Syntax : Journal of Sotware Engineering, Computer Science and Information Technology
Vol.1, No.1 Tahun 2020

PENGEMBANGAN SISTEM OTENTIKASI PADA SEBUAH APLIKASI YANG BERBASISKAN WEB

M. Arif Rahman
Rekayasa Perangkat Lunak, Universitas Dahrmawangsa Medan, Jl. K. L Yos Sudarso No.224, Medan, Sumatera Utara
email: arif@dharmawangsa.com

Abstrak - Tujuan dibuatnya sistem ini ditujukan untuk penambahan pengamanan sistem yang telah ada, agar keamanan diperoleh lebih maksimal. Keamanan yang maksimal memang tidak terlalu menjamin apa yang telah dilakukan tetapi ini ditujukan untuk pertahanan atau benteng terakhir dari sebuah sistem yang dimiliki, yang mana dibuat dengan faedah yang berlaku. Dalam perancangan sistem ini penulis tidak sekedar memakai metode kriptografi yang telah ada pada PHP yaitu MD5. Pada dasarnya penerapan MD5 tidaklah cukup bagi sebuah keamanan suatu aplikasi yang berbasiskan web maka dari itu penulis mencoba merancang sistem pengacakan yang bertujuan agar lebih menjamin data atau password yang ada pada suatu database. Dengan adanya penambahan pada sistem baru yang lebih baik maka dapat memperlancar proses pengamanan data yang akurat serta keamanan data lebih terjamin. Hasil penelitian ini berupa sebuah aplikasi yang bisa diterapkan langsung pada aplikasi yang dibuat programmer sendiri.

Abstract – *The purpose of this system made is point to the additional previous system that has been exited to protect maximally. The maximal protection is not guarantee what had been done but, it is aims do depend of firewall of a system. As well as the function itself. In design this system the researcher not only using the cryptography. That contains in PHP program is MD5. Basically the applying MD5 is not enough to secure an application based on web. Therefore the researcher's Design a random system in purpose more guarantee data or password in a database. By adding a new good system, as a result it will easier to processing secure of data accurately and also guarantee secure of data itself. The result of this research is an application in which it is able directly apply that make by the programmer itself.*

Keywords*: Application, Encrypt, Information system, MD5, PHP*

PENDAHULUAN

Mengingat pentingnya informasi yang cepat, tepat dan akurat serta keamanan terhadap database yang ada nantinya mampu melindungi data, maka dari itu menimbulkan pertanyaan bagi penulis serta beberapa masalah yaitu:

1. Bagaimana menjaga kemanan *web email* kita terutama *Password* login?
2. Bagaimana kerahasian data *User* serta informasi?
3. Dan bagaimana penerapankeamanan yang benar terhadap sebuah account *web?*

Berdasarkan permasalahan di atas, dapat dikemukakan beberapa hipotesa sebagai berikut:

1. Menjaga keamaan *web email* didasari dari seorang user yang mempunyai akun pada sebuah web yang mungkin berisikan informasi penting. Keamanan yang paling dibutuhkan yaitu keamanan pada password yang mungkin bisa dikombinasikan dengan *username* dari seorang user. Maka dari itu kewaspadaan yang menjadi

keutamaan dalam menjaga keamanan sebuah password atau akun yang ada.

2. Kerahasian data atau mungkin informasi dari user pada sebuah web mail bisa dilakukan dengan pengamanan berganda/ perulangan identifikasi user, tetapi itu nantinya akan memakan waktu lamam dan menghabiskan waktu seorang user berkutik pada menu *Login* salah satunya. Maka dari itu pada aplikasi web dan webserver adanya metode kriptografi yang nantinya akan diterapkan untuk melakukan pengacakan data atau informasi seorang user agar pihak selain tidak mengetahuinya.
3. Penerapan keamanan yang tinggi bertujuan agar kenyamanan serta keamanan seorang dapat terjamin, sehingganya user harus tau dan mengerti apa-apa saja yang nantinya yang akan dilakukan untuk agar sebuah akun miliknya tidak dapat diketahui orang lain.

Tujuan dari penelitian yang dilakukan adalah sebagai berikut:

Adapun tujuan dari penelitian ini adalah penerapan keamanan berganda dengan merancang sebuah sistem otentikasi halaman web dengan metode kriptografi yang ada.

METODE PENELITIAN

Authentification adalah proses dalam rangka *validasi user* pada saat memasuki sistem, nama dan *password* dari *user* di cek melalui proses yang mengecek langsung ke daftar mereka yang diberikan hak untuk memasuki sistem tersebut. Autorisasi ini di *set up* oleh administrator, webmaster atau pemilik situs (pemegang hak tertinggi atau mereka yang ditunjuk di sistem tersebut. Untuk proses ini masing-masing user akan di cek dari data yang diberikannya seperti nama, *password* serta hal-hal lainnya yang tidak tertutup kemungkinannya seperti jam penggunaan, lokasi yang diperbolehkan.

Metode otentikasi konvensional yang selama ini familiar di gunakan adalah menggunakan kombinasi "*username*" dan "*password*" atau biasa juga di sebut dengan metode "*single factor authentication*". Username adalah sebuah penanda unik yang dapat digunakan untuk mengidentifikasi seorang user yang mencoba masuk (log on) kedalam sebuah sistem komputer. Password adalah sebuah kombinasi rahasia yang terdiri dari kombinasi huruf, angka, dan karakter khusus. Username dan password di kombinasikan bersama-sama untuk mekanisme otentikasi pada sebuah sistem komputer.

Kita dapat membuat account di dalam AD (*Active Directory*) untuk seluruh entitas (*users*, *computers* dan *resources* lain) yang kemudian kita gunakan strategi penggroupan untuk *account-account* ini. *Setting* untuk *access control* kemudian diterapkan terhadap *group-group* tersebut agar *account* yang ada dapat menggunakan *authenticated identity*-nya untuk mengakses *resource*.

Dalam hal mengedukasi *user*, kita perlu menyediakan berbagai pedoman ke *user*, kita perlu mendorong agar *user* tidak men-*share password* mereka, dan juga selalu menggunakan *password* yang kompleks/*strong*. Implementasinya dari autentikasi *user* ini adalah berupa *login* dalam sebuah website.

.

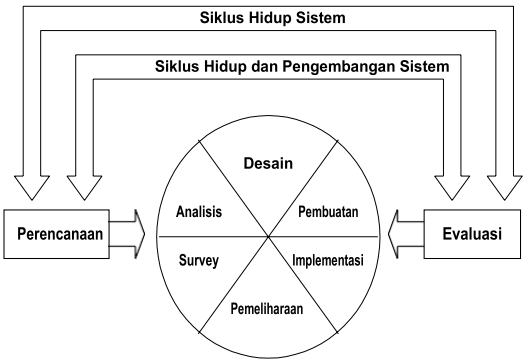
ada dua pendekatan sistem dalam mendefinisikan sistem.

1. Pendekatan yang menekankan pada prosedur.
   Mendefinisikan system sebagai suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan, untuk melakukan suatu kegiatan dalam mencapai suatu sasaran tertentu.
2. Yang mengarah pada komponen dan elemennya.

Sistem adalah kumpulan elemen yang saling berkaitan dan bertanggung jawab memproses masuka (input) sehingga menjadi keluaran (output).

Jadi, Sistem informasi merupakan suatu tatanan yang saling terkait antara unsur data, sotware, hardware, sumberdaya manusia dan kelembagaan serta aturan mainnya. Mengembangkan system informasi berarti mengembangkan seluruh unsure tersebut secara menyeluruh, tidak bias dilakukan secara menyeluruh, tidak bias dilakukan secara parsial atau sendiri-sendiri. jadi Siklus hidup sistem informasi dimulai dari perencanaan, pengembangan (survei, analisa, desain, pembuatan, implementasi, pemeliharaan), dan dievaluasi secara terus- menerus untuk menetapkan apakah sistem informasi tersebut masih layak diaplikasikan, jika tidak, sistem informasi tersebut akan diganti dengan yang baru dan dimulai dari perencanaan kembali.

Siklus Daur Hidup Pengembangan Sistem dapat kita lihat pada Gambar berikut:



Gambar Daur Hidup Pengembangan Sistem

HASIL DAN PEMBAHASAN

Berdasarkan proses yang diterapkan pada sebuah web yang ada, serta hasil pengamatan dan penelitian keamanan yang dilakukan pada sebuah web. Masih terdapatnya penerapan keamanan yang masih standar sehingga keamanan kurang efektivitas dan efesiensi data tidak terjamin. Aplikasi di mulai dari form login. Di ibaratkan sebuah.

Aplikasi di mulai dari form login. Di ibaratkan sebuah website yang mengharuskan *user* untuk login untuk dapat masuk dalam konten sebuah website dapat dilihat pada Gambar berikut:

Gambar Form Login

Seolah olah user belum mendaftar dalam website tersebut, maka pertama harus melakukan pendaftaran / *sign up.* Berikut merupakan contoh aplikasi untuk sign up / pendaftaran di suatu alamat web tertentu belum memanfaatkan kriptografi dalam implementasinya (Gambar. 3.2) :

Gambar Form Pendaftaran

Sepintas tidak ada masalah dalam form diatas, pada text field untuk isian password sudah menunjukkan kerahasiaan data user. Pada kasus ini pada text field Password kita isi "**GAWAT123**". Setelah user klik button daftar, maka ada pemberitahuan bahwa data telah berhasil di simpan dalam bentuk ucapan terima kasih.

Sekarang pertanyaannya bagaimana keadaan data yang kita unggah di dalam database server. Apakah data yang kita kirimkan bisa terjaga kerahasiaanya. Berikut kondisi data yang di terima oleh server (Gambar):

id	nama	password	ktp
7	Joko Sulistyo	GAWAT123	31.2312.655436.0001
6	Whilda Chaq	ABAN2MIF	0980828619284721

Gambar Screenshoot pada database

Pada kolom password data tersimpan polos tanpa ada perubahan dari yang user ketikkan. sehingga admin sebuah web dapat mengetahui password user dan kerahasiaan data user sudah tidak bisa terjamin lagi.

Seperti yang telah dijelaskan sebelumnya, bahwa terdapat kelemahan-kelemahan yang ditemukan pada kegiatan peng-aplikasian kemanan sebuah web yang biasanya dilakukan pada fasilitas *login*. Setelah dilakukan analisa terhadap kegiatan tersebut, desain sistem baru diperlukan untuk menutupi dan memperbaiki kelemahan-kelemahan yang ada pada sistem yang ada.

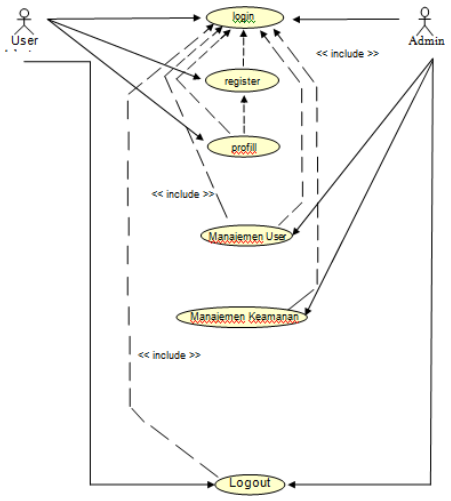
Dalam memperbaiki proses kegiatan peng-aplikasian yang akan dilakukan adalah:

1. Memperbaiki proses yang ada dengan memanfaatkan sistem komputer sebagai sarana untuk membangun sebuah sistem yang natinya akan membantu user dalam penjagaan/ pengaplikasian data informasi seorang *user*.
2. Mengaplikasikan Bahasa Pemrograman WEB PHP sebagai sarana untuk pengaplikasian kemanan data dan informasi seorang user berupa penerapan aplikasi yang ada.

1. Use Case Diagram

Use case mendiskripsikan interaksi tipikal antara pengguna system dengan system itu sendiri. Setiap langkah dalam use case adalah elemen dalam interaksi antara actor dan system. Setiap langkah harus berupa pernyataan sderhana dan dengan jelas menunjukan siapa yang menjalankan langkah tersebut. Langkah tersebut harus menunjukan tujuan actor, bukan mekanisme yang harus di lakukan actor. Kosekuensinya, kita tidak menjenjabarkan antar muka pengguna dalam use case.

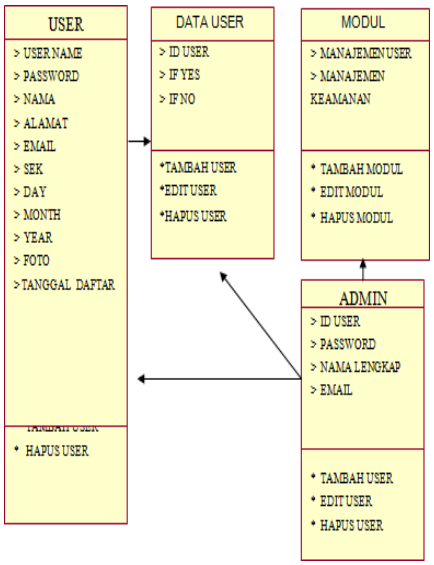
Perancangan system degan menggunakan use case diagram dapat dilihat pada gambar berikut ini:



Gambar Use case Diagram

2. Class Diagram

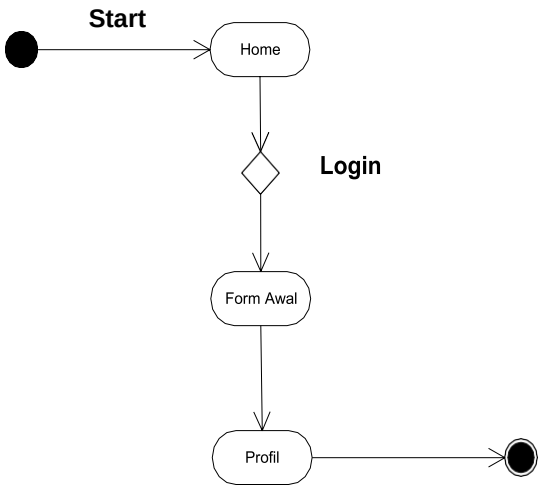
Class diagram menggambarkan struktur dan deskripsi class, package dan objek beserta hubungan satu sama lain seperti containment, pewarisan, asosiasi, dan lain-lain. Class diagram juga menggambarkan keadaan (atribut/properti) suatu sistem, sekaligus menawarkan layanan untuk memanipulasi keadaan tersebut (metoda/fungsi).



Gambar Class Diagram

3. Statechart Diagram

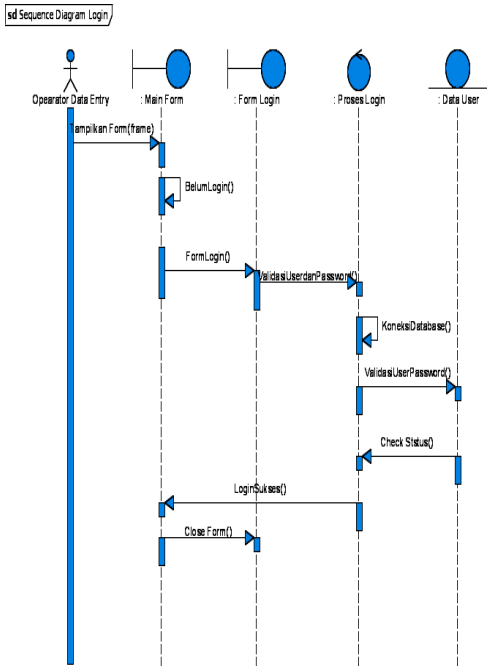
Statechart diagram menggambarkan transisi dan perubahan keadaan (dari satu state ke state lainnya) suatu objek pada sistem sebagai akibat dari stimuli yang diterima. state digambarkan dengan bentuk segiempat dengan sudut membulat dan memiliki nama sesuai kondisinya saat itu. Transisi antar state umumnya memiliki kondisi guard yang merupakan syarat terjadinya transisi yang bersangkutan. Adapun statechart diagram dapat dilihat pada gambar berikut ini :



Gambar Statechart Diagram

3.2.1 Sequence Diagram

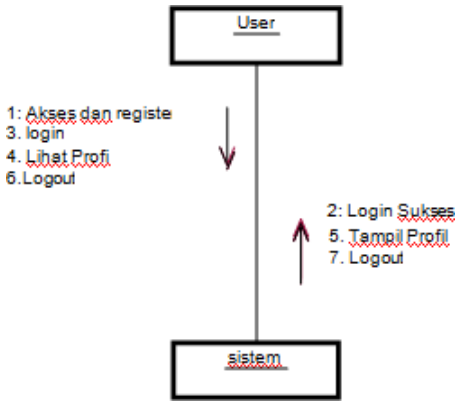
Sequence diagram digunakan untuk menggambarkan scenario atau rangkaian langkah-langkah yang dilakukan sebagai respons dari sebuah event untuk menghasilkan output tertentu. Diawali dari apa yang men-trigger aktivitas tersebut, proses dan perubahan apa saja yang terjadi secara internal dan output apa yang dihasilkan.Adapun sequence diagram dari program autentikasi ini dapat dilihat pada gambar berikut ini :



Gambar Sequence diagram login

4. Collaboration Diagram

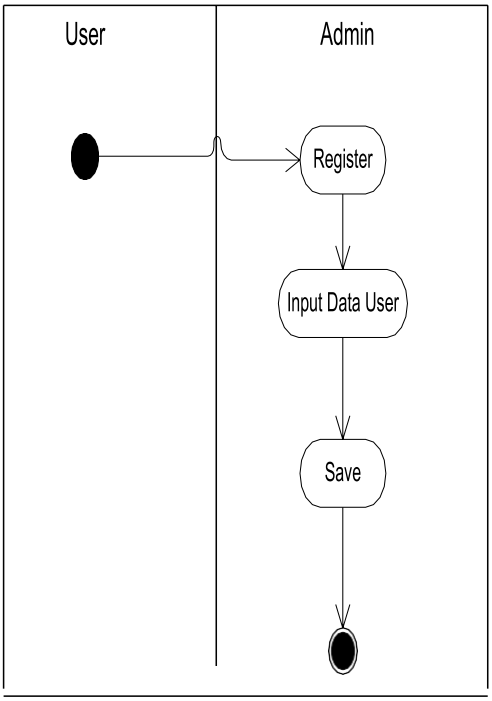
Collaboration diagram menggambarkan object dan hubungannya (mengacu ke konteks). Jika penekannya pada waktu atau urutan gunakan sequence diagrams, tapi jika penekanannya pada konteks gunakan collaboration diagram.Model collaboration diagram dapat dilihat pada gambar bertikut :



Gambar Diagram Collaboration

5. Activity Diagram

Menggambarkan berbagai alir aktivitas dalam system yang sedang dirancang,bagaimana masing-masing alir berawal,decision yang mungkin terjadi dan bagaimana akhirnya.Adapun activity diagram dari customer dapat dilihat pada gambar berikut ini :

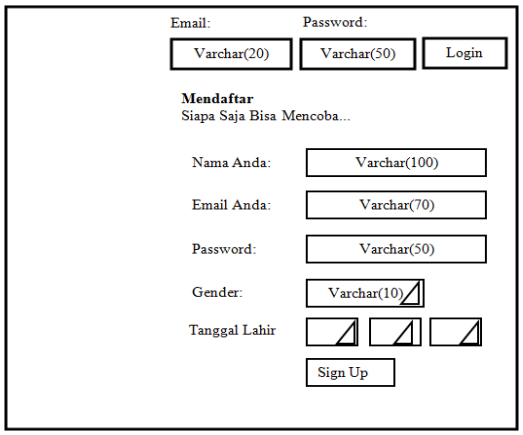


Gambar Activity diagram

Desain Program

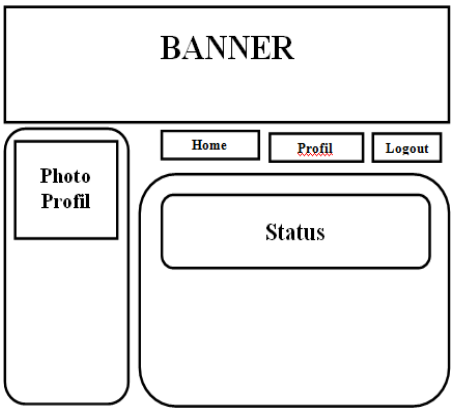
Desain program dibuat ditujukan untuk merancang tampilan atau form yang nantinya ditampilkan kepada pemakai akhir/ *User*, dalam pengolahan data beserta informasi yang diinginkan.

1. Desain Form Index



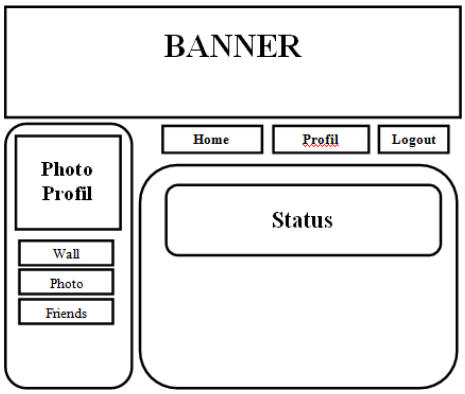
Gambar Halaman Form Awal

2. Halaman Form *Home*



Gambar Halaman Form Home

3. Halaman Form User



Gambar Halaman Form User

Implementasi Dan Pengujian Sistem

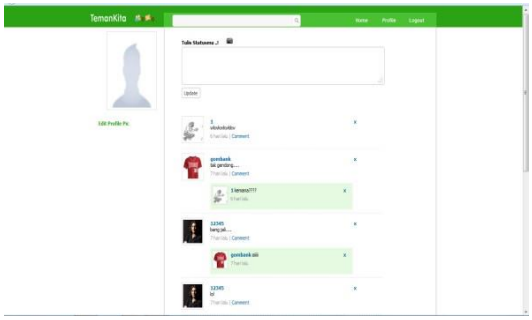
1. Halaman Utama/ Login

Gambar Tampilan Halaman Utama/ *Login*

2. Halaman Utama/ Sign Up

Gambar Tampilan Halaman Utama/ *Sign Up*

3. Halaman *Home User*



Gambar Tampilan Home/ *User*

4. Hasil Pengaplikasian Enkripsi *MD5*(Table *User*)

uid	password	nama	tgl_lahir	gender	email
38	a8144eeb20933dcf5c460cc73f8cbebe	__	1970-01-01	Laki-Laki	tampan@gmail.com
39	a8144eeb20933dcf5c460cc73f8cbebe	arif1234	1970-01-01	Laki-Laki	arif4@yahoo.com
36	6082d69b3232fa87bccbd18e85299a65	aaaa	1970-01-01	Laki-Laki	toshiba@yahoo.com
37	21232f297a57a5a743894a0e4a801fc3	admin	1970-01-01	Laki-Laki	admin@yahoo.com
34	6c940bb3ddc43f6954d624d95e104aac	arif	1970-01-01	Laki-Laki	arif3@yahoo.com
33	a8144eeb20933dcf5c460cc73f8cbebe	arif	1990-01-01	Laki-Laki	arif@tampan.com
32	6082d69b3232fa87bccbd18e85299a65	rudi	1990-01-01	Laki-Laki	rudi@yahoo.co.id
29	69866fb93d2c32fc020d2b38722174bc	1	1970-01-01	Laki-Laki	qwerty@yahoo.com
26	69866fb93d2c32fc020d2b38722174bc	12345	1990-04-01	Laki-Laki	12345@yahoo.com
30	d3ea81863cb29a55a20d9dfcd92c31eb	arif	1970-01-01	Laki-Laki	arif2@yahoo.com
27	040b7cf4a55014e185813e0644502ea9	gombank	1992-02-01	Laki-Laki	gombank@yahoo.com
25	827ccb0eea8a706c4c34a16891f84e7b	koil	1990-12-10	Laki-Laki	koil@yahoo.com
22	827ccb0eea8a706c4c34a16891f84e7b	firdaus	1999-01-10	Laki-Laki	firdaus69@gmail.com

Gambar Hasil Pengaplikasian Enkripsi MD5 (*Table User*)

5. Penerapan Coding

```php
<?php
include_once 'include/db.php';

// Jika user melakukan pendaftaran
$nama     = $_POST['nama'];
$gender   = $_POST['gender'];
$tgl      = $_POST['tgl'];
$bln      = $_POST['bulan'];
$thn      = $_POST['tahun'];
$tanggal  = "$thn-$bln-$tgl";
$email    = $_POST['email'];
$pass     = $_POST['pass'];
//$password = md5($pass);
$pengacak = "AJWKXLAJSCLWLW";
$password = md5($pengacak.md5($pass).$pengacak);

```

Gambar Penerapan Coding Pengacakan (*Sign Up User*)

3. *Menu Login User*

Gambar Penerapan Coding (*Login User*)

KESIMPULAN

Dari hasil penelitian yang penulis lakukan dan dengan melakukan pengembangan sistem otentikasi pada aplikasi yang berbasiskan web dapat disimpulkan hal-hal sebagai berikut :

1. Bahwa dalam menjaga keamanan suatu data terutama *password* yang dimiliki oleh seorang User yang berisi informasi penting, maka peningkatan keamanan perlu diterapkan. Dan pada penelitian yang dilakukan penulis maka peningkatan tersebut dapat diterapkan pada aplikasi yang telah dikembangkan oleh peneliti.
2. Dengan penggunaan metode kriptografi yang telah ada dan dipadukan dengan sistem pengacakan yang dikembangkan oleh peneliti, sistem identifikasi *User* bisa menghindari proses "*hack"* yang dilakukan oleh pihak selain *User* yang nantinya melakukan tindakan yang tidak diinginkan.
3. Penerapan keamanan yang tinggi diterapkan secara realistis dalam dunia kriptografi, tidak ada algoritma kriptografi yang aman 100%. Arti aman adalah data yang di enkripsi tidak dapat di terjemahkan orang lain tanpa seizin pembuat.

UCAPAN TERIMAKASIH

Alhamdulillah, berkat rahmat Allah SWT yang telah memberikan segala karunia-Nya sehingga penulis dapat menyelesaikan penelitian ini dengan baik dan tepat waktu. Dan tak lupa shalawat dan salam kepada Nabi Muhammad SAW yang telah berjasa besar dengan membukakan jalan dalam perkembangan ilmu pengetahuan seperti sekarang ini.

Tujuan dari penulisan penelitian ini adalah untuk memenuhi salah satu syarat dalam pelaksanaan Tridharma perguruan tinggi.

Dalam rangka penelitian ini tidak terlepas dari bantuan beserta dorongan dari berbagai pihak, peneliti ingin mengucapkan terima kasih kepada Kedua orang tua yang telah mensupport peneliti dalam melaksanakan penelitian, kepada Universitas Dharmawangsa Sebagai tempat peneliti bernaung, kemudian terima kasih kepada Ketua Yayasan Pendidikan Dharmawangsa beserta staf dan karyawan. Tidak terlupa kepada mahasiswa dan mahasiswi Universitas Dharmawangsa.

DAFTAR PUSTAKA

Fathansyah, Ir, *"Sistem Basis Data ",* Penerbit CV. Informatika, Bandung, 2012.

Hakim, Lukmanul. 2008. *Membongkar Trik Rahasia Para Master Php.* Yogyakarta : Toko Media.

Hartono, Jogiyanto. 2002. *Pengenalan Komputer: dasar ilmu komputer, pemrograman, sistem informasi dan inteligensi buatan*, Ed. III. Yokyakarta : Andi Offset.

Hana. 2009. Gaya-hidup.infogue, *http://gayahidup. infogue. com/memilih_profesi_ berdasarkan_ kepribadian*. Diakses tanggal 21 Oktober 2010.

Hoffer A Jeffrey, etc, ***"****Modern Systems Analisis and Design****",*** Second Edition, The Benjamin/ Coming Publishing Company, Inc, Menlo Park, 1996.

Kusrini, M.Kom. 2008. *Aplikasi Sistem Pakar Menentukan Faktor Kepastian Pengguna dengan Metode Kuantifikasi Pertanyaan*. Yogyakarta : Andi Offset.

Munawar. 2005. *Permodelan Visual dengan UML*. Jakarta : Graha Ilmu.

Stinson, D. R, "*Cryptography: Theory and Practice****"****,* Chapman and Hall, 2002.

Wahono, Romi Satria. 2007. *Algoritma forward Chaining pada Rule-Based Expert System. http: //ilmukomputer.org/2007/03/27/ algoritma-forward-chaining-pada-rule-based -expert-system/.* Diakses tanggal 21 Oktober 2010**.**