TWO-FACTOR AUTHENTICATION UNTUK KEMANAN TRANSAKSI ONLINE STUDI KASUS WEBDOSEN UNIVERSITAS BUDI LUHUR

M. Anif
FTI - Universitas Budi Luhur

ABSTRAK

Hampir semua organisasi menghadapi masalah berkaitan dengan perlindungan asset digital yang dimilikinya, Beberapa hal dilakukan oleh organisasi untuk mengatasi masalah tersebut. Yaitu dilakukan dengan melindungi sistem komputer dan aplikasinya dari penyalahgunaan oleh pengguna lain yang tidak berkepentingan melalui penggunaan password. Memang, kalau kita perhatikan dalam kurun waktu singkat password tidak akan tergantikan. Dimana, password adalah cara efektif untuk melindungi asset yang sebagian sudah dilindungi melalui akses fisik, yang terbatas dan diawasi. Namun password yang memiliki sifat statis tidak 100% dapat mengamankan sistem tersebut dari penyalahgunaan.

Begitu juga halnya dengan proses pengisian nilai Tugas, UTS dan UAS di Universitas Budi Luhur telah mengalami perkembangan yang sangat pesat, dengan versi terakhirnya aplikasi tersebut yang sudah berbasis Web. Namun pada tatanan keamanan belum bisa dikatakan aman dalam penggunaannya. User masuk ke dalam aplikasi melalui Single-Factor Authentication atau menggunakan password yang bersifat statik (static password).

Tujuan dari tulisan ini adalah untuk menawarkan pemikiran yang dapat diterapkan dalam setiap network. Untuk menghilangkan penyalahgunaan dari sistem keamanan yang serupa dengan cara mengisolasi mereka dari kelemahan yang dimiliki oleh faktor yang pertama (metode Single-Factor Authentication) tersebut, dengan menambahkan faktor yang kedua menggunakan password dinamis (metode Two-Factor Authentication) yang penerapannya dibantu dengan menggunakan token. Dalam hal ini token yang dipakai diganti dengan Handphone sebagai media penerima passkey. Passkey tersebut dibangkitkan dengan algoritma acak dari komputer server dan dikirim dengan SMS. Sehingga diharapkan tingkat keamanan akan lebih baik dari sebelumnya.

Keyword : Security, Dynamic Password, Authentication, SMS

I. PENDAHULUAN

LATAR BELAKANG

Single-Factor Authentication seperti *password* pada banyak kasus tidak terlalu aman digunakan pada aplikasi yang dilepas di internet. Hal tersebut karena *password* lebih mudah diingat, dan mudah untuk pengunjung mendeteksi *password* tersebut, seperti tanggal lahir, nama anak, atau nama keluarga, dll. Apalagi *hacker* dapat mengidentifikasi jutaan *password* dengan program yang dibuatnya ketika aplikasi ini di jalankan di internet.

Penerapan Teknologi Informasi ditujukan untuk meningkatkan efisiensi operasi dan meminimalisasi risiko operasi, meningkatkan produktivitas, ketepatan dan keamanan operasi. Selain itu Teknologi Informasi juga digunakan sebagai piranti analisis dan instrumen pemasaran. Dari faktor-faktor tersebut dapat dirasakan pelayanan yang dilakukan sebuah perusahaan kepada pelanggan akan meningkat. Begitu juga dengan pemanfaatan Teknologi Informasi ini di Universitas Budi Luhur diharapkan dapat menjadi nilai tambah dalam pelayanan yang lebih baik kepada dosen dan mahasiswa.

Universitas Budi Luhur, sejak awal berdirinya memiliki mahasiswa aktif per-semester lebih kurang 5000 mahasiswa, dalam perkembangannya selalu saja ada permasalahan dalam pelayanan kepada mahasiswa khususnya keterlambatan mendapatkan kartu hasil studi, kesalahan dalam pengisian nilai dan lain sebagainya. Sehingga kenyamanan dalam pelayanan tidak dirasakan oleh dosen maupun mahasiswa. Namun demikian sejak tahun ajaran baru 2005/2006, Universitas Budi Luhur mencoba memberikan pelayanan yang lebih baik kepada mahasiswa khususnya untuk pengisian nilai mahasiswa yaitu dengan meluncurkan aplikasi berbasis *web* melalui teknologi internet, sehingga Kartu hasil studi bisa dikeluarkan lebih cepat.

Permasalahan ketepatan waktu sudah teratasi, namun permasalahan baru mulia timbul. Transaksi yang dilepas di internet tentu saja harus aman dari gangguan yang bermacam-macam. Sehingga penerapan *Password* yang sekarang dilakukan apabila sifatnya statis tidaklah cukup untuk menjaga transaksi tetap aman, seperti yang sudah dilakukan oleh pihak universitas. Terutama Dosen yang mengisi nilai mahasiswa masih kurang nyaman dan ada ketakutan transaksi yang sudah dilakukan dirubah oleh pihak lain.

Dalam perkembangannya untuk menjadikan aplikasi tersebut lebih aman sudah scharusnya ditambahkan atau diganti dengan metode yang lebih baik. Metode yang ditawarkan adalah pengembangan dari *Single-Factor Authentication* menjadi *Two-Factor Authentication* dengan alat bantu *token* yang memanfaatkan *handphone.*

1. Masalah

- Aplikasi yang berjalan di dalam *web* belum aman
- Penggunaan *password* statis (*single-factor authentication*)

2. Rumusan Masalah

Rumusan masalah adalah bagaimana metode *Single-Factor Authentication* pada aplikasi Pengisian Nilai Mahasiswa Berbasis *Web* dikembangkan menjadi *Two-Factor Authentication*.

3. Batasan Masalah dan Ruang lingkup

Dalam penulisan ini masalah dan ruang lingkup masalah dibatasi pada: Analisa dan penerapan metode *Two-Factor Authentication* untuk keamanan transaksi melalui internet pada Aplikasi Pengisian Nilai Mahasiswa di Universitas Budi Luhur.

4. Tujuan dan Manfaat

Adapun tujuan dari penulisan ini adalah untuk mengindentifikasi celah keamanan yang dianggap rawan dan mengembangkan aplikasi menjadi lebih aman dengan menerapkan algoritma acak, yang digunakan untuk membentuk *password* dinamis sebagai faktor kedua untuk keabsahan dalam melakukan transaksi.

Manfaat dari penelitian ini adalah untuk membangun aplikasi berbasis *web* yang lebih aman, sehingga dapat menjadi nilai tambah bagi Universitas Budi Luhur untuk memberikan pelayanan yang maksimal kepada dosen dan mahasiswa.

II. ANALISIS DAN PEMBAHASAN

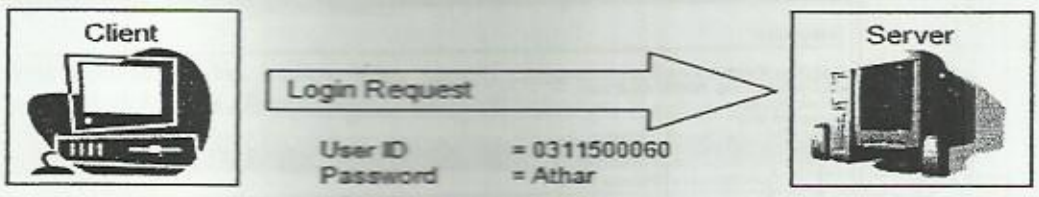
Universitas Budi Luhur, setiap semesternya memiliki +/- 5000 mahasiswa aktif dengan masing-masing mahasiswa rata-rata mengambil 8 mata kuliah. Tentunya banyak kendala yang dihadapi oleh Bagian nilai yang terdapat di Biro Administrasi Akademik. Seperti memasukan nilai mahasiswa. Selama ini nilai di *input* oleh dosen dengan menggunakan sistem yang terakhir berbasis *WEB* pada jaringan publik yang menyediakan berbagai kemudahan. Namun dari sudut pandang lain permasalahan baru mulai timbul, Transaksi yang dilepas di internet tentu saja harus aman dari gangguan yang bermacam-macam.

1. ANALISA SISTEM BERJALAN

Analisa sistem berjalan dapat digambarkan seperti yang terlihat pada dengan langkah-langkah sebagai berikut :

a. Proses login

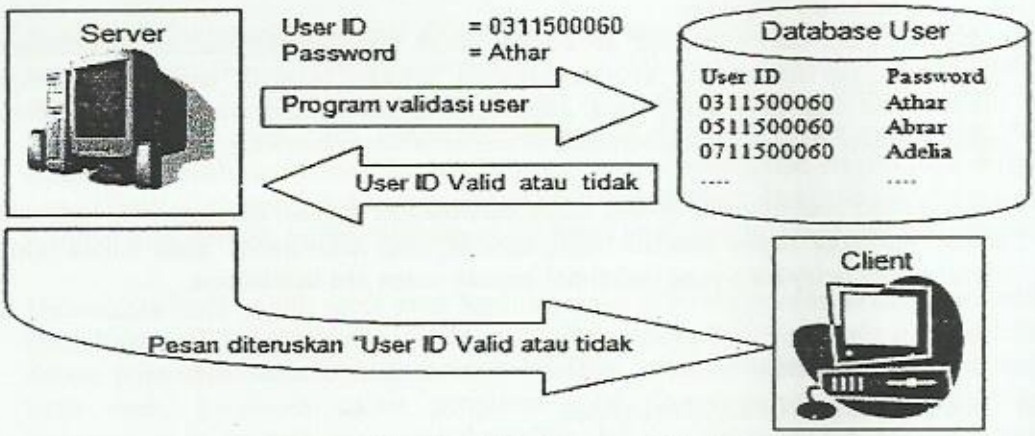
Pada tahapan ini yang diperlihatkan pada gambar 2.1 *user* mengisi ***user id*** dan ***password*** pada komputer *client*, kemudian meminta ke *server* untuk melakukan pemeriksaan keabsahan *user*.



Gambar 2.1 : Proses login

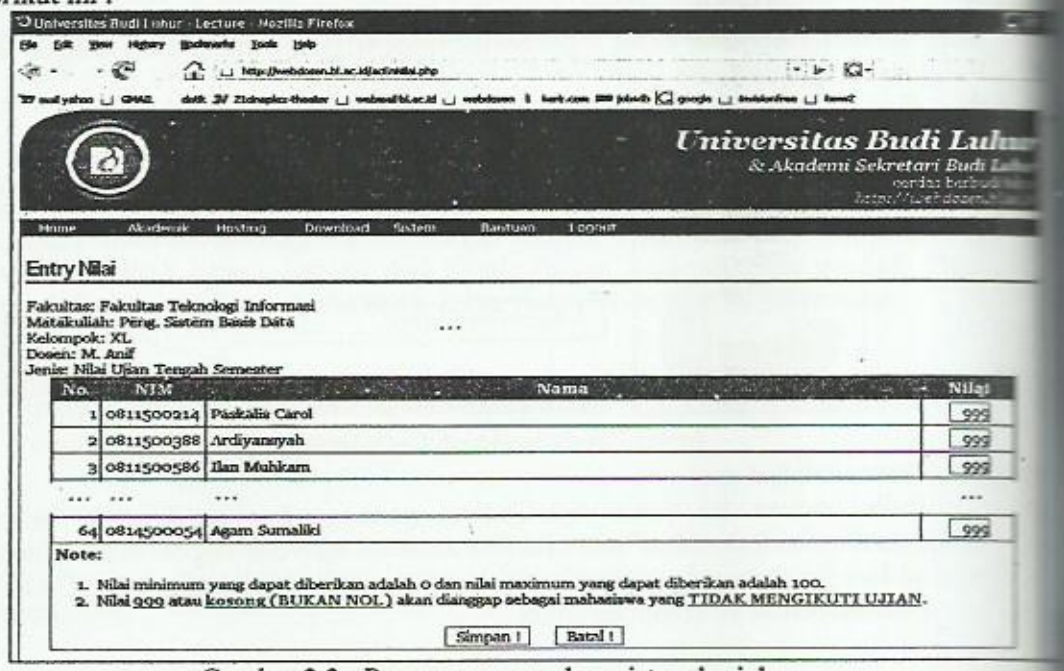
b. Proses validasi *user*

Pada tahapan ini yang diperlihatkan pada gambar 2.2 *server* melakukan pemeriksaan keabsahan *user* kedalam database *user* dan respon akan dikembalikan ke komputer *server*, *valid* atau tidak *valid user id* dan *password* yang dikirimkan. Dan diteruskan ke komputer *client*.



Gambar 2.2 : Proses validasi *user*

c. Proses Transaksi.
User masuk kedalam aplikasi dengan memilih menu entri nilai, dengan tahapan verifikasi hanya menggunakan *password* yang sama. Kemudian melakukan transaksi demi transaksi tanpa melakukan autentikasi dalam bentuk apapun sampai aplikasi berakhir. Yang diperlihatkan pada gambar 2.3 rancangan masukan sistem berjalan berikut ini :



Gambar 2.3 : Rancangan masukan sistem berjalan

2. PERMASALAH PADA SISTEM BERJALAN

Berdasarkan analisa sistem di atas dapat dilihat kelemahan yang terjadi pada tahapan ke 3, dimana semua transaksi yang dilakukan oleh *user* tidak lagi melakukan validasi autentikasi (keabsahan sebuah transaksi) sehingga ada kemungkinan transaksi dapat disalah gunakan oleh pengguna lain yang memanfaatkan kelemahan ini.

3. PENYELESAIAN MASALAH

METODE PENDEKATAN YANG DIGUNAKAN :

Menggunakan metode *two factor autentication*, dimana setiap transaksi harus menggunakan *passkey* yang dibangkitkan dengan menggunakan algoritma acak dan *passkey* yang dibangkitkan dari komputer di *server* kemudian dikirimkan ke *token* dalam hal ini *handphone*. dari hasil yang diterima oleh *handphone* di-*input*-kan ke komputer *client* untuk menjadi faktor kedua dalam bertransaksi.

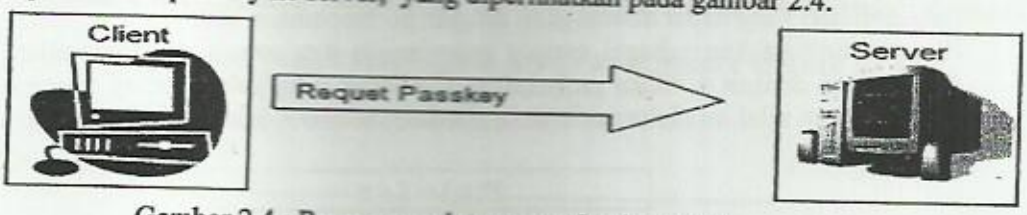
Pemilihan dengan menggunakan algoritma acak didasarkan pada *type authentication token* [atul kahate, 289] yang salah satu tipenya menggunakan metode *Challenge/Response Tokens*. Atas dasar ini diharapkan setiap transaksi dilakukan oleh orang yang tepat, dan setiap transaksi menggunakan *passkey* yang berbeda sehingga manipulasi transaksi tidak mudah terjadi.

4. SISTEM USULAN

Banyak sekali solusi yang ditawarkan dunia ilmu pengetahuan, namun disini kita mencoba menggunakan salah satu solusi atau pendekatan dengan menambahkan satu tahapan pemeriksaan terhadap transaksi, yaitu dengan menambahkan metode *two factor authentication*. Disini transaksi harus diisi dengan sebuah *passkey* yang diproses secara acak melalui komputer *server* dan mengirimkannya kemedia *handphone* yang dimiliki oleh *user* untuk proses validasi terhadap keabsahan transaksi. Contoh dapat diperlihatkan dengan langkah-langkah sebagai berikut :

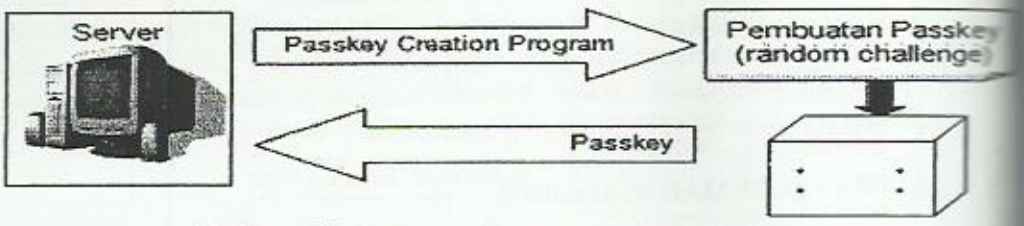
Untuk langkah **pertama** dan **kedua** sama seperti yang dilakukan pada sistem berjalan, sedangakan langkah ke tiga dikembangkan menjadi beberapa langkah sbb:

a. Proses permintaan passkey ke server, yang diperlihatkan pada gambar 2.4.



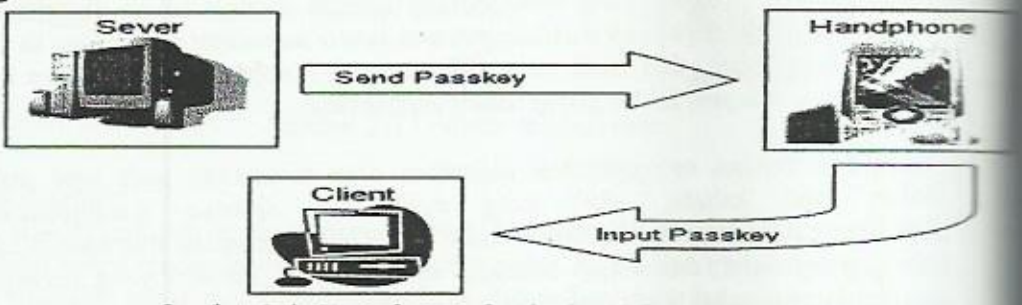
Gambar 2.4 : Proses permintaan *passkey* ke *server*

b. Proses pembuatan *passkey*, yang diperlihatkan pada gambar 2.5.



Gambar 2.5 : Proses pembuatan *passkey*

c. Transfer *passkey* ke *handphone* dan di *input* ke komputer *client* , yang diperlihatkan pada gambar 2.6.



Gambar 2.6 : Transfer *passkey* ke *handphone*

1) ANALISA *PASSKEY* :

Untuk menghasilkan sebuah *passkey* dapat dinyatakan dengan rumus sbb:

$$k = \{ s_1, s_2, s_3, s_4, s_5, s_6 \}$$

Dimana:

k adalah ***passkey*** dengan menggabungkan $s_1, s_2, s_3, s_4, s_5, s_6$.

s_i berisi satu karakter yang diambil dari data *array* dengan pola acak. Demikian juga untuk s_2, s_3, s_4, s_5, s_6.

Karakter yang disimpan ke $s_1, s_2, s_3, s_4, s_5, s_6$ menggunakan teori kemungkinan (probabilitas) yang dapat diterangkan dengan perumpamaan sbb:

Jika **a** diumpamakan sebagai tempat menyimpan data *array*, dimana panjang *array* **a** disimbolkan dengan **n,** Maka probabilitas nilai acak yang keluar secara matematik adalah **1/n** kemudian nilai ini disimpan kedalam sebuah notasi **r**, untuk r_1 di rumuskan sbb:

$$P(r_1) = 1 / n$$

Kemudian nilai yang terdapat pada r_1 dijadikan posisi dimana kita mengambil karakter yang terdapat pada array **a**.

$$s_1 = a(r_1)$$

Demikian juga dilakukan untuk mendapatkan nilai acak r_2, r_3, r_4, r_5, r_6.

2) PEMBUATAN *PASSKEY*

yang diperlihatkan

sbb:

cak. Demikian juga

teori kemungkinan

ana panjang *array* a
ra matematik adalah
rumuskan sbb:

mengambil karakter

r_6.

Misalnya :

a = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"

n = panjang a

r_1 = *random* angka 0 s/d n

Jika:

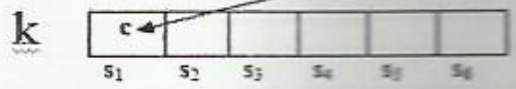
Kita misalkan hasil *random* untuk r_1 yang keluar angka 12

Maka:

karakter yang diambil berada pada *array* a diposisi r_1 yaitu c kemudian disimpan ke s_1. yang digambarkan sbb:

a = "0 1 2 3 4 5 6 7 8 9 a b c d e f g h I j k l m n o p q r s .....X Y Z"

posisi = 0 1 2 3 4 5 6 7 8 9 10 11 12 13.....



dan seterusnya dilakukan hal yang sama untuk r_2, r_3,r_4, r_5, r_6.

3) ALGORITMA *PASSKEY*

1. kosongkan k
2. isi array a dengan sejumlah data *array*
3. ulangi sebanyak 6 kali, lakukan

   isi r dengan nilai yang sudah diacak dengan batasan yang sudah ditentukan

   cari karakter yang terdapat pada *array* a di posisi r simpan ke s

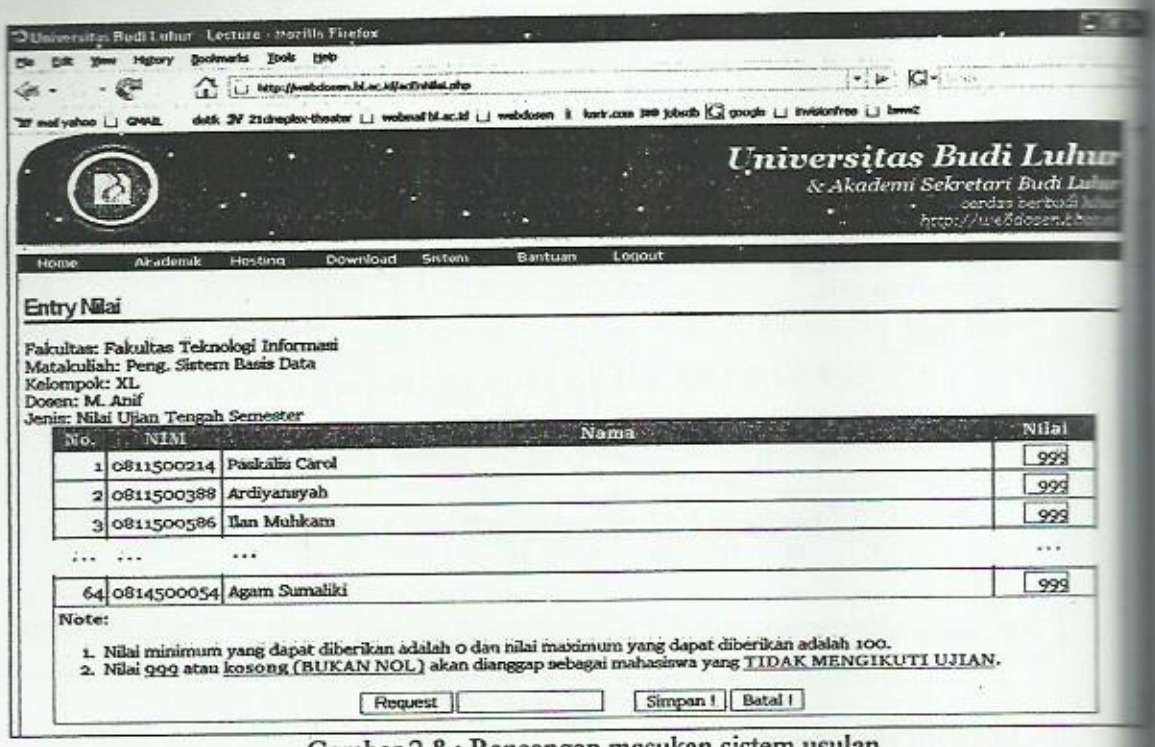
   gabungkan s ke k setiap terjadi pengulangan
4. akhiri pengulangan

4) *PROTOTYPE* APLIKASI

Dari tahapan analisa, dapat kita sajikan sebuah prototipe untuk menyelesaikan masalah diatas, seperti berikut :

RANCANGAN MASUKAN SISTEM USULAN

Dari rancangan masukan sistem berjalan dikembangkan sebuah rancangan baru, yaitu dengan menambahkan dua buah komponen dan perbaikan terhadap komponen tombol simpan. Seperti terlihat pada gambar 2.8 berikut :



Gambar 2.8 : Rancangan masukan sistem usulan

RANCANGAN PROSES SISTEM USULAN

Dengan ditambahkan dua komponen tersebut, tentunya masing masing komponen memiliki fungsi dan kegunaannya, yang diperlihatkan seperti berikut :

1. Komponen tombol **Request** yang berfungsi untuk meminta kepada server passkey yang digunakan untuk bertransaksi. Dan passkey tersebut dikirim ke sebuah handphone milik user yang bersangkutan.
2. Komponen **Kotak Teks** yang berfungsi untuk menginputkan passkey yang diterima melalui handphone tersebut.
3. Selain itu memperbaiki algoritma dari komponen tombol **Simpan** dengan menambahkan fungsi pemeriksaan kebenaran passkey yang dimasukan. Untuk selanjutnya dilakukan proses penyimpanan ke dalam database nilai.
4. Sedangkan komponen tombol **Batal** masih melakukan fungsi yang sama.

III. KESIMPULAN

Dari pembahasan melalui penggunaan metode *two-factor authentication* menjadikan aplikasi yang ditanam dijaringan publik/*internet* akan lebih aman dari pada sebelumnya yang hanya menggunakan *single-factor authentication.* Dan dapat

meningkatkan kepe
penyelahgunaan pe

IV. DAFTAR P

1. Criptograph
2. Managemen
Thomson C
3. Two-Factor
Hockings (
2005
4. A Strong A
Dario Aniba
5. www.crypto
6. What To Lo
March 31, 2

ngan baru, yaitu
omponen tombol

sing komponen

kepada server
ebut dikirim ke

n passkey yang

Simpan dengan
masukan. Untuk
ai.
g sama.

authentication
aman dari pada
n. Dan dapat

meningkatkan kepercayaan pengguna, sehingga rasa ketakutan yang dalam terhadap penyelahgunaan penggunaan menjadi tidak dirasakan lagi.

IV. DAFTAR PUSTAKA

1. Criptography and *network* security, Atul Kahate, Mc Grow Hill, 2003.
2. Management Information Security, Michael E. Whitman and Herbert J. Mattord, Thomson Course Teknology, 2004.
3. Two-Factor *Authentication* using Tivoli Access Manager *Web*SEAL, Christopher Hockings (hockings@au1.ibm.com), Software Engineer, IBM, Updated 06 Oct 2005
4. A Strong *Authentication* Mechanism for Consumer-Facing Online Transactions, Dario Anibal Marra, MIT - Department of EECS, Chisec Group, May 16, 2005
5. www.cryptocard.com
6. What To Look For In Consumer Strong *Authentication* Solutions, Jonathan Penn, March 31, 2005