IMPLEMENTASI ONE TIME PASSWORD BERBASIS GAMBAR PADA WEBSITE ECOMMERCE PTIIK UNTUK MENINGKATKAN SEKURITAS

Winny Ayu Paramita[1], Himawat Aryadita[2], Aswin Suharsono[3]
Program Studi Teknik Informatika
Program Teknologi Informasi dan Ilmu Komputer
Universitas Brawijaya Malang
[1]winnyayuparamita@gmail.com, [2] himawat@ub.ac.id, [3]aswin@ub.ac.id

ABSTRACT

Data which stored on the internet is not secured enough so it needs to be secured by right authentication system. Authentication mechanism that is often used now is textual passwords where many and varied characters cause users easily forget the password. One Time Password (OTP) authentication mechanism image based is expected to solve both issues. OTP is a mechanism to log in using password that can only be used one time. Image-based passwords is used because a scientific experiment show that humans are very good in identifying, remembering, and accommodate image patterns rather than text patterns. OTP image based which are implemented in ecommerce website PTIIK UB Faculty aims to design a secure authentication system of the Man In The Middle attacks and Brute Force passive then wanted to know how the user response. Validation testing using a black-box system produces 100 % valid. User acceptance testing is done by distributing 50 questionnaires that produce that 34.7 % respondents have not responded positively to this method because of these factors: because the characters in the picture is always changing so the user needs to see one by one, the picture is less common so it is difficult to remember and this method is unconventional. Testing security by performing passive Man In The Middle attacks and brute force attacks through existing programs resulted that password can not be found. Passwords can be known if the attacker knows the flow of this method then implementing it in a brute-force program.

Keywords : *one time password, graphical password, security, ecommerce*

ABSTRAK

Data yang tersimpan di internet belum terjamin keamanannya sehingga perlu diamankan dengan sistem autentikasi yang tepat. Mekanisme autentikasi yang sering dipakai sekarang adalah *textual password* dimana banyak dan bervariasinya karakter menyebabkan pengguna mudah lupa pada *password*nya. Mekanisme autentikasi *One Time Password* (OTP) berbasis gambar diharapkan dapat mengatasi dua masalah tersebut. OTP adalah mekanisme *login* menggunakan *password* yang hanya dapat digunakan satu kali saja. *Password* berbasis gambar digunakan karena percobaan ilmiah menunjukkan bahwa manusia sangat baik dalam mengidentifikasi, mengingat, dan menampung pola gambar daripada pola teks. OTP berbasis gambar yang diimplementasikan pada website *ecommerce* Fakultas PTIIK Universitas Brawijaya ini bertujuan untuk mendesain sistem autentikasi yang aman dari serangan *Man In The Middle pasif* dan *Brute Force* kemudian ingin mengetahui bagaimana respon pengguna. Pengujian validasi menggunakan metode *black-box* menghasilkan sistem 100% valid. *User acceptance testing* dilakukan dengan membagikan 50 kuesioner yang menghasilkan sebanyak 34,7% responden belum merespon positif metode ini karena beberapa faktor yaitu karena karakter pada gambar selalu berubah sehingga pengguna perlu melihat satu persatu, gambar kurang umum sehingga susah diingat dan faktor keterbiasaan. Pengujian keamanan dengan melakukan serangan *Man In The Middle* pasif dan serangan *brute force* melalui program yang telah ada menghasilkan bahwa *password* tidak dapat ditemukan. *Password* dapat diketahui apabila penyerang mengetahui alur dari metode ini kemudian mengimplementasikannya ke dalam sebuah program *brute force*.

Kata Kunci : *one time password, graphical password,* keamanan*, ecommerce*

1. PENDAHULUAN

Latar Belakang

Perkembangan teknologi saat ini menyebabkan maraknya kegiatan jual beli secara online. *E-commerce* merupakan salah satu teknologi yang digunakan untuk melakukan proses perdagangan yang dilakukan melalui *World Wide Web*. Setiap pengguna yang ingin terlibat di dalam kegiatan *ecommerce* perlu mendaftarkan diri dengan mengisi data-data yang nantinya diperlukan untuk menunjang segala transaksi yang ada.

Data yang tersimpan di ruang internet belum tentu terjamin keamanannya. Data tersebut bisa dicuri atau disadap untuk kepentingan tertentu. Oknum-oknum tertentu bisa saja mencoba semua kemungkinan *password* yang mungkin (*Brute Force*) atau berusaha menyadap informasi yang kita kirim ke server dengan menggunakan serangan *Man in The Middle* untuk mencoba masuk ke dalam akun kita. Untuk mengatasi serangan-serangan itu, data dan informasi yang disimpan bisa diselamatkan dengan menggunakan sistem autentikasi yang tepat. Autentikasi adalah proses validasi pengguna pada saat memasuki sistem. Autentikasi bertujuan untuk membuktikan siapa anda sebenarnya, apakah anda benar-benar orang yang diklaim sebagai dia (*who you claim to be*) [11]. Salah satu mekanisme autentikasi yang digunakan untuk mencegah berbagai bentuk pencurian identitas dengan memastikan bahwa kombinasi nama atau password pengguna tidak dapat digunakan sebanyak dua kali adalah One Time Password (OTP). OTP merupakan mekanisme login ke dalam sebuah jaringan atau layanan dengan menggunakan password yang unik yang hanya dapat digunakan satu kali saja. [5]

Mekanisme autentikasi dibagi ke dalam tiga bentuk umum yaitu *token-based system, biometrics-based system*, dan *knowledge-based system. Token-based system* adalah autentikasi yang menggunakan objek yang bersifat eksklusif dan hanya dimiliki oleh pengguna tertentu sebagai identifikasi. *Biometrics-based system* menggunakan bagian tubuh tertentu misalnya sidik jari untuk proses autentikasi. Sedangkan *knowledge-based system* terbagi menjadi dua yaitu *textual password* dan *graphical password* yang keduanya sama-sama menggunakan informasi dimana hanya diketahui oleh pengguna tersebut [7].

Mekanisme autentikasi yang sering dipakai sekarang adalah *textual password*. Banyak dan bervariasinya karakter pada *textual password* menyebabkan pengguna mudah lupa *password* yang telah dibuat sendiri. Hal ini ditunjang dengan percobaan ilmiah yang menunjukkan bahwa manusia sangat baik dalam mengidentifikasi, mengingat, dan menampung pola gambar daripada pola teks [15]. Dalam penelitian kali ini penulis mengimplementasikan proses *login* dengan menggunakan gambar. Dalam penelitian sebelumnya, "*Secured Authentication Protocol System using Images"* telah dapat mengatasi masalah yang dihadapi dan dapat menjamin kerahasiaan dan autentikasi saat mengirim pesan [4].

Berdasarkan paparan informasi di atas, penulis mengambil judul skripsi "*Implementasi One Time Password (OTP) Berbasis Gambar pada Website E-commerce PTIIK untuk Meningkatkan Sekuritas*". Implementasi difokuskan pada kemanan data pada saat proses autentikasi.

Rumusan Masalah

Berdasarkan penjelasan pada latar belakang yang telah dikemukakan, maka masalah yang akan diteliti oleh penulis adalah:

1. Bagaimana mendesain sistem autentikasi yang aman untuk *website ecommerce* khususnya *website ecommerce* fakultas PTIIK Universitas Brawijaya?
2. Bagaimana implementasi OTP berbasis gambar pada *website ecommerce* fakultas PTIIK Universitas Brawijaya?
3. Apakah OTP berbasis gambar pada website *ecommerce* PTIIK dapat mencegah serangan *Man In The Middle* dan *Brute Force*?
4. Bagaimana respon dari pengguna saat menggunakan metode OTP berbasis gambar pada proses autentikasi?

Batasan Masalah

Batasan masalah dari penelitian ini yaitu:

1. Penelitian difokuskan pada metode *One Time Password* (OTP) berbasis gambar saat melakukan proses daftar, *login*, ubah akun dan *reset password* pada pembeli dan penjual
2. Pilihan gambar sebanyak 36 gambar untuk *password* sebagai percobaan pertama sudah ditetapkan.
3. Gambar yang telah dipilih dapat dipilih kembali sebagai *password*nya dan minimal enam karakter (tiga gambar) yang harus dimasukkan sebagai *password* dengan urutan gambar yang tidak boleh berubah.
4. Pengembangan *website ecommerce* PTIIK ini menggunakan metode *waterfall* yang terdapat proses *reuse* di dalamnya

5. Pengujian keamanan yang dilakukan adalah untuk mencegah seseorang mengetahui password pengguna dari serangan *Man In The Middle* berbentuk pasif dengan menggunakan *Wireshark* dan dari serangan *Brute Force* dengan menggunakan program yang sudah ada yaitu *Fireforce* dan program yang dibuat dengan menggunakan PHP Curl
6. Website *ecommerce* dalam penelitian ini menggunakan bahasa pemrograman PHP dengan *framework Code Igniter* dan basis data MySQL.

Tujuan

Tujuan dari skripsi ini yaitu :

1. Mendesain sistem autentikasi yang aman pada *website ecommerce* fakultas PTIIK Universitas Brawijaya
2. Mengimplementasikan OTP berbasis gambar pada *website ecommerce* fakultas PTIIK Universitas Brawijaya
3. Mencegah adanya serangan *Man in The Middle Attack* dan *Brute Force* pada *website ecommerce* fakultas PTIIK Universitas Brawijaya
4. Mengetahui bagaimana respon pengguna terhadap metode OTP berbasis gambar pada *website ecommerce* fakultas PTIIK Universitas Brawijaya ini

.

Manfaat

Manfaat yang didapatkan dari skripsi ini yaitu:

1. Bagi penulis
   a. Dapat lebih memahami tentang metode OTP berbasis gambar.
   b. Mengimplementasikan pengetahuan tentang keamanan jaringan dan pemograman web
2. Bagi pembaca/ pengguna
   a. Mendapatkan wawasan akan pengimplementasian dari OTP berbasis gambar pada website *ecommerce*.
   b. Mendapatkan rasa aman pada data-datanya yang tersimpan di *website ecommerce*

Kajian Pustaka

Kajian pustaka pada penelitian ini adalah membandingkan penelitian ini dengan penelitian sebelumnya yang berjudul '*Secured Authentication Protocol System using Images'*.

Perbedaan antara penelitian sebelumnya dan yang diusulkan adalah pada proses autentikasi dan pengujian yang dilakukan. Pada penelitian sebelumnya menggunakan *hidden characters* untuk melakukan proses *mapping* terhadap komponen-komponen yang ada sedangkan pada penelitian yang diusulkan menggunakan tabel yang menyimpan urutan gambar dan *index* untuk proses *mapping* terhadap komponen-komponen yang ada. Perbedaan yang kedua adalah pada sisi pengujian. Penelitian sebelumnya lebih difokuskan pada pengujian keamanan sedangkan penelitian yang diusulkan akan menguji dari sisi keamanan dan dari sisi *user* (*user acceptance testing*)

Autentikasi

Autentikasi adalah suatu mekanisme yang digunakan oleh suatu sistem untuk mengidentifikasi user yang berhak mengakses informasi pada sistem tersebut. Mekanisme autentikasi yang ada saat ini dibagi ke dalam tiga bentuk umum:

a. *Token-based system* menggunakan suatu objek yang eksklusif yang hanya dimiliki oleh *user* tertentu sebagai bentuk identifikasi. Salah satu contohnya adalah penggunaan kartu ATM, dimana setiap pemilik memiliki satu kartu untuk proses autentikasi.
b. *Biometrics-based system* menggunakan ciri khas tubuh tertentu dari *user* sebagai proses autentikasi. Cara ini memiliki tingkat keamanan yang sangat tinggi, namun belum banyak digunakan karena membutuhkan biaya yang cukup mahal dan proses identifikasi yang cukup lama. Beberapa contohnya adalah *fingerprints*, iris *scan*, dan *facial recognition*.
c. *Knowledge-based system* menggunakan suatu informasi yang hanya diketahui oleh *user*. Sistem ini dibagi ke dalam dua kategori umum yaitu tekstual *password* dan *graphical password*.[7]

Autentikasi dapat dikatakan aman apabila terhindar dari *password attacks*. *Password attacks* yang dapat terdiri dari *Brute Force Attacks, Dictionary Attack, Phishing Attacks, Shoulder Surfing, Key Loggers, Replay Attacks (*bagian dari *man in the middle attack) dan Video Recording Attack [12].* Pada skripsi kali ini, penulis menggunakan *brute force* dan *man in the middle* pasif untuk pengujian keamanan autentikasi.

One Time Password

One Time Password merupakan mekanisme *login* ke dalam sebuah jaringan atau layanan dengan menggunakan *password* yang unik yang hanya dapat digunakan satu kali saja. Hal ini digunakan untuk mencegah berbagai bentuk pencurian identitas dengan memastikan bahwa kombinasi nama atau *password* pengguna tidak dapat digunakan sebanyak dua kali. Password yang digunakan tetap sama pada proses *login* yang biasa dilakukan, namun pada one time *password password* yang digunakan berubah setiap melakukan proses *login*. One time *password* adalah bentuk dari autentikasi yang kuat dan menawarkan perlindungan yang lebih efektif untuk rekening bank, jaringan perusahaan dan sistem lain yang berisi data sensitif. [5]

Pengujian Validasi

Pada kulminasi pengujian terintegrasi, perangkat lunak secara lengkap dirakit sebagai suatu paket; kesalahan *interfacing* telah diungkap dan dikoreksi, dan seri akhir dari pengujian perangkat lunak, yaitu pengujian validasi dapat dimulai. Validasi perangkat lunak dicapai melalui sederetan pengujian *black-box* yang memperlihatkan konformitas dengan persyaratan. [10]

Pengujian *black-box* berusaha menemukan kesalahan dalam kategori berikut:

1. Fungsi-fungsi yang tidak benar atau hilang.
2. Kesalahan *interface.*
3. Kesalahan dalam struktur data atau akses *basis data* eksternal.
4. Kesalahan kinerja.
5. Inisialisasi dan kesalahan terminasi

User Acceptance Testing

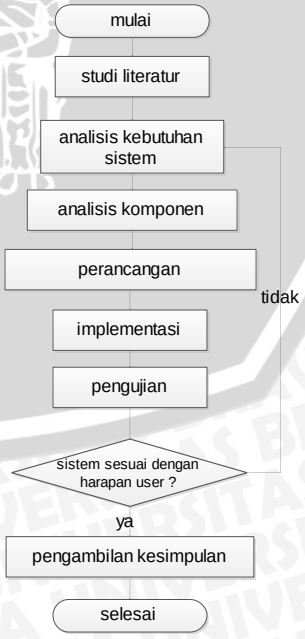
User Acceptance Testing (UAT) adalah salah satu prosedur proyek perangkat lunak akhir dan kritis yang harus terjadi sebelum perangkat lunak baru dikembangkan akan tergulir keluar ke pasar. Selama UAT, pengguna perangkat lunak sebenarnya menguji perangkat lunak untuk memastikan dapat menangani tugas-tugas yang diperlukan dalam skenario dunia nyata dan sesuai dengan spesifikasi [9].

Pengujian Keamanan

Pengujian (*Testing*) keamanan saat proses autentikasi dilakukan dengan dua jenis serangan yaitu *Man In The Middle* dan *Brute Force.* Untuk serangan Man In The Middle digunakan *software* penyadap Wireshark. Wireshark adalah sebuah *network packet analyzer* yang mencoba menangkap paket-paket jaringan dan berusaha untuk menampilkan semua informasi di paket tersebut sedetail mungkin [2]. Sedangkan untuk serangan *brute force*, peneliti menggunakan program *Fireforce* dan program yang dibuat dengan menggunakan CURL. *FireForce* adalah ekstensi *Firefox* yang dirancang untuk melakukan serangan *brute-force* pada *form GET* dan *POST [3].* CURL alias URL Client merupakan sebuah *library* yang berbasis *command line*, dimana dapat digunakan untuk memasukkan parameter ke dalam *web request [6].*

2. METODE PENELITIAN

Pengembangan proses aplikasi dikembangkan dengan metode pengembangan perangkat lunak SDLC menggunakan model *waterfall* yang didalamnya terdapat *reuse* karena tahapan pengembangan aplikasi yang dilakukan oleh penulis sesuai dengan tahapan model *waterfall* yang akan digambarkan pada Gambar 3.1. Sedangkan untuk pemakaian *reuse*, penulis menyisipkan salah satu tahapan dari *software reuse* yaitu analisis komponen karena pada pengembangan aplikasi ini, penulis melakukan proses *reuse* terhadap komponen-komponen yang ada. Komponen-komponen tersebut digunakan untuk menunjang fungsionalitas dari *website ecommerce*. Pada skripsi ini, pengembangan *reuse* mayoritas dipakai untuk fungsi transaksi kegiatan penjualan pembelian.



Gambar 1 Diagram alir runtutan pengerjaan skripsi secara umum

3. PERANCANGAN

Aplikasi yang dikembangkan pada penelitian ini adalah sebuah aplikasi berbasis *web ecommerce* yang proses autentikasinya menggunakan OTP berbasis gambar. Aplikasi berbasis web ini akan digunakan di Fakultas PTIIK Universitas Brawijaya. Secara fungsionalitas website ini tidak berbeda dengan website *ecommerce* pada umumnya, namun proses autentikasi yang diterapkan menggunakan metode *One Time Password* (OTP) berbasis gambar. Alur sistem secara umum digambarkan seperti gambar di bawah ini.

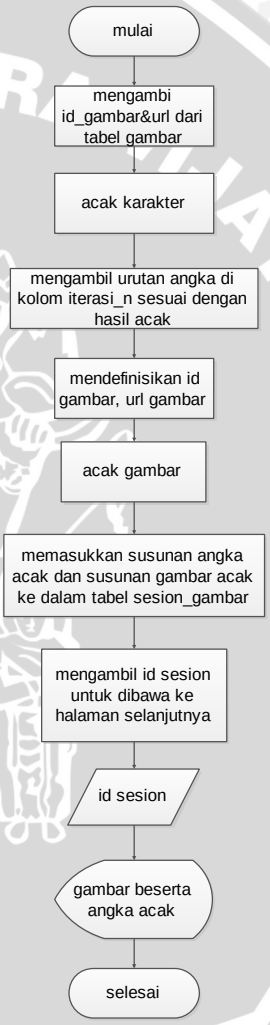
Gambar 2. Arsitektur sistem secara umum

Pengunjung yang mengunjungi website ini dapat melihat barang-barang yang dijual. Namun untuk melakukan kegiatan jual beli secara online, pengunjung tersebut harus mendaftarkan dirinya sebagai pembeli atau penjual. Setelah mendaftar, penjual dapat menjual produknya dan pembeli dapat membeli barang yang tersedia di *web*site ini. Sedangkan *administrator* bertugas memproses pesanan pembelian dari pembeli.

Proses daftar, *login*, ubah, dan reset *password* menggunakan OTP berbasis gambar. Pengguna mengisi data untuk akunnya seperti biasa. Namun untuk mengisi *field password*, pengguna perlu memilih minimal tiga gambar dari 36 gambar yang tersedia. Kemudian karakter yang tertera pada gambar yang telah menjadi pilihannya dimasukkan ke *field password*. Gambar-gambar yang dipilih itulah yang nantinya akan menjadi *password* pengguna tersebut. Karakter-karakter yang tertera pada gambar dan juga posisi gambar akan berubah setiap pengguna me-*reload* halaman. Hal ini mengakibatkan karakter yang dimasukkan oleh pengguna selalu berubah-ubah setiap ia melakukan proses daftar, *login*, ubah, atau *reset password*. Untuk itu, pengguna hanya perlu mengingat gambar yang telah dipilih secara berurutan untuk masuk ke dalam aplikasi.

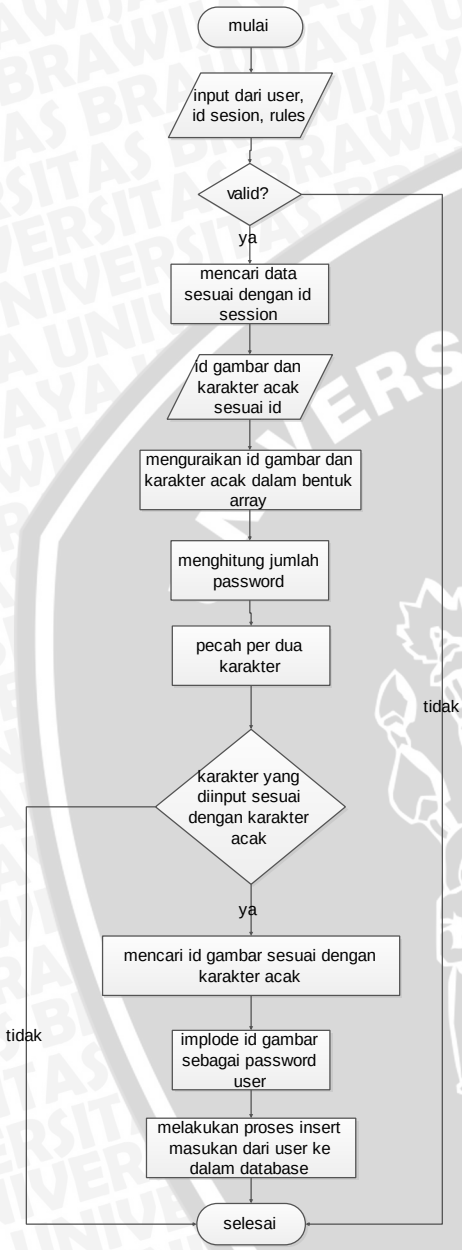
Perancangan algortima pada aplikasi dimodelkan dalam bentuk *flowchart*. Adapun algoritma yang dimodelkan adalah beberapa algoritma yang merupakan algoritma utama pada aplikasi, yaitu algoritma proses menampilkan gambar beserta karakter yang acak, proses *register*, proses *login*, proses *edit* akun dan proses *reset password*.

Flowchart proses menampilkan gambar acak beserta karakter acak dapat dilihat pada Gambar 3. Proses ini digunakan sebagai fitur memilih *password* untuk pembeli dan penjual.



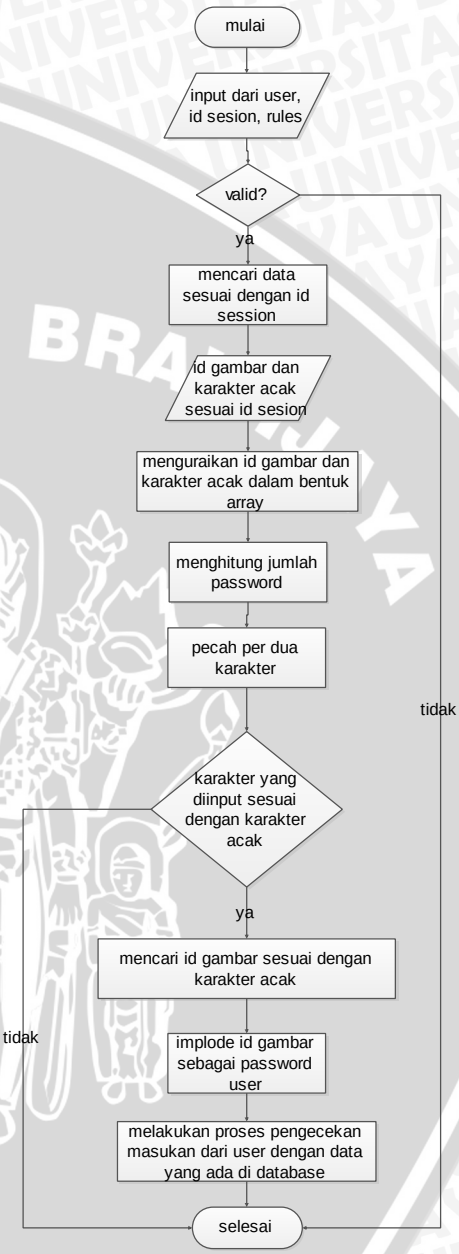
Gambar 3.*Flowchart* Proses Menampilkan Gambar Acak Beserta Karakter Acak

Flowchart proses *register* untuk pembeli dan penjual dapat dilihat pada Gambar 4



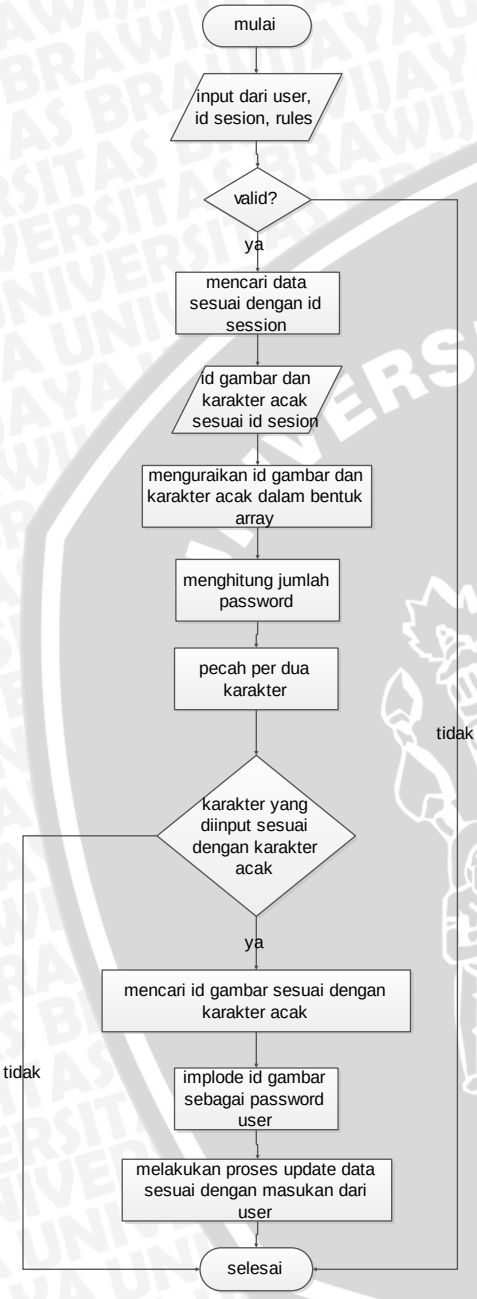
Gambar 4 *Flowchart* Proses Algoritma Register

Flowchart proses *login* untuk pembeli dan penjual dapat dilihat pada Gambar 5



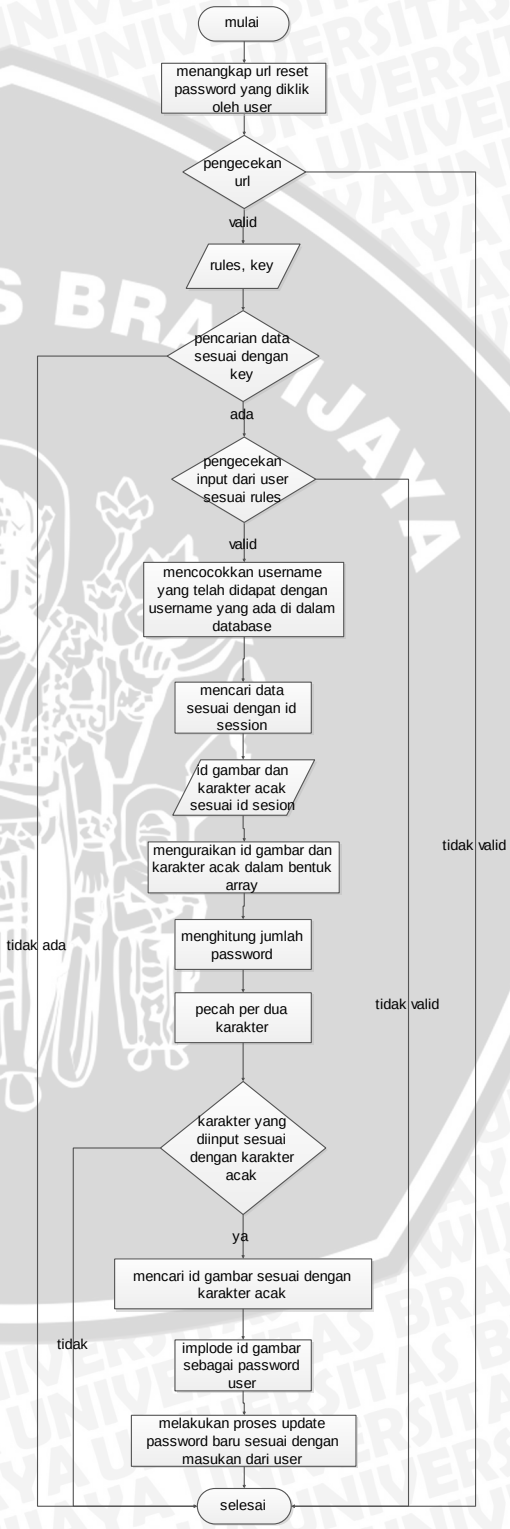
Gambar 5 *Flowchart* Proses Algoritma *Login*

Flowchart proses *edit* akun untuk pembeli dan penjual dapat dilihat pada Gambar 6



Gambar 6 *Flowchart* Proses Algoritma *Edit* Akun

Flowchart proses *reset password* untuk pembeli dan penjual yang lupa terhadap *password*nya dapat dilihat pada Gambar 7

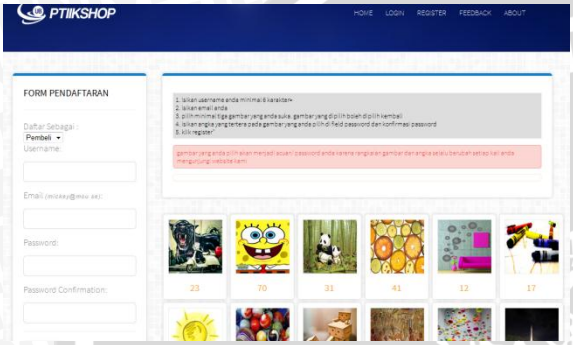


Gambar 7 *Flowchart* Proses Algoritma *Reset Password*

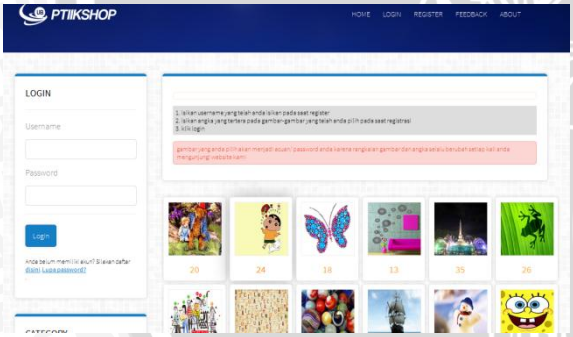
4. IMPLEMENTASI

Aplikasi ini diimplementasikan dengan notebook ASUS K42Jc dengan Operating system Microsoft Windows 7 Ultimate 32-bit, Adobe Dreamweaver CS5, Bahasa Pemrograman PHP, Bahasa Pemrograman MySQL, dan dengan Framework Code Igniter.

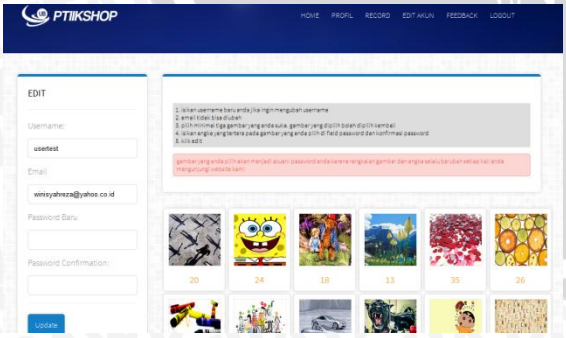
Berikut di bawah ini adalah tampilan dari halaman *register*, *login*, *edit* akun dan *reset password* yang merupakan implementasi dari OTP berbasis gambar



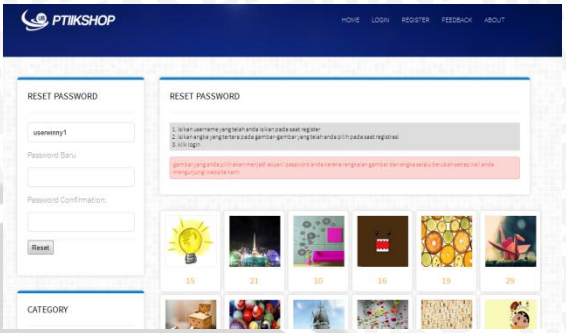
Gambar 8 Tampilan Halaman *Register*



Gambar 9 Tampilan Halaman *Login*



Gambar 10 Tampilan Halaman *Edit* Akun



Gambar 11 Tampilan Halaman *Reset Password*

5. PENGUJIAN DAN ANALISIS

Pengujian Validasi

Pengujian validasi digunakan untuk mengetahui apakah sistem yang dibangun sudah benar sesuai dengan yang dibutuhkan. Pengujian validasi menggunakan metode pengujian *Black Box* dengan hasil seperti di bawah ini

Tabel 1. Hasil pengujian validasi

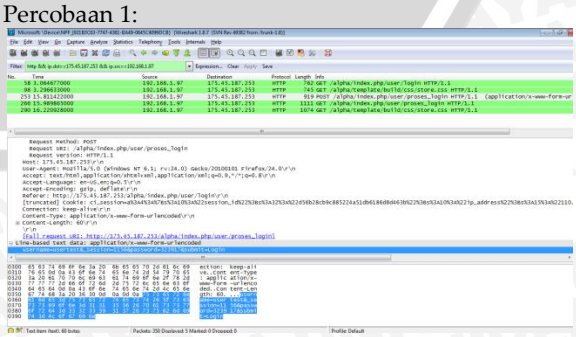
No.	Nama Kasus Uji	Status Validitas
1	Kasus Uji Login Sah	Valid
2	Kasus Uji Login Tidak Sah	Valid
3	Kasus Uji Register	Valid
4	Kasus Uji Mengedit Akun Personal	Valid
5	Kasus Uji Mengelola *Reset Password*	Valid

Pengujian Keamanan

Kasus Uji *Man in The Middle*

Pengujian dilakukan dengan menggunakan *wireshark*. *Wireshark* akan menangkap paket-paket jaringan dan menampilkan informasi paket tersebut. Pengujian dilakukan tiga kali berturut-turut saat proses *login* dengan pengguna yang sama. Berikut adalah informasi yang ditangkap oleh *wireshark* saat pengguna masuk ke dalam sistem

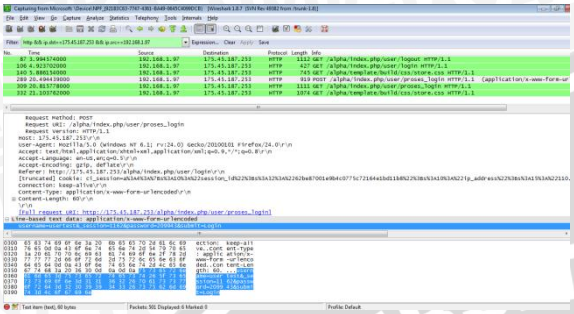
Percobaan 1:



Gambar 12 Gambar *Printscreen* Hasil Pengujian dengan Menggunakan *Wireshark* Pengujian Pertama

Informasi yang didapat dari percobaan 1 adalah:
username=usertest&_session=1156&password=323917&submit=Login

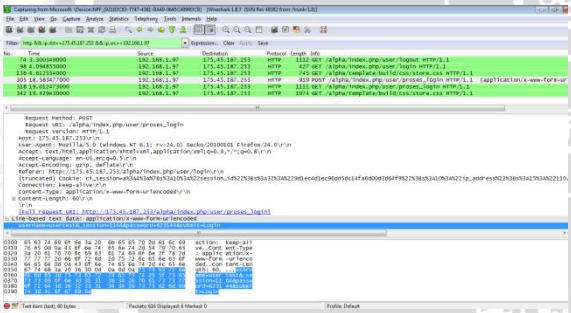
Percobaan 2:



Gambar 13 Gambar *Printscreen* Hasil Pengujian dengan Menggunakan *Wireshark* Pengujian Kedua

Informasi yang didapat dari percobaan 2 adalah:
username=usertest&_session=1162&password=209943&submit=Login

Percobaan 3:



Gambar 14 Gambar *Printscreen* Hasil Pengujian dengan Menggunakan *Wireshark* Pengujian Ketiga

Informasi yang didapat dari percobaan 3 adalah:
username=usertest&_session=1164&password=623144&submit=Login

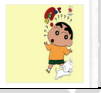
Berdasarkan hal tersebut maka dapat diambil kesimpulan bahwa dari tiga kali proses *login* yang dilakukan oleh pengguna yang sama, *password* yang diinputkan oleh pengguna berbeda-beda sehingga *password* sebenarnya tidak dapat diketahui melalui cara ini.

Kasus Uji *Brute Force*

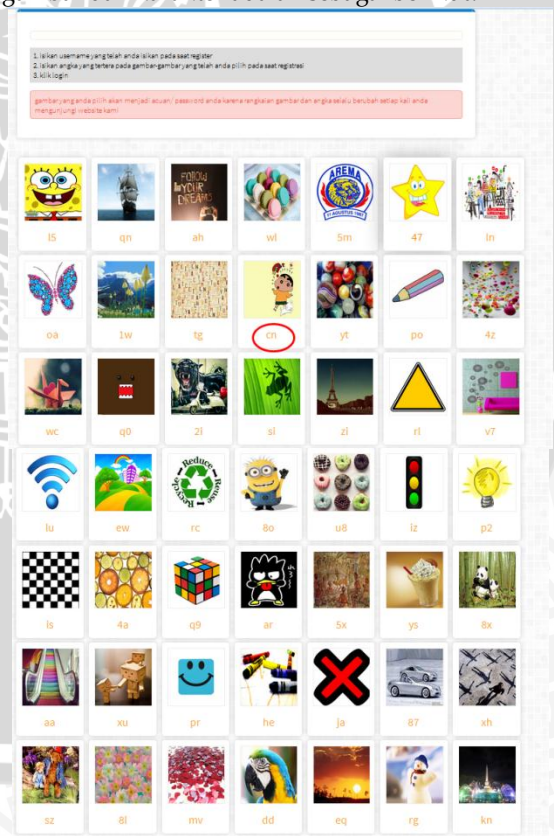
Pengujian dilakukan dengan dua tahap yaitu mencoba melakukan brute force terhadap sistem dengan menggunakan *software Fireforce* dan dengan menggunakan program buatan sendiri yang menggunakan CURL.

Pengujian dilakukan dengan mencoba melakukan *brute force* terhadap sistem dengan menggunakan *software Fireforce* sebanyak 20 kali. Penguji mengambil salah satu data pengguna yaitu pengguna yang mempunyai *username* bernama 'aredoes'. Pengguna 'aredoes' ini mempunyai *password* sebagai berikut:

Tabel 2. Password Pengguna 'aredoes'

Password urutan pertama	
Password urutan kedua	
Password urutan ketiga	

Saat melakukan proses brute force, susunan gambar dan karakter adalah sebagai berikut.



Gambar 15 Gambar *Printscreen* Halaman Login Saat Melakukan Proses Brute Force

Password yang ditemukan dari 20 kali pengujian adalah sebagai berikut:

Tabel 5.8 Tabel Daftar Hasil *Password* yang Ditemukan Melalui *Software Fireforce*

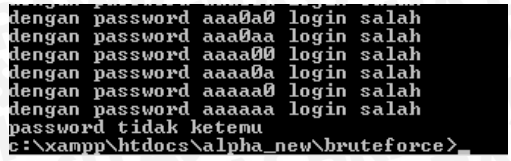
Pengujian ke-	Hasil
1	*Password found*: aaaaac
2	*Password found*: aaaaaf
3	*Password found*: aaaaab
4	*Password found*: aaaaaf
5	*Password found*: aaaaaf
6	*Password found*: aaaaaf
7	*Password found*: aaaaac
8	*Password found*: aaaaaf
9	*Password found*: aaaaab
10	*Password found*: aaaaac
11	*Password found*: aaaaab
12	*Password found*: aaaaae
13	*Password found*: aaaaae
14	*Password found*: aaaaaf
15	*Password found*: aaaaae
16	*Password found*: aaaaae
17	*Password found*: aaaaad
18	*Password found*: aaaaae
19	*Password found*: aaaaaf
20	*Password found*: aaaaaf

Dari dua puluh hasil proses pengujian, *password* yang ditemukan oleh *software fireforce* tidak berhasil membuka halaman dari pengguna 'aredoes'. Software ini tidak dapat menemukan password sebenarnya dari pengguna 'aredoes' yang bernilai 'cncncn'

Pengujian *brute force* menggunakan PHP Curl ini dibagi menjadi dua bagian yaitu:

1. Direct post *username* dan *password*

Direct post field username dan *password* ini merupakan hal yang dilakukan oleh program-program *brute force* pada umumnya, karena pada metode autentikasi web pada umumnya hanya menggunakan *username* dan *password* dalam proses autentikasinya. Hasil dari pengujian ini adalah password tidak ditemukan seperti gambar di bawah ini:



Gambar 16 Gambar *Printscreen* Hasil *Brute* Force dengan *Direct Post Field Username* dan *Password*

2. Direct post *username*, *password* dan *id session*

Direct post field username, password dan *id session* ini dilakukan karena pada metode autentikasi OTP berbasis gambar menggunakan tiga objek tersebut dalam proses autentikasinya. Hasil dari pengujian ini adalah password dapat ditemukan seperti gambar di bawah ini

Gambar 17 Gambar *Printscreen* Hasil *Brute* Force dengan *Direct Post Field Username*, *Password* dan *Id Session*

Hasil pengujian dengan menggunakan *direct post username* dan *password* menunjukkan bahwa *password* tidak dapat ditemukan. Kedua pengujian ini tidak dapat menemukan *password* sebenarnya dikarenakan variabel yang diinisialisasi adalah *username* dan *password* di mana pada metode OTP berbasis gambar ini terdapat satu variabel lagi yaitu *id session*. Sehingga pada pengujian dengan *direct post username, password* dan *id session* menghasilkan bahwa *password* dapat ditemukan. Dengan ini maka *password* dari pengguna dapat ditemukan dengan catatan sebagai berikut:

a. Penyerang mengetahui metode yang digunakan oleh OTP berbasis gambar ini yaitu dengan menambahkan satu variabel *id session*
b. Tidak memuat ulang halaman web ketika melakukan proses *brute force* karena *id session* akan selalu berubah sehingga *password* yang ditemukan tidak dapat digunakan.

User Acceptance Testing

UAT (*User Acceptance Testing*) digunakan untuk mengetahui apakah sistem yang dibangun telah dapat diterima atau belum oleh pengguna sistem. UAT difokuskan pada implementasi OTP yang terdapat pada proses *autentikasi*. UAT dilakukan dengan memberikan kuesioner kepada 25 mahasiswa PTIIK untuk menilai keseluruhan dan memberikan komentar maupun saran terhadap implementasi OTP tersebut.

Pertanyaan yang diajukan dapat dilihat pada tabel di bawah ini:

Tabel 3. Pertanyaan Kuesioner

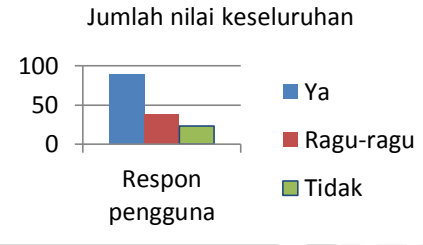
No	Pertanyaan
1	Apakah mengingat *password* dengan menggunakan One Time Password berbasis gambar lebih mudah diingat daripada *password* dengan menggunakan strong *password*?
2	Apakah meskipun anda tidak menggunakan aplikasi ini dalam jangka waktu yang cukup lama, anda akan tetap mengingat *password* anda?
3	Menurut anda, apakah sistem autentikasi menggunakan One Time Password mudah digunakan?
4	Menurut anda, apakah sistem autentikasi menggunakan One Time Password merupakan ide yang bagus?
5	Menurut anda, apakah tiga puluh enam gambar cukup untuk menjadi alternatif pilihan *password*?
6	Menurut anda, berapa gambar yang bisa dijadikan alternatif pilihan *password* untuk pengguna?
7	Apakah anda menyukai metode One Time Password berbasis gambar daripada metode *password* dengan menghafal karakter-karakter seperti biasanya?
8	Sebutkan alasan anda mengapa menyukai atau tidak menyukai metode One Time Password berbasis gambar ini?
9	Sebutkan alasan anda mengapa menyukai atau tidak menyukai metode One Time Password berbasis gambar ini?

Hasil penilaian terhadap jawaban dari responden dapat dilihat seperti di bawah ini,

Tabel 4. Jumlah Hasil Kuesioner

Pertanyaan Nomor ke-	Ya	Ragu-ragu	Tidak
1	16	4	5
2	8	14	3
3	16	4	5
4	18	4	3
7	16	5	4
9	15	7	3
Jumlah	89	38	23

Hasil rekapitulasi dalam bentuk grafik dapat dilihat di bawah ini. Bisa dilihat bahwa sebanyak 59,3 % pengguna merespon positif metode OTP berbasis gambar ini, sedangkan sisanya yaitu 40,7% belum dapat menerima atau merespon positif pada metode OTP berbasis gambar ini.



Gambar 18 Gambar Grafik Rekapitulasi Hasil Kuesioner

Selanjutnya terkait dengan jumlah pilihan gambar (pertanyaan nomor 5), sebanyak 13 responden menyatakan bahwa 36 gambar cukup untuk menjadi alternatif pilihan *password*, dan sebanyak 7 responden menyatakan bahwa tiga puluh enam gambar terlalu banyak untuk menjadi alternatif pilihan *password*, sisanya 5 responden menyatakan bahwa tiga puluh enam gambar terlalu sedikit.

Untuk pertanyaan "Menurut anda, berapa gambar yang bisa dijadikan alternatif pilihan *password* untuk pengguna?", dari 25 jawaban yang diberikan responden, kita ambil rata-rata yaitu sebesar 43 pilihan gambar. Namun dikondisikan dengan tata letak gambar pada halaman *website*, maka peneliti memutuskan untuk membulatkan ke bilangan kuadat terdekat yaitu sebesar 49 gambar agar dapat di posisikan tujuh gambar mendatar dan tujuh gambar menurun.

KESIMPULAN DAN SARAN

Berdasarkan hasil perancangan, implementasi dan pengujian yang dilakukan, maka diambil kesimpulan sebagai berikut :

1. OTP berbasis gambar belum 100% aman digunakan untuk metode autentikasi pada *website ecommerce* PTIIK
2. OTP berbasis gambar pada *website ecommerce* PTIIK diimplementasikan dengan menggunakan bahasa pemrograman PHP dengan *framework Code Igniter* dan basis data MySQL.
3. Dari tiga kali proses *login* yang dilakukan oleh pengguna yang sama, *password* yang diinputkan oleh pengguna berbeda-beda sehingga *password* sebenarnya tidak dapat diketahui melalui man in the middle

4. Berdasarkan hasil pengujian serangan *brute force* dengan menggunakan *software Fireforce* dan *direct post username dan password* dengan menggunakan PHP Curl tidak berhasil menemukan *password* sebenarnya dari pengguna karena variabel yang diinisialisasi adalah *username* dan *password* di mana pada metode OTP berbasis gambar ini terdapat satu variabel lagi yaitu *id session*. Sehingga pada pengujian dengan *direct post username, password* dan *id session* menghasilkan bahwa *password* dapat ditemukan.
5. *Password* dari pengguna dapat ditemukan dengan catatan penyerang mengetahui metode yang digunakan oleh OTP berbasis gambar ini yaitu dengan menambahkan satu variabel *id session* dan tidak memuat ulang *form login* ketika melakukan proses *brute force* karena *id session* akan selalu berubah sehingga *password* yang ditemukan tidak dapat digunakan.
6. Berdasarkan kuesioner yang telah disebarkan, rata-rata permintaan jumlah pilihan gambar oleh responden adalah sebanyak 43 gambar. Untuk itu, peneliti membulatkan ke bilangan kuadat terdekat yaitu sebesar 49 gambar agar dapat di posisikan tujuh gambar mendatar dan tujuh gambar menurun.
7. Dari hasil UAT, hasil yang kurang memuaskan terdapat pada pertanyaan "Apakah meskipun anda tidak menggunakan aplikasi ini dalam jangka waktu yang cukup lama, anda akan tetap mengingat password anda?". Hasil didapatkan sebanyak 52% responden ragu-ragu dapat mengingat password dengan metode OTP berbasis gambar ini dalam jangka waktu yang panjang. Hal ini disebabkan gambar kurang umum sehingga susah diingat.
8. Berdasarkan hasil analisis dari *user acceptance testing,* sebesar 65,3% pengguna merespon dengan baik metode OTP berbasis gambar ini karena mereka berpendapat bahwa metode ini merupakan inovasi yang menarik dan sesuatu yang berbentuk visual lebih mudah diingat dibandingkan dengan sesuatu yang bersifat teks atau numerik. Meskipun demikian perlu diperhatikan bahwa dalam pengimplementasian OTP berbasis gambar ini masih ada pengguna yang belum dapat menerima karena beberapa alasan, diantaranya *password* tiap gambar saat *login* selalu berubah sehingga user perlu melihat satu persatu, gambarnya kurang umum sehingga susah untuk diingat dan masih belum terbiasa

Saran yang dapat diberikan untuk pengembangan perangkat lunak ini antara lain :

1. Untuk pengembangan lebih lanjut, disarankan ditambahkan metode keamanan seperti *security question* atau memblokir IP dari sebuah komputer yang telah melakukan lima kali gagal *login* untuk menghindari serangan *brute force*
2. Dalam menindaklanjuti hasil *user acceptance testing*, disarankan untuk pengembangan lebih lanjut menggunakan gambar-gambar yang mudah diingat contohnya gambar yang bersifat homogen.
3. Untuk pengembangan lebih lanjut, disarankan metode ini tidak hanya digunakan pada *web based application* tetapi juga *desktop application* atau *mobile application.*

DAFTAR PUSTAKA

[1] http://www.rolo.org/brute-force-attack.html diakses tanggal 1 Desember 2013

[2] http://www.sciencedaily.com/releases/2011/05/110524104653.htm diakses tanggal 10 Januari 2013

[3] Shepard, Roger. 1967. *Recognition Memory for Words, Sentences, and Pictures*.

[4] Tyas, Zahra. 2010. *Implementasi E-commerce untuk Ozone Distro*

[5] http://www.rolo.org/brute-force-attack.html diakses tanggal 1 Desember 2013

[6] http://www.sciencedaily.com/releases/2011/05/110524104653.htm diakses tanggal 10 Januari 2013

[7] Shepard, Roger. 1967. *Recognition Memory for Words, Sentences, and Pictures*.

[8] Tyas, Zahra. 2010. *Implementasi E-commerce untuk Ozone Distro*

[9] http://www.rolo.org/brute-force-attack.html

diakses tanggal 1 Desember 2013
[10] http://www.sciencedaily.com/releases/2011/05/110524104653.htm diakses tanggal 10 Januari 2013
[11] Shepard, Roger. 1967. *Recognition Memory for Words, Sentences, and Pictures*.
[12] Tyas, Zahra. 2010. *Implementasi E-commerce untuk Ozone Distro*
[13] http://www.rolo.org/brute-force-attack.html diakses tanggal 1 Desember 2013
[14] http://www.sciencedaily.com/releases/2011/05/110524104653.htm diakses tanggal 10 Januari 2013
[15] Shepard, Roger. 1967. *Recognition Memory for Words, Sentences, and Pictures*.
[16] Tyas, Zahra. 2010. *Implementasi E-commerce untuk Ozone Distro*