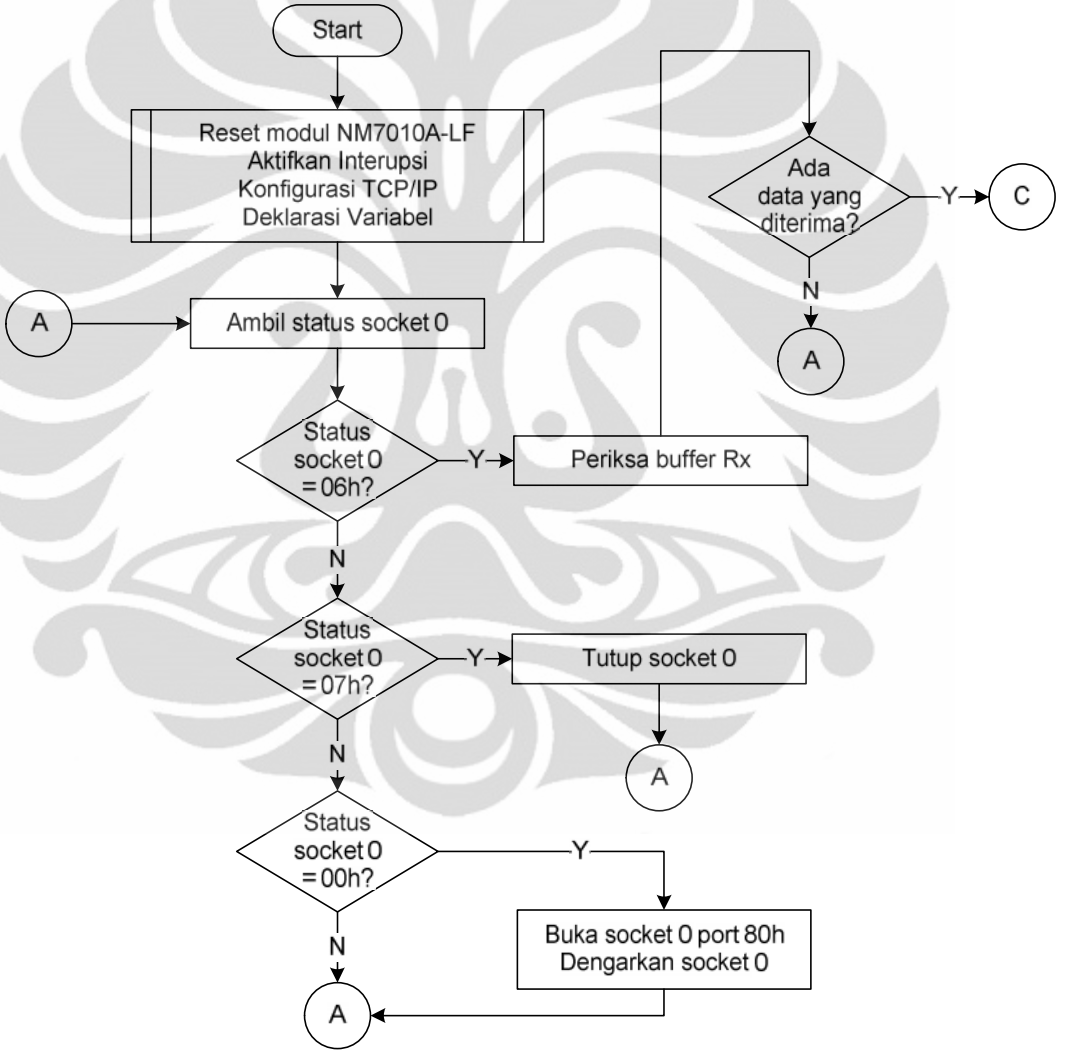
Gambar 3.11. Rangkaian perangkat keras sistem

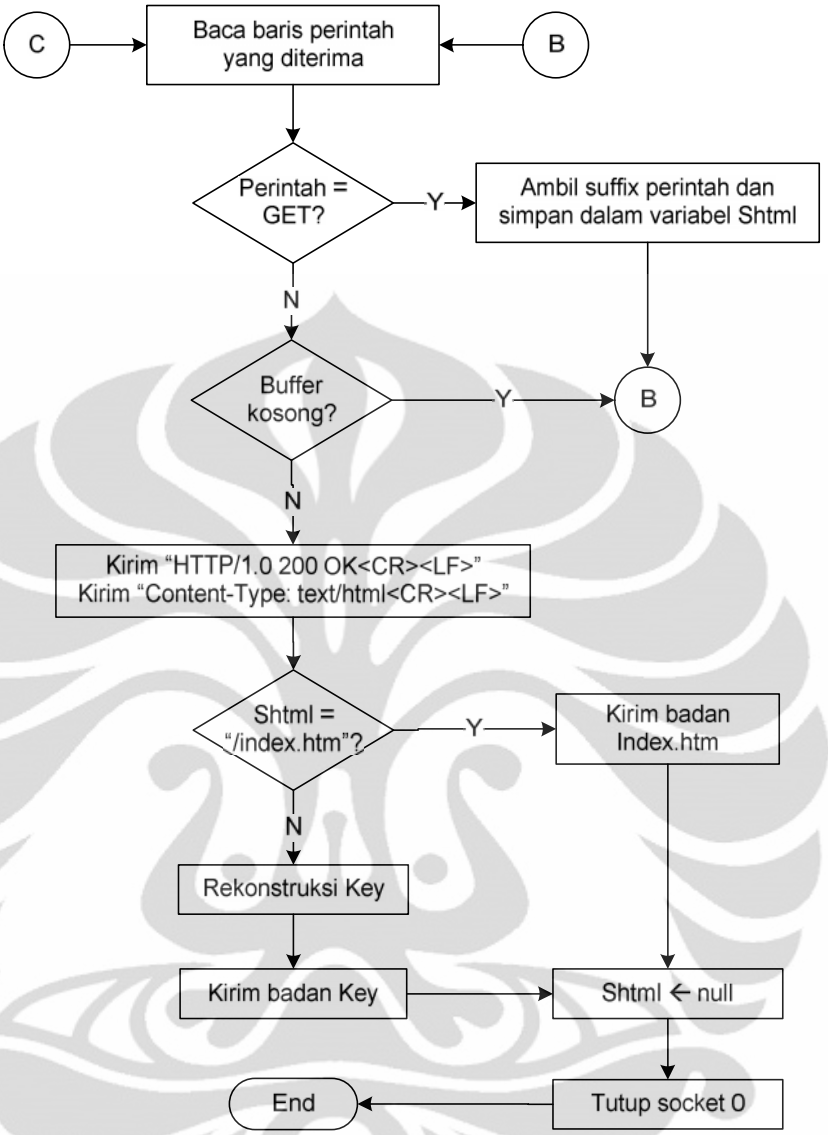
d. *Switch*

Switch digunakan untuk menghubungkan modul kontrol akses dengan komputer pada jaringan lokal. Pada sistem ini, modul berdiri sendiri dan bertindak seperti sebuah *web server*. Simulasi sistem tanpa *switch* dapat dilakukan dengan menghubungkan secara langsung antara modul kontrol akses dengan komputer pengguna yang memiliki konektor MAG-Jack, dengan menggunakan kabel UTP yang kedua ujungnya diberi terminasi RJ-45 dan bertipe *crossover*.

3.4.2. Perancangan Perangkat Lunak

Perancangan perangkat lunak di bagi menjadi 2 yaitu: perancangan program pada mikrokontroler dan program pada halaman web. Program pada mikrokontroler ini ditulis dengan menggunakan BASCOM AVR 1.11.9.2 sebagai *compiler*-nya. Diagram alir program pada mikrokontroler dapat dilihat seperti pada Gambar 3.12. berikut:





Gambar 3.12. Diagram alir program pada mikrokontroler

Langkah pertama yaitu inisialisasi mikrokontroler dan modul jaringan terlebih dahulu yang meliputi jenis mikrokontroler, alamat IP, alamat MAC, dan sebagainya. Inisialisasi mikrokontroler dan modul jaringan dilakukan dengan perintah kode program seperti pada Gambar 3.13. berikut ini:

```
Config Tcpip = Int0 , Mac = 12.128.12.34.56.78 , Ip = 192.168.1.8
, Submask = 255.255.255.0 , Gateway = 192.168.1.1 , Localport =
1000 , Tx = $55 , Rx = $55 , Twi = &HCC , Clock = 300000
```

Gambar 3.13. Kode program untuk inisialisasi mikrokontroler

Langkah selanjutnya program mengambil status dari socket 0. Bila status socket 0 = *established* (06h) maka program akan memeriksa *buffer* Rx dari modul NM7010A, dan jika ada data yang diterima dalam *buffer* Rx maka program akan membacanya. Bila data yang diterima adalah perintah "GET" maka program akan menyimpan awalan yang mengikuti perintah tersebut ke dalam variabel Shtml. Program akan memeriksa apakah *buffer* Rx sudah kosong, bila belum kosong maka program akan kembali membaca. Jika *buffer* Rx sudah kosong maka program mengirimkan "HTTP/1.0 200 OK" dan mengirimkan "Content-Type: text/html" (format body html yang akan dikirimkan). Pembacaan format dan penyimpanan perintah ke dalam variable Shtml dilakukan dengan perintah kode program seperti pada gambar 3.14. berikut ini:

```
Do
Tempw = Tcpread(0 , S)
If Left(s , 3) = "GET" Then
      Gosub Page
End If
Loop Until S = ""
Tempw = Tcpwrite(0 , "HTTP/1.0 200 OK{013}{010}")

Page:
   P1 = Instr(s , " ")
   P1 = P1 + 1
   P2 = Instr(p1 , S , " ")
   P2 = P2 - P1
   Shtml = Mid(s , P1 , P2)
   Shtml = Lcase(shtml)
Return
```

Gambar 3.14. Kode program untuk pembacaan format

Setelah itu, cek nilai Shtml. Jika Shtml = "/index.htm" maka program akan mengeksekusi perintah program yang terdapat dalam fungsi tersebut dan program akan mengirimkan badan html-nya. Jika Shtml ≠ "/index.htm" maka program akan melakukan rekonstruksi key dan mengirimkan badan html-nya. Alamat atau nilai Shtml inilah yang menjadi acuan dari eksekusi program.

Format dan pengiriman badan html dilakukan dengan perintah kode program seperti pada Gambar 3.15. berikut ini:

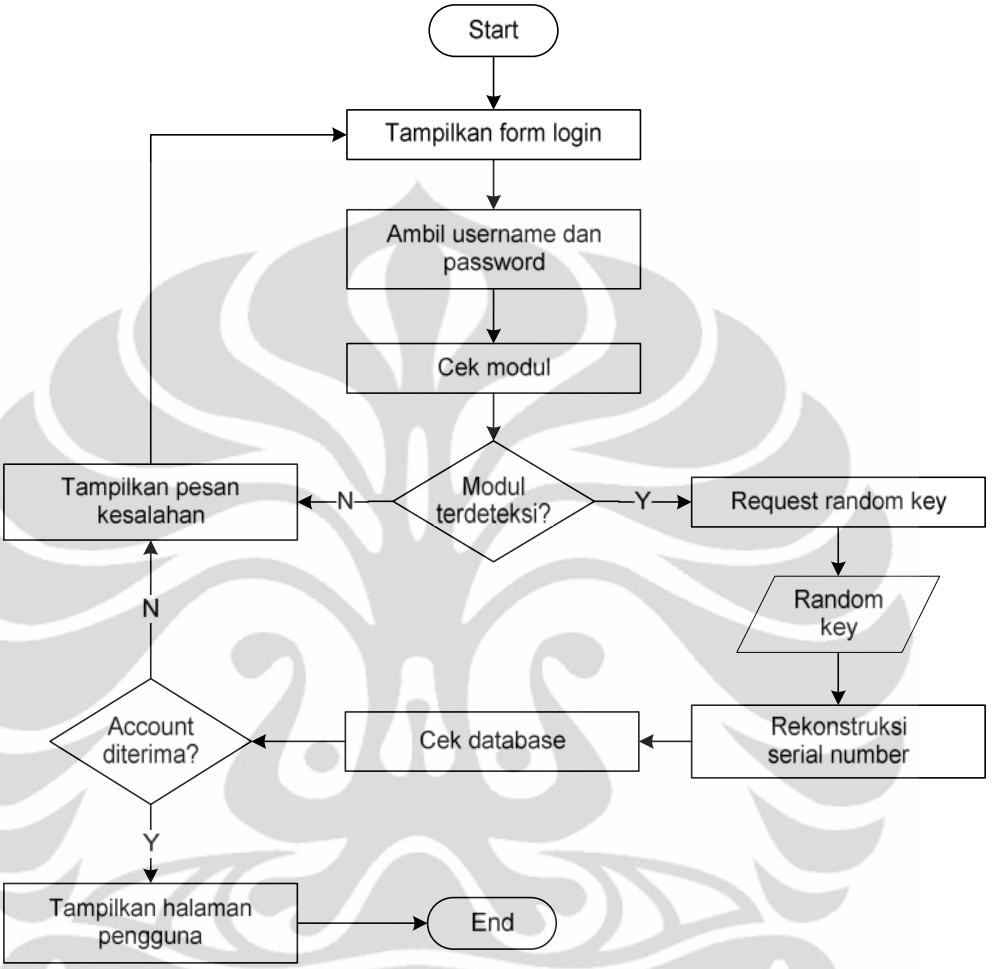
```
Stuur:
   Dim Wsize As Word
   Tempw = Tcpwrite(0 , "Content-Type: text/html{013}{010}")
   If Shtml = "/index.htm" Then
      S    =    "<html><head><title>    Modul    Kontrol    Akses
</title></head><body><p><b>Status            modul            sudah
terpasang<br></b></p></body></html>"
      Wsize = Len(s)
      Sheader = "Content-Length: " + Str(wsize) + "{013}{010}"
      Tempw = Tcpwritestr(0 , Sheader , 255)
      Tempw = Tcpwrite(0 , S , Wsize)
   Else
      Gosub Rekonstruksi
      S    =    "<html><head><title>    Modul    Kontrol    Akses
</title></head><body><p><b>"  +  Shtml  +  "<br></b>"  +  Snumber  +
"</p></body></html>"
      Wsize = Len(s)
      Sheader = "Content-Length: " + Str(wsize) + "{013}{010}"
      Tempw = Tcpwritestr(0 , Sheader , 255)
      Tempw = Tcpwrite(0 , S , Wsize)
   End If
   Shtml = ""
Return
```

Gambar 3.15. Kode program untuk pengiriman badan html

Setelah semua badan HTML terkirim, program akan menghapus isi variabel Shtml, lalu menutup *socket* 0. Bila status socket 0 = *wait connection close* (07h) maka program akan menutup *socket* 0 dan kembali ke langkah A. Bila status *socket* 0 = *connection closed* (00h) maka program membuka *port* 80h socket 0 dan mulai mendengarkan jaringan dari *socket* 0, lalu program kembali ke langkah awal.

Program pada halaman web ditulis menggunakan bahasa pemrograman PHP dan pangkalan data MySQL.

Diagram alir program pada halaman web dapat dilihat seperti pada Gambar 3.16. berikut:



Gambar 3.16. Diagram alir program pada halaman web

Program akan meminta masukan identitas subjek berupa *username* dan *password* dan mengecek keberadaan modul kontrol akses dengan fungsi isModulConnected(). Jika modul tidak terpasang, pengguna menerima pesan kesalahan dan halaman web kembali ke *form* login. Jika modul terpasang, *server* meminta *random key* ke modul dan melakukan rekonstruksi *serial number*. Setelah didapatkan *serial number*, server melakukan otentikasi ke pangkalan data. Bila pola yang dikirim cocok dengan pola yang ada di pangkalan data, halaman untuk pengguna ditampilkan. Jika data tidak cocok, tampil pesan kesalahan dan program kembali menampilkan *form* login.

Pengecekan pangkalan data dilakukan dengan perintah kode program seperti pada Gambar 3.17. berikut ini:

```
If (isset($_REQUEST["namalogin"]) && isset($_REQUEST["password"]))
{
      $namalogin = stripslashes($_REQUEST["namalogin"]);
      $password = stripslashes($_REQUEST["password"]);
      $sql = "SELECT id, namalogin, namalengkap, hakakses FROM
admin WHERE namalogin='" . $namalogin . "' AND password=md5('" .
$password . "')";
      $res = mysql_query($sql);
      if (mysql_num_rows($res)>0) {
            $row = mysql_fetch_assoc($res);
            $namalogin = $row["namalogin"];
            $namalengkap = $row["namalengkap"];
            $id = $row["id"];
            $hakakses = $row["hakakses"];
}
```

Gambar 3.17. Kode program untuk pengecekan pangkalan data

3.4.3. Perancangan Tabel Pangkalan Data

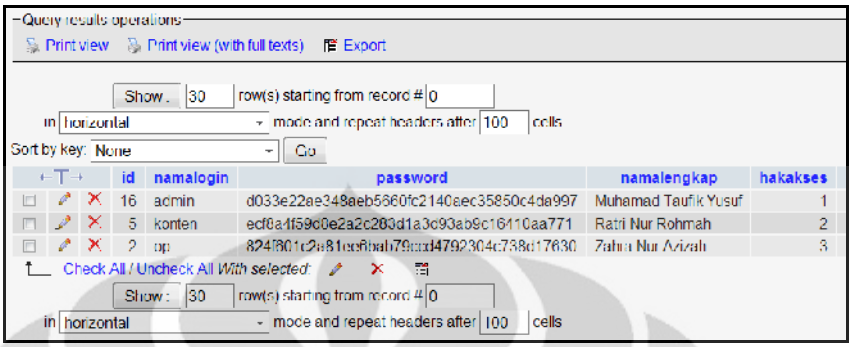
Pangkalan data dibuat hanya satu dengan satu tabel admin di dalamnya. Tabel tersebut dialokasikan untuk menyimpan *id*, *namalogin*, *password*, *namalengkap*, *hakakses* dan *serialnumber* pengguna. Tabel dapat dilihat seperti pada Gambar 3.18. berikut ini:

	Field	Type	Collation	Attributes	Null	Default	Extra	Action
	id	tinyint(4)			No			
	namalogin	varchar(20)	latin1_general_ci		No			
	password	varchar(100)	latin1_general_ci		No			
	namalengkap	varchar(50)	latin1_general_ci		No			
	hakakses	tinyint(2)			No			
	serialnumber	varchar(50)	latin1_general_ci		No			

Check All / Uncheck All *With selected:*

Gambar 3.18. Tabel pangkalan data admin

Jika dilakukan *browsing* pada isi tabel admin tersebut, dapat dilihat nilai *record* yang ada seperti pada Gambar 3.19. berikut:



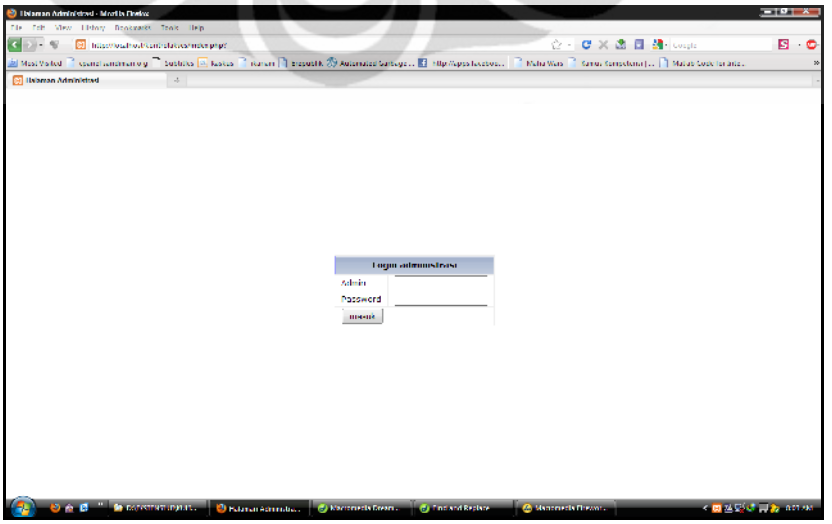
Gambar 3.19. Record pada *account* subjek di pangkalan data admin

3.5. Perancangan Layout

Perancangan halaman web ini digunakan sebagi antar muka bagi pengguna, halaman web yang akan dibuat terdiri dari 2 halaman yaitu halaman login dan halaman hasil.

3.5.1. Halaman Login

Halaman login yang merupakan halaman yang pertama kali muncul saat pengguna masuk ke situs ini. Halaman ini terdiri dari: form isian *username* dan *password* untuk masuk ke halaman hasil. Tampilan halaman login dapat dilihat pada Gambar 3.20. berikut ini:



Gambar 3.20. Halaman web untuk login sistem

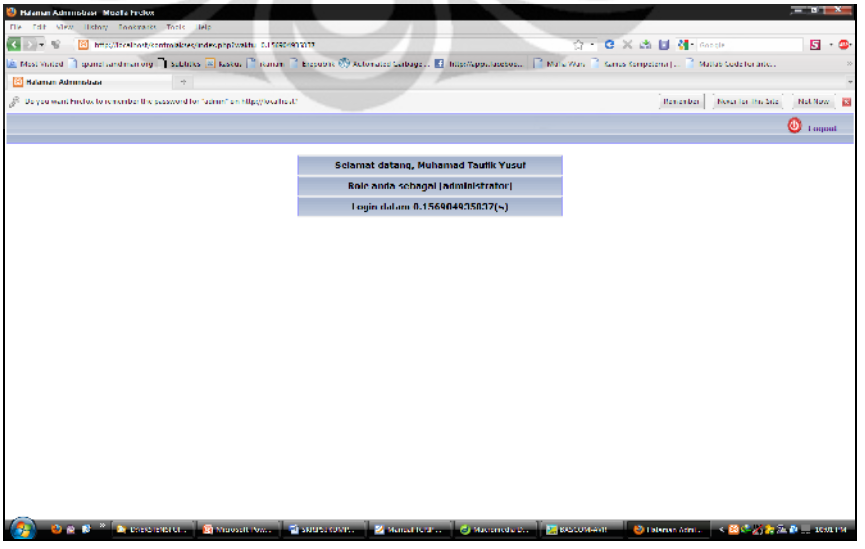
Untuk menampilkan halaman login dilakukan dengan perintah kode program seperti pada gambar 3.21. berikut ini:

```
function showLogin() {
      ?>
      <table style="width: 100%; height: 100%;">
      <tr><td style="text-align: center; vertical-align: midle;">
            <form action="index.php">
            <input type="hidden" name="aksi" value="proseslogin">
            <table class="daftar" align="center" cellspacing=1>
            <tr><th colspan=2>Login administrasi</th></tr>
            <tr><td>Admin</td><td><input                type="text"
name="namalogin"  size=20 maxlength=20></td></tr>
            <tr><td>Password</td><td><input        type="password"
name="password" size=20 maxlength=20></td></tr>
            <tr><td  colspan=2><input  type="submit"  value="  masuk
"></td></tr>
            </table>
            </form>
      </td></tr>
      </table>
      <?
}
```

Gambar 3.21. Kode program untuk menampilkan halaman login

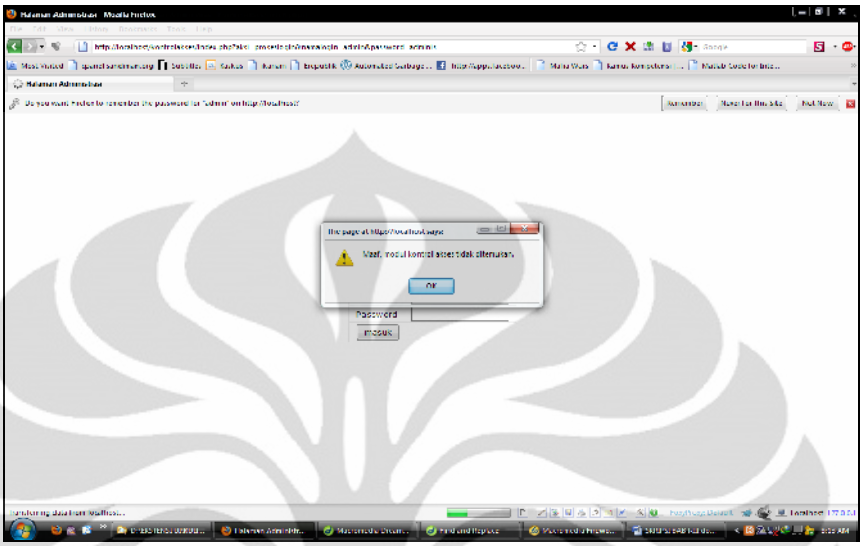
3.5.2. Halaman Hasil

Halaman hasil merupakan halaman yang menampilkan hasil proses login. Jika login berhasil, tampil halaman yang menandakan proses login berhasil. Tetapi jika login gagal, akan diberikan notifikasi kegagalan. Tampilan halaman hasil jika login berhasil dapat dilihat pada Gambar 3.22. sebagai berikut:



Gambar 3.22. Halaman hasil jika login berhasil

Tampilan halaman hasil beserta notifikasi kegagalan jika login gagal dapat dilihat seperti pada Gambar 3.23. berikut ini:



Gambar 3.23. Halaman hasil jika login gagal

Untuk menampilkan peringatan kepada pengguna jika gagal login dilakukan dengan perintah kode program seperti pada Gambar 3.24. berikut ini:

```
<script language="JavaScript">
      alert("Maaf, modul kontrol akses tidak ditemukan.");
      window.location("?");
</script>

<script language="JavaScript">
      alert("Maaf, username atau password salah.");
      window.location("?");
</script>
```

Gambar 3.24. Kode program untuk menampilkan pesan kegagalan

Untuk menampilkan halaman pengguna jika berhasil login dilakukan dengan perintah kode program seperti pada Gambar 3.25. berikut ini:

```
function showPanel() {
      $cookie = $_COOKIE["modulkontrolakses"];
      $data = explode("#", $cookie);
      $namalengkap = $data[1];
      $hakakses = $data[4];

      if ($hakakses == 1) { $hakakses = "administrator"; }
      else if ($hakakses == 2) { $hakakses = "konten admin"; }
      else $hakakses = "operator";
      $waktu = stripslashes($_REQUEST["waktu"]);

      ?>
      <table width=100%>
      <tr><td class="panel">
            <table width=100%>
            </td><td class="regular" style="text-align: right;">
            <?
            if (isLoggedIn()) {
            ?>
            <img     src="gambar/logout.png"     width=25>     <a
href="?aksi=proseslogout"  style="display:  inline-table;  height:
27px; vertical-align: middle;">Logout</a>
            <?
            }
            ?>
            </td></tr>
            </table>
      </td></tr>
      </table>

      <br>
      <table     class="daftar"     width=400     cellspacing=1
align="center">
      <tr><th  colspan=7>Selamat  datang,  <?  echo  $namalengkap  ?>
</th></tr>
      <tr><th    colspan=7>Role    anda    sebagai    <?    echo
"[".$hakakses."]" ?> </th></tr>
      <tr><th  colspan=7>Login  dalam  <?  echo  $waktu."(s)"  ?>
</th></tr></table>
<?
}
```

Gambar 3.25. Kode program untuk menampilkan halaman pengguna

BAB 4
IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1. Deskripsi Sistem

Deskripsi sistem untuk implementasi dan pengujian modul kontrol akses, dijelaskan sebagai berikut:

Hardware:

a. 1 Unit Laptop Asus F5RL dengan spesifikasi:
   - Prosessor Intel Core 2 Duo CPU T5450 @ 1.66GHz
   - Harddisk 120GB
   - Memory 1408MB RAM
   - ATI RADEON XPRESS 1100 256.0 MB
   - Atheros L2 Fast Ethernet 10/100 Base-T Controller

b. 1 Unit Netbook Acer AOHAPPY dengan spesifikasi:
   - Prosessor Intel Atom CPU N550 @1.50GHz
   - Harddisk 300GB
   - Memory 1024MB RAN
   - Atheros AR8152 PCI-E Fast Ethernet Controller

c. Ethernet Switch/ Kabel UTP RJ-45 bertipe crossover

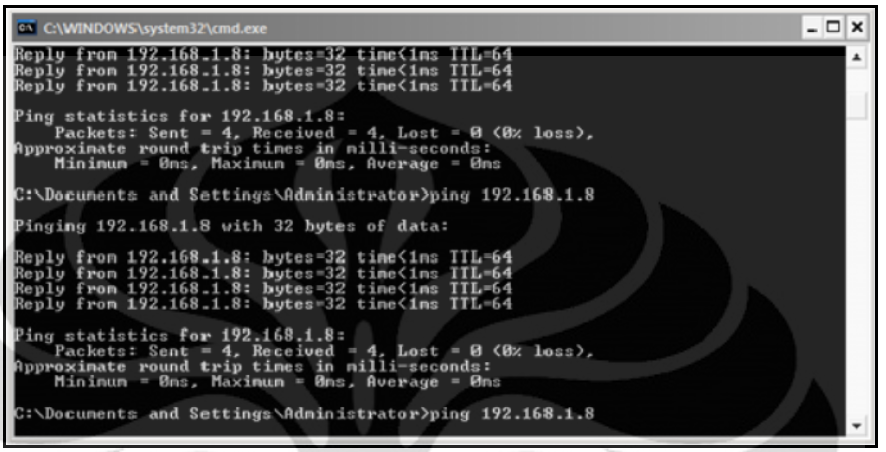
Software:

- BASCOM AVR 1.11.9.2
- Avr-Osp II Version .547
- ApacheFriends XAMPP (basic package) version 1.6.3a
- Macromedia Dreamweaver MX
- Mozilla Firefox/3.5.18
- Cain & abel v4.9.36

Implementasi modul kontrol akses yang sudah berhasil dilakukan dapat di uji dengan menggunakan perintah ping pada *command prompt*. Perintah tersebut dapat dituliskan dengan sintaks ping, sebagai berikut:

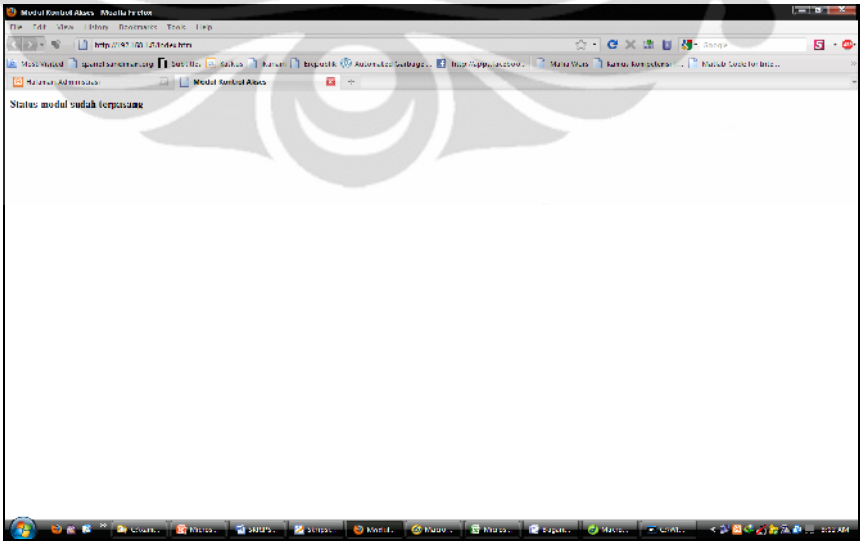
```
Ping 192.168.1.8
```

Jika modul kontrol akses sudah terkoneksi dengan baik, perintah tersebut menampilkan statistik paket data yang dikembalikan. Hasil perintah ping dapat dilihat seperti pada Gambar 4.1. berikut ini:



Gambar 4.1. Perintah ping untuk cek implementasi modul kontrol akses

Pengujian implementasi juga dapat dilihat dengan mengetikkan alamat http://192.168.1.8/index.htm pada *browser* internet. jika modul kontrol akses sudah terkoneksi dengan baik, pada browser ditampilkan tulisan "status modul sudah terpasang" seperti pada Gambar 4.2. berikut ini:



Gambar 4.2. Pengecekan implementasi lewat *browser* internet

4.2. Deskripsi Pengujian

Pengujian sistem dilakukan untuk memeriksa apakah sistem dapat berjalan seperti yang diharapkan. Dilakukan dengan cara menjalankan modul yang telah dibuat. Pada pengujian sistem, satu unit laptop difungsikan sebagai *web server* dan satu unit netbook difungsikan sebagai *client*. Dari hasil pengujian ini dapat diketahui tingkat keberhasilan operasional sistem beserta keakuratan data yang di transmisikan dan juga dapat diketahui informasi berupa perbedaan waktu akses sistem. Pengujian dilakukan dengan beberapa kriteria yaitu:

- Rata-rata keberhasilan pengguna login ke dalam sistem.
- Perbandingan waktu yang dibutuhkan untuk login dengan dan tanpa modul kontrol akses.
- Keakuratan data yang ditransmisikan melalui sistem.
- Pengujian dengan *online cracking password*.
- Survei terhadap kepuasan pengguna sistem.

4.3. Hasil Pengambilan Data

Pengujian dilakukan untuk mendapatkan data yang kemudian akan digunakan untuk menganalisa kinerja sistem berdasarkan fungsi-fungsinya yang diharapkan dapat berjalan dengan baik.

4.3.1. Rata-Rata Keberhasilan Pengguna Login ke dalam Sistem

Pengambilan data keberhasilan login dilakukan untuk mengetahui tingkat keberhasilan operasional sistem dalam mengontrol akses login pengguna ke dalam pangkalan data. Tabel 4.1.a. berikut ini adalah percobaan untuk mengetahui tingkat keberhasilan login super admin.

Tabel 4.1.a. Tingkat keberhasilan login super admin

Nama login	Percobaan ke-	Hasil
Admin	1	Berhasil
	2	Berhasil
	3	Berhasil
	4	Berhasil

Nama login	Percobaan ke-	Hasil
	5	Berhasil
	6	Berhasil
	7	Berhasil
	8	Berhasil
	9	Berhasil
	10	Berhasil
Prosentase keberhasilan		100%

Terlihat dari tabel diatas, nama login super admin sudah dapat login ke dalam sistem dengan baik. Tabel 4.1.b. berikut ini adalah percobaan untuk mengetahui tingkat keberhasilan login konten admin.

Tabel 4.1.b. Tingkat keberhasilan login konten admin

Nama login	Percobaan ke-	Hasil
Konten	1	Berhasil
	2	Berhasil
	3	Berhasil
	4	Berhasil
	5	Berhasil
	6	Berhasil
	7	Berhasil
	8	Berhasil
	9	Berhasil
	10	Berhasil
Prosentase keberhasilan		100%

Terlihat dari tabel diatas, nama login konten admin sudah dapat login ke dalam sistem dengan baik. Tabel 4.1.c. berikut ini adalah percobaan untuk mengetahui tingkat keberhasilan login operator.

Tabel 4.1.c. Tingkat keberhasilan login operator

Nama login	Percobaan ke-	Hasil
Operator	1	Berhasil
	2	Berhasil
	3	Berhasil
	4	Berhasil
	5	Berhasil
	6	Berhasil
	7	Berhasil
	8	Berhasil
	9	Berhasil
	10	Berhasil
Prosentase keberhasilan		100%

Terlihat dari tabel diatas, nama login operator juga sudah dapat login ke dalam sistem dengan baik. Berdasarkan tabel 4.1.a, b dan c diatas, dapat digambarkan grafik tingkat keberhasilan sistem dalam mengontrol akses login pengguna ke dalam pangkalan data dengan menggunakan modul kontrol akses seperti terlihat pada Gambar 4.3. berikut ini:

Gambar 4.3. Grafik tingkat keberhasilan sistem

Dari hasil pengukuran, dapat dilihat bahwa tingkat keberhasilan dari sistem ini dengan mengunakan modul sudah mencapai 100%. Sehingga dapat dikatakan sistem sudah berjalan dengan baik.

4.3.2. Perbandingan Waktu yang Dibutuhkan untuk Login

Pengambilan data terhadap waktu yang dibutuhkan oleh sistem untuk menampilkan halaman hasil pada proses login dilakukan untuk mengetahui seberapa jauh respon sistem, dalam hal ini kecepatan dalam menampilkan output jika proses yang dilakukan berbeda. Untuk mendapatkan informasi tersebut digunakan bantuan fungsi yang disediakan PHP, fungsi tersebut disisipkan atau disimpan dalam skrip program sehingga akan mengoptimalkan pengukuran informasi yang dibutuhkan. Untuk mendapatkan informasi waktu digunakan fungsi microtime().

Fungsi microtime digunakan untuk menghasilkan nilai waktu saat ini dalam dua bagian yaitu detik dan mikrodetik. Dapat dilakukan dengan perintah kode program seperti pada Gambar 4.4. berikut ini:

```
#script_timer
<?php
function getmicrotime() {
            list($usec, $sec) = explode(" ",microtime());
            return ((float)$usec + (float)$sec);
}

$time_start = getmicrotime();
// script login disini
$time_end = getmicrotime();
$waktu = $time_end - $time_start;

echo 'This page was created in ' .$waktu. ' seconds.';
?>
```

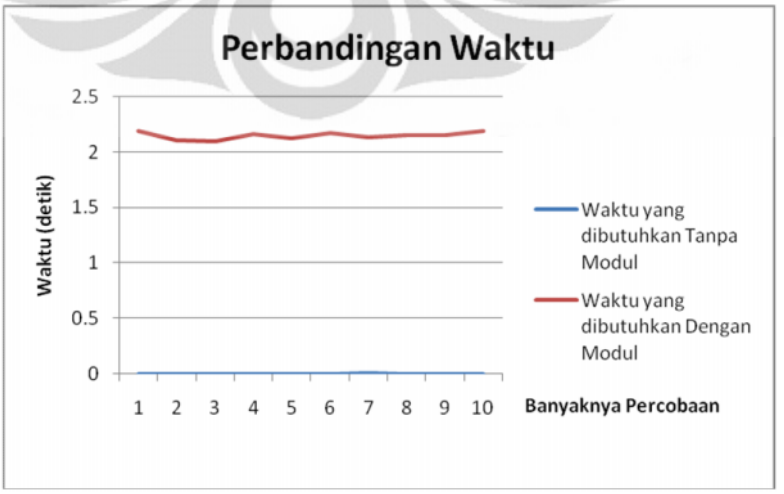
Gambar 4.4. Kode program untuk menghasilkan nilai waktu

Hasil perbandingan waktu yang dibutuhkan untuk login dengan menggunakan modul kontrol akses dan tanpa modul kontrol akses dapat dilihat pada Tabel 4.2. berikut ini:

Tabel 4.2. Perbandingan waktu login

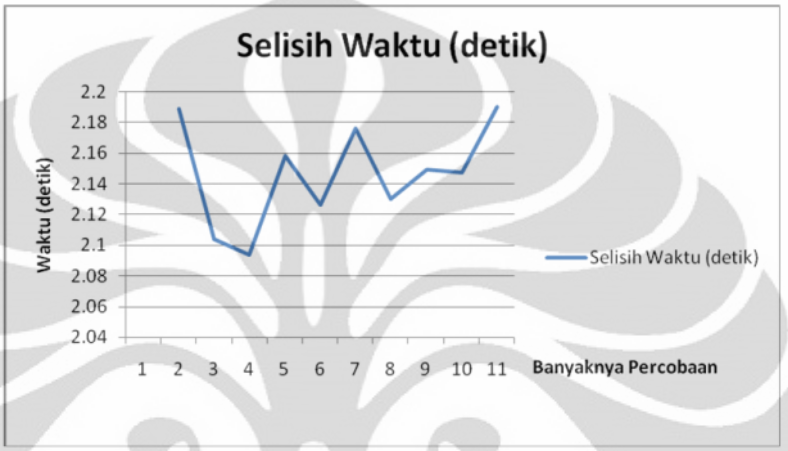
Percobaan ke-	Waktu yang dibutuhkan		Selisih
	Tanpa modul	Dengan Modul	
1	0.00347590446472	2.19234800339	2.1888721
2	0.00456809997559	2.10851097107	2.10394287
3	0.00372695922852	2.09740400314	2.09367704
4	0.00262093544006	2.16083502769	2.15821409
5	0.00373005867004	2.13026690483	2.12653685
6	0.00342488288879	2.17976808548	2.1763432
7	0.00842189788818	2.13857984543	2.13015795
8	0.00330901145935	2.15264105797	2.14933205
9	0.00338006019592	2.15088796616	2.14750791
10	0.00387406349182	2.19431900978	2.19044495
Rata-rata *delay*			2.1465029

Jika di gambarkan dengan grafik, tabel diatas dapat dilihat seperti pada Gambar 4.5. berikut ini:



Gambar 4.5. Grafik perbandingan waktu login

Berdasarkan gambar grafik diatas, dapat dilihat bahwa dengan modul, waktu proses login menjadi lebih lama. Hal ini dikarenakan adanya proses otentikasi yang lebih panjang. Sehingga waktu yang dibutuhkan menjadi lebih lama. Sedangkan pada proses login tanpa modul hanya diperlukan otentikasi dengan pangkalan data saja. Selisih waktu dapat digambarkan seperti pada Gambar 4.6. berikut ini:



Gambar 4.6. Grafik selisih waktu

Pada gambar diatas terlihat selisih waktu login cukup bervariasi, tetapi masih berada di posisi sepersepuluh detik. Sesuai dengan Tabel 4.2. diatas, hasil rata-rata *delay* yang didapat adalah 2.14 detik. *Delay* jika dibandingkan dengan login tanpa modul mencapai 529.58% atau mencapai 5x lipat-nya dari waktu tanpa menggunakan modul. Jika dibandingkan dengan waktu respon secara manual, waktu *delay* yang terjadi masih dapat diterima.

4.3.3. Keakuratan Data

Pengujian keakuratan data dilakukan untuk melihat kesesuaian antara data yang dikirimkan dan diterima oleh sistem. *Test vector* data *random key* yang digunakan adalah "286667dd30f0fb9384fec7c2e968dca4". Data yang masuk adalah data kompresi *password* pengguna yang ditransmisikan dari *web server* ke modul kontrol akses melalui protokol TCP/IP. Data yang keluar adalah data masukan yang telah direkonstruksi menggunakan *secret splitting* oleh modul kontrol akses dan kemudian juga telah diproses oleh *web server*.

Secret splitting dilakukan dengan perintah kode program seperti pada Gambar 4.7. berikut ini:

```
Rekonstruksi:
   Dim N As Integer
   Dim Temp As Byte , Ptx As Byte , Ctx As Byte
   Dim Text As String * 40
   Dim Temps As String * 2

   Snumber = ""
   Text = "286667dd30f0fb9384fec7c2e968dca4"                    'kunci
   For N = 1 To Len(text)
      Temps = Mid(shtml , N , 1)
      Ptx = Hexval(temps)
      Temps = Mid(text , N , 1)
      Ctx = Hexval(temps)
      Temp = Ptx Xor Ctx
      Temps = Hex(temp)
      Temps = Right(temps , 1)
      Snumber = Snumber + Temps
   Next N
Return
```

Gambar 4.7. Kode program untuk *secret splitting*

Pada Tabel 4.3. berikut ini, disajikan data yang ditransmisikan melalui modul kontrol akses.

Tabel 4.3. Keakuratan data yang ditransmisikan melalui modul

No	Nama login	Transmisi data pada modul		Akurasi
1	Admin	masuk	21232f297a57a5a743894a0e4a801fc3	100%
		keluar	f4bda8a7a7824b73ea7a4c5de14274ea	
		harusnya	f4bda8a7a7824b73ea7a4c5de14274ea	
2	Konten	masuk	286667dd30f0fb9384fec7c2e968dca4	100%
		keluar	b8c2f29340039ce37525f15cedaf949e	
		harusnya	b8c2f29340039ce37525f15cedaf949e	
3	Operator	masuk	11d8c28a64490a987612f2332502467f	100%
		keluar	6fcec2794ef28cc2058cd741caf81fe7	
		harusnya	6fcec2794ef28cc2058cd741caf81fe7	

Dari Tabel 4.3. diatas, terlihat tingkat akurasi data yang keluar untuk masing-masing data masukan untuk tiap-tiap nama login mencapai 100%. Hal ini

terjadi karena algoritma pengolahan data sudah sesuai sehingga dapat dikatakan sistem sudah baik.

4.3.4. Pengujian dengan *Online Cracking Password*

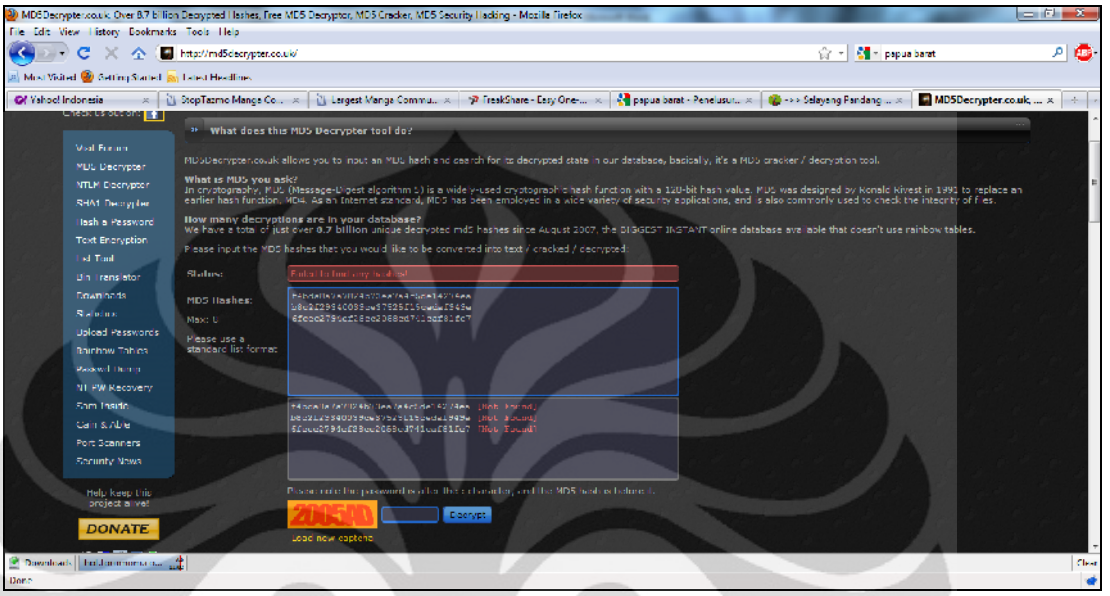
Di internet terdapat banyak situs yang menyediakan cracking terhadap *password* pangkalan data. Situs-situs tersebut diantaranya adalah:

- md5.rednoize.com
- md5decryption.com
- opencrack.hashkiller.com
- www.bigtrapeze.com
- md5.hashcracking.com
- www.hashchecker.com
- md5crack.com
- md5decrypter.co.uk
- md5hashcracker.appspot.com
- gdataonline.com
- alimamed.pp.ru
- passcracking.com

Pengujian dengan *online cracking password* dilakukan untuk melihat sisi keamanan data *password* yang disimpan dalam pangkalan data admin menggunakan salah satu situs diatas. Pada Gambar 4.8. berikut ini digambarkan hasil *cracking* data yang tidak menggunakan modul kontrol akses.

Gambar 4.8. Hasil pengujian *online cracking* tanpa menggunakan modul

Dari gambar diatas, terlihat data *password* yang disimpan dalam pangkalan data admin dapat diketahui nilai aslinya. Pada gambar 4.9. berikut ini digambarkan hasil *cracking* data yang menggunakan modul kontrol akses.



Gambar 4.9. Hasil pengujian *online cracking* dengan menggunakan modul

Pada Gambar 4.9. diatas terlihat data *password* pada pangkalan data admin tidak dapat di *crack* dengan *online cracking password* sehingga dapat dikatakan *password* yang disimpan dalam pangkalan data admin lebih terlindungi.

4.3.5. Survei Terhadap Pengguna Sistem

Metode survei digunakan untuk melengkapi pengujian terhadap sistem. Survei terdiri dari 7 pertanyaan dan diisi oleh 10 responden. Data tersebut, di ubah ke bentuk angka dan dihitung nilai rata-rata jawabannya untuk kemudian ditafsirkan hasilnya.

Tabel 4.4. Hasil survei penggunaan sistem

No	Pertanyaan	Jawaban Responden				Rata-rata
		3	2	1	0	
1	Tampilan antarmuka login	5	5	-	-	2.5
2	Waktu respon saat login	2	8	-	-	2.2
3	Pesan kesalahan	3	5	2	-	2.1

No	Pertanyaan	Jawaban Responden				Rata-rata
		3	2	1	0	
4	Tingkat keberhasilan	8	2	-	-	2.8
5	Bermanfaat untuk menambah rasa aman	5	5	-	-	2.5
6	Kemudahan penggunaan	4	6	-	-	2.4
7	Kepuasan pengguna	5	5	-	-	2.5
Rata-rata						2.4

Tabel 4.4. diatas menggambarkan kepuasan pengguna secara keseluruhan terhadap sistem. Kepuasan tertinggi ada pada tingkat keberhasilan sistem dengan nilai rata-rata 2.8 dan terendah pada pesan kesalahan dengan nilai rata-rata 2.1. Waktu respon sistem hanya mendapat nilai rata-rata 2.2 disebabkan adanya jeda waktu yang jauh berbeda antara waktu respon ketika menggunakan modul dengan waktu respon tanpa menggunakan modul. Namun sebagian besar menjawab waktu respon cukup. Aspek kemudahan penggunaan seharusnya mendapatkan nilai tinggi karena pengguna tidak perlu melakukan pengaturan, namun hanya mendapat nilai rata-rata 2.4 karena banyak pengguna menganggap sistem ini mudah digunakan tapi dengan akun yang sudah harus terdaftar sebelumnya. Secara keseluruhan sistem ini dapat dikatakan cukup baik karena memiliki nilai rata-rata sebesar 2.4 dari nilai maksimal 3. Jika dilihat dalam prosentase, maka tingkat kepuasannya mencapai 80%.

BAB 5
KESIMPULAN

Dari hasil percobaan yang dilakukan, didapatkan kesimpulan:

1. Modul kontrol akses sudah berhasil diimplementasikan pada sistem yang dirancang dan dapat berjalan dengan baik.
2. Tingkat keberhasilan operasional sistem dalam mengontrol akses login pengguna ke dalam pangkalan data sudah baik. Terlihat dari keberhasilan login pengguna dengan menggunakan modul sudah mencapai 100%.
3. Waktu yang diperlukan untuk proses login cukup bervariasi namun tidak berbeda jauh karena masih berada di posisi sepersepuluh detik. Hasil rata-rata *delay* yang didapat adalah 2.14 detik karena adanya proses otentikasi yang lebih panjang. Proses otentikasi yang lebih panjang membuat waktu yang dibutuhkan menjadi 5 kali lebih lama.
4. Akurasi data yang masuk ke modul dan yang keluar setelah di rekonstruksi dari modul untuk masing-masing nama login mencapai 100%. Menandakan algoritma pengolahan datanya sudah sesuai.
5. Data yang keluar dari modul kontrol akses dapat terlindungi dari pengguna yang tidak memiliki hak akses, terlihat data *password* tidak bisa di *crack* dengan *online cracking password*.
6. Menurut tingkat kepuasan pengguna, secara keseluruhan sistem dapat dikatakan cukup baik karena memiliki nilai rata-rata sebesar 2.4 dari nilai maksimal 3. Jika dilihat dalam prosentase, maka tingkat kepuasannya mencapai 80%.

DAFTAR ACUAN

[1] "Access Control", http://en.wikipedia.org/wiki/Access_control, diakses terakhir 15 Maret 2011.

[2] "Access Control Model", http://www.techexams.net/technotes/securityplus/mac_dac_rbac.shtml, diakses terakhir 17 Maret 2011.

[3] Erliasari, Dian. *Mekanisme Discretionary Access Control untuk Database Security*. Report Paper, Bandung: ITB, 2001.

[4] Fathansyah. *Buku Teks Ilmu Komputer: Basis Data.* Bandung: Informatika, 2002.

[5] "MySQL Database", http://www.info-teknologi.com/belajar-mysql-database/, diakses terakhir 15 Maret 2011.

[6] Menezes, Alfred J., Paul C. Van Ooschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. Boca Raton: CRC Press LLc, 1997.

[7] Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C Second Edition*. New York: John Wiley & Sons Inc, 1996.

[8] Atmel Corp. "Atmel AVR ATmega32 Data Sheet." *http://www.atmel.com.* 2005.

[9] WIZnet Co. Inc. "NM7010A-LF Datasheet v2.6." *http://www.wiznet.co.kr*. Juli 24, 2007.

[10] Innovative Electronic, "Manual TCP/IP Starter Kit.", *http://www.innovativeelectronics.com*, 2007.

LAMPIRAN

Nama: ……

TANGGAPAN TERHADAP PENGGUNAAN MODUL KONTROL AKSES UNTUK AKSES WEB DATABASE

1. Apakah antarmuka sistem ini sudah baik?
    a. Sudah baik
    b. Cukup baik
    c. Kurang baik
    d. Tidak baik
2. Apakah waktu respon sistem mengganggu anda?
    a. Tidak mengganggu sama sekali
    b. Kadang mengganggu
    c. Mengganggu
    d. Sangat mengganggu
3. Apakah pesan kesalahan yang ada cukup membantu anda ?
    a. Sangat membantu
    b. Cukup membantu
    c. Kurang membantu
    d. Tidak membantu
4. Apakah tingkat keberhasilan sistem sudah cukup?
    a. Sudah berhasil
    b. Cukup berhasil
    c. Kurang berhasil
    d. Tidak berhasil
5. Apakah sistem ini bermanfaat untuk menambah rasa aman pada diri anda?
    a. Bermanfaat
    b. Cukup bermanfaat
    c. Kurang bermanfaat
    d. Tidak bermanfaat
6. Apakah sistem ini mudah digunakan?
    a. Sangat mudah
    b. Cukup mudah
    c. Sulit
    d. Tidak bisa
7. Apakah anda puas dengan sistem ini?
    a. Sangat puas
    b. Cukup puas
    c. Kurang puas
    d. Tidak puas