KEAMANAN *LOGIN WEB* MENGGUNAKAN METODE 3DES BERBASIS TEKNOLOGI *QUICK RESPONSE CODE*

[1)]Heru Adya Gunawan, [2)]Zainal Arifin & [3)]Indah Fitri Astuti

[1,2,3)]Program Studi Ilmu Komputer, FMIPA, Universitas Mulawarman
Email : erudyaz@gmail.com[1)], zainal_arifin@fmipa.unmul.ac.id[2)], indahfitriastuti@fmipa.unmul.ac.id[3)]

ABSTRAK

Keamanan dalam menjaga kerahasiaan data merupakan aspek yang penting dari sebuah sistem informasi didalam *internet*. Mengingat masalah dalam mengamankan data, maka tidak akan lepas dari penggunaan sistem *login*. Saat *user* melakukan *login* pasti akan memasukkan data berupa *username* dan *password* dimana *password* itu bersifat privasi dan rahasia. Data *password* pengguna harus dapat dijaga keamanannya. Salah satu cara mengamankan *password* tersebut dengan menggunakan enkripsi.

Penggunaan enkripsi 3DES dikombinasikan dengan teknologi *Quick Response code* dinilai praktis dan dapat memberi solusi pada masalah tersebut. *User* tidak perlu melakukan *login* berulang kali ke suatu *website* yang sama. *Username* dan *password* milik *user* disimpan dalam *database*. Saat *user* melakukan *login*, maka aplikasi otomatis mengisi *form web* dengan *username* dan *password* yang tersimpan tersebut tanpa perlu menuliskan kembali data pada setiap *web*. Hasil akhir dari penelitian ini berupa aplikasi yang dapat melakukan *login* dengan data yang telah terenkripsi sehingga kerahasiaan data tersebut dapat terjaga.

Kata kunci : Keamanan, *Login*, 3DES, *Quick Response code*.

PENDAHULUAN

Dalam sebuah sistem informasi masalah keamanan dan menjaga kerahasiaan data merupakan salah satu aspek yang penting. Namun masalah keamanan ini sering kali kurang mendapat perhatian dari pihak pemilik dan pengelola sistem informasi. Masalah keamanan berada di urutan kedua atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu kinerja sistem, seringkali keamanan dikurangi atau ditiadakan. Jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka sulit memisahkannya dengan proses *login*. *Login* bertujuan untuk memberikan layanan keamanan pada sistem.[1]

Saat melakukan *login* pengguna akan memasukkan *password* dimana *password* tersebut bersifat privasi dan rahasia. Oleh karena itu, masalah keamanan menjadi masalah yang sangat penting mengingat internet merupakan jaringan publik yang saling terhubung dalam suatu jaringan dan akan sangat berbahaya jika *password* yang dimasukkan *user* tersebut tidak dienkripsi sebelum dikirim ke *server* melalui jaringan.[2]

3DES (*Triple Data Encryption Standard*) merupakan salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan data dengan cara menyandikan data. Proses yang dilakukan dalam penyandian datanya yaitu proses enkripsi dan dekripsi. Algoritma 3DES merupakan algoritma pengembangan dari algoritma DES (*Data Encryption Standard*). Perbedaan DES dengan 3DES terletak pada panjangnya kunci yang digunakan. Pada DES menggunakan satu kunci yang panjangnya 56-bit sedangkan pada 3DES menggunakan tiga kunci yang panjangnya 168-bit (masing-masing panjangnya 56-bit). Pada 3DES, tiga kunci yang digunakan bisa bersifat saling bebas ($K1 \neq K2 \neq K3$) dan hanya dua buah kunci yang saling bebas dan satu kunci lainnya sama dengan kunci pertama ($K1 \neq K2$ dan $K3 = K1$) ataupun hanya menggunakan satu buah kunci yang sama ($K1 = K2 = K3$). Karena tingkat kerahasiaan algoritma 3DES terletak pada panjangnya kunci yang digunakan, maka penggunaan algoritma 3DES dianggap lebih aman dibandingkan dengan algoritma DES.[3]

QR Code (*Quick Response Code*) merupakan wujud *barcode* dua dimensi yang memiliki kemampuan menyimpan informasi berupa teks atau string. Penggunaan QR Code untuk menyimpan informasi penting belakangan ini semakin marak dan awam. Penggunaan QR Code sudah sangat lazim di Jepang. Hal ini dikarenakan kemampuannya menyimpan data yang lebih besar dari pada kode batang sehingga mampu mengkodekan informasi dalam bahasa Jepang sebab dapat menampung huruf kanji.

Awalnya QR Code digunakan untuk pelacakan kendaraan bagian di manufaktur, namun kini QR Code digunakan dalam konteks yang lebih luas termasuk aplikasi komersial dan kemudahan

pelacakan aplikasi berorientasi yang ditujukan untuk pengguna telepon seluler. Di Jepang penggunaan QR Code sangat popular. Hampir semua jenis ponsel di Jepang bisa membaca QR Code sebab sebagian besar pengusaha disana telah memilih QR Code sebagai alat tambahan dalam program promosi produknya baik yang bergerak dalam perdagangan maupun dalam bidang jasa. Pada umumnya QR Code digunakan untuk menanamkan informasi alamat situs suatu perusahaan.

TINJAUAN PUSTAKA

Keamanan

Bagi sebuah institusi atau pengguna lainnya sarana komunikasi data elektronis memunculkan masalah baru, yaitu keamanan. Pada zaman yang serba canggih ini, sistem autentikasi konvensional dengan KTP, SIM, dan yang lainnya yang berstandar pada keunikan tanda tangan tidak berlaku untuk komunikasi elektronis. Komunikasi data elektronis memerlukan perangkat keamanan yang benar-benar berbeda dengan komunikasi konvensional.

Login

Login atau juga biasa disebut *log in, log on, sign on, signin, sign in* adalah proses untuk mengakses komputer dengan memasukkan identitas dari akun pengguna dan kata sandi untuk mendapatkan hak akses menggunakan sumber daya komputer tujuan.

Triple Data Encryption Standard

3DES (*Triple Data Encryption Standard*) merupakan suatu algoritma simetris pada kriptografi yang digunakan untuk mengamankan data dengan cara menyandikan data. Algoritma 3DES adalah suatu algoritma pengembangan dari algoritma DES (*Data Encryption Standard*). Pada dasarnya algoritma yang digunakan sama, hanya pada 3DES dikembangkan dengan melakukan enkripsi dengan implementasi algoritma DES sebanyak tiga kali. 3DES memiliki tiga buah kunci yang berukuran 168-bit (tiga kali kunci 56-bit dari DES).Pada algoritma 3DES dibagi menjadi tiga tahap, setiap tahapnya merupakan implementasi dari algoritma DES. Secara umum 3DES dirumuskan sebagai berikut:

Enkripsi : $C = K_3(K_2(K_1(P)))$
Dekripsi : $P = K_1(K_2(K_3(C)))$

Keterangan:
P = *plaintext*
C = *ciphertext*

Varian di atas umumnya disebut dengan mode EEE (dikarenakan menggunakan tiga kali proses enkripsi). Namun, kemudian dilakukan sebuah penyederhanaan terhadap varian tersebut sehingga melahirkan mode baru yang disebut sebagai EDE (enkripsi - dekripsi- enkripsi), dengan adanya penyisipan fungsi dekripsi. Penggunaan tiga kali DES pada 3DES diharapkan dapat meningkatkan keamanan dikarenakan juga adanya penggunaan kunci yang lebih panjang yaitu kunci dengan ukuran 168 bit (tiga kali ukuran DES, 56 bit). Pada penggunaan triple DES dengan mode EDE dapat dilakukan dengan menggunakan 3 kunci, 2 kunci ataupun hanya menggunakan 1 kunci. Penggunaan triple DES dengan 1 kunci merupakan bentuk penyederhanaan yang menggunakan kunci K = K1 = K2 = K3.

Tahap pertama, plainteks yang diinputkan dioperasikan dengan kunci eksternal pertama (K1) dan melakukan proses enkripsi dengan menggunakan algoritma DES sehingga menghasilkan pra-cipherteks pertama. Tahap kedua, pra-cipherteks pertama yang dihasilkan pada tahap pertama, kemudian dioperasikan dengan kunci eksternal kedua (K2) dan melakukan proses enkripsi atau proses dekripsi (tergantung cara pengenkripsian yang digunakan) dengan menggunakan algoritma DES sehingga menghasilkan pra-cipherteks kedua. Tahap terakhir, pra-cipherteks kedua yang dihasilkan pada tahap kedua, dioperasikan dengan kunci eksternal ketiga (K3) dan melakukan proses enkripsi dengan menggunakan algoritma DES, sehingga menghasilkan cipherteks (C).[3]

Quick Response Code

Quick Response code (QR code) adalah suatu jenis kode matriks atau kode batang dua dimensi yang dikembangkan oleh Denso Wave, sebuah divisi Denso Corporation yang merupakan sebuah perusahaan Jepang dan dipublikasikan pada tahun 1994. QR merupakan singkatan dari *quick response* atau respons cepat, yang sesuai dengan tujuannya untuk menyampaikan informasi dengan cepat dan mendapatkan respons yang cepat pula. Berbeda dengan kode batang atau *barcode* yang hanya menyimpan informasi secara horizontal, *Quick Response code* mampu menyimpan informasi secara horizontal dan vertikal. Oleh karena itu secara otomatis *Quick Response code* dapat menampung informasi yang lebih banyak daripada kode batang atu *barcode*.

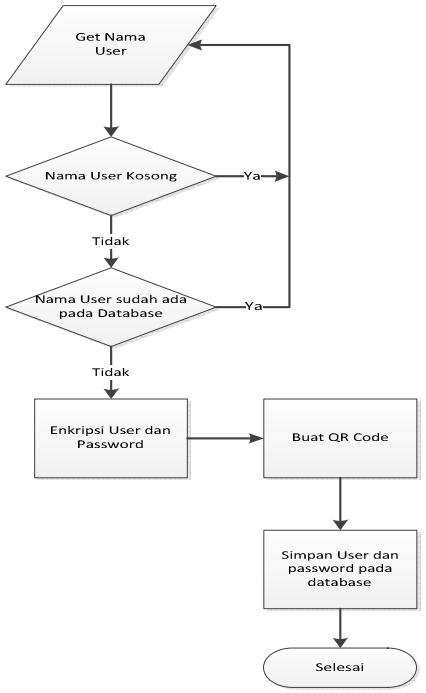
Quick Response Code Library

Library ini berfungsi untuk melakukan *encode* dan *decode* pada gambar QR-code. *Library* ini memiliki *support* terhadap reed-solomon *error correction code* pada QR-code, sehingga dapat

membaca QR-code yang rusak sekalipun dengan catatan QR-code tersebut harus sudah mengandung modul *error correction*. Selain itu, *library* ini akan melakukan *pre-processing* seperti *noise reduction* pada gambar terlebih dahulu sebelum melakukan *decode*.

HASIL DAN PEMBAHASAN

Pada tahap pendaftaran profil *user*, setelah aplikasi mendapatkan nama profil dan password yang di-*input*-kan *user* aplikasi akan meng-*generate* sebuah *Quick Response Code* terenkripsi dengan isi teks nama profil *user* dan *password* sesuai dengan yang didaftarkan. Nama profil *user* dan *password* akan disimpan ke dalam *database*. Sebelum proses penyimpanan, aplikasi melakukan pengecekan agar tidak ada *user* yang mendaftarkan dua profil dengan nama yang sama. Skema tahap pendaftaran profil *user* dapat dilihat pada Gambar 1.



Gambar 1. Diagram Alir Pendaftaran Profil *User*

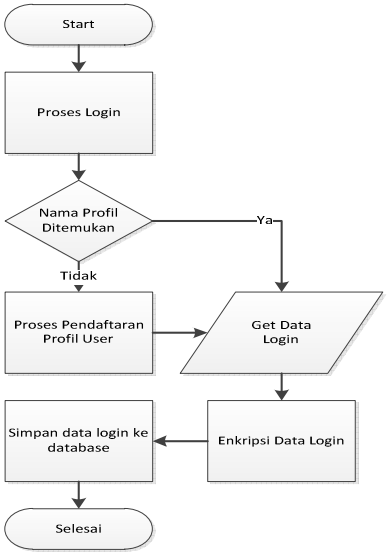
Proses Pendaftaran Data Login

Pada tahap ini, aplikasi akan menyimpan data *login* situs *web* yang di-*input*-kan ke dalam *database* sesuai dengan nama profil *user* data milik *user.* Apabila nama profil *user* data belum ada, aplikasi akan mengalihkan ke tahapan pendaftaran profil *user*. Skema tahap peng-*input*-an data *login* dapat dilihat pada gambar 2.

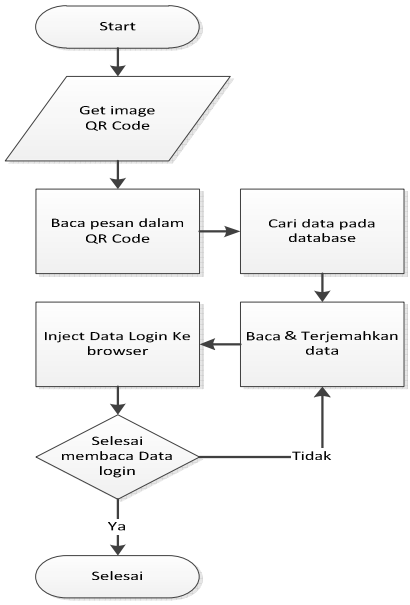
Proses Login Menggunakan *Quick Response Code*

Pada proses *login* menggunakan *Quick Response Code*, aplikasi akan menangkap data *Quick Response Code* dengan cara *drag* dan *drop*. Selanjutnya aplikasi akan melakukan *decode* gambar *Quick Response Code* tersebut untuk mendapatkan isi teks yang terkandung di dalamnya.

Isi teks yang didapatkan dari *Quick Response Code* adalah *encrypted* teks. Enkripsi yang digunakan adalah enkripsi *Triple Data Encryption Standard* (3DES). Kemudian aplikasi akan membuka *database* dengan data *user* sesuai dengan isi teks yang ada di dalam *Quick Response Code*. Apabila telah ditemukan data tersebut aplikasi akan membuka dan membaca isi data. Skema Proses *Login* Menggunakan *Quick Response Code* dapat dilihat pada gambar 3.



Gambar 2. Diagram Alir Penginputan Data *Login*



Gambar 3. Diagram Alir Proses *Login* Menggunakan *Quick Response Code*

PENGUJIAN SISTEM

Untuk mengetahui sistem telah bekerja dengan baik, maka perlu dilakukan pengujian terhadap sistem. Perangkat lunak diuji coba dari segi fungsionalitas dengan berbagai macam skenario. Pengujian ini merupakan implementasi dari perancangan perangkat lunak. Pengujian ini meliputi uji coba fungsionalitas serta analisa dari hasil uji coba yang dilakukan.

Pengujian pembuatan profil baru

Pengujian pembuatan profil baru dapat dilihat pada tabel 1.

Tabel 1. Pengujian Membuat Profil Baru

Data Uji	Hasil Yang Diharapkan	Hasil Nyata	Hasil
Nama profil yang di-*input*-kan benar.	Profil terdaftar dengan sukses.	Profil terdaftar dengan *password* yang terenkripsi dan QR code.	OK
User mendaftarkan nama profil yang sama dengan profil yang sudah terdaftar.	Pendaftaran profil gagal, Muncul peringatan.	Muncul peringatan bahwa nama profil telah digunakan. *User* diminta meng-*input*-kan nama lain.	OK
User tidak meng-input-kan nama profil, lalu menekan tombol daftar pada form pendaftaran profil.	Pendaftaran profil gagal, muncul peringatan.	Muncul peringatan untuk meng-*input*-kan nama profil.	OK

Pengujian memasukkan data *login* situs *web*

Tabel 2. Tabel pengujian memasukkan data *login* situs *web*

Data Uji	Hasil Yang Diharapkan	Hasil Nyata	Hasil
User memasukkan *username* dan *password* sesuai akun yang dimiliki pada situs *web* tersebut dan menekan tombol simpan.	Data *login* terdaftar	Data *login* tersimpan dalam *database* sesuai nama profil.	OK
User tidak meng-*input*-kan salah satu dari *username* atau *password*.	Pendaftaran data *login* gagal	Muncul peringatan bahwa nama data *login* tidak tersimpan. User diminta mengisi dengan lengkap	OK

Pengujian *login* dengan *Quick Response code*

Tabel 3. Tabel Pengujian *Login* Dengan *Quick Response Code*

Data Uji	Hasil Yang Diharapkan	Hasil Nyata	Hasil
Gambar QR code	*Login* berhasil.	Aplikasi berhasil melakukan *login*. Situs *web* tujuan terbuka pada halaman *browser*	OK

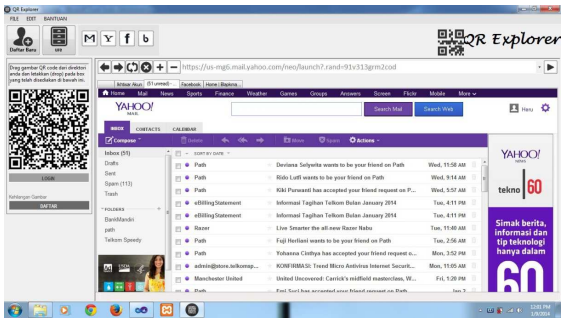
Pengujian *login* ke halaman *web*

Pengujian *login* ke halaman *web* dilakukan menggunakan *browser* yang tersedia pada aplikasi. Koneksi internet yang digunakan adalah koneksi langsung. Untuk membuktikan hasil uji coba *login* pada halaman *web*, penulis menyertakan *screenshot* hasil uji coba. Pengujian *login* ke halaman yahoo.com dapat dilihat pada Tabel 4.

Tabel 4. Tabel Pengujian *Login* Ke Halaman Yahoo.com

Data Uji	Hasil Yang Diharapkan	Hasil Nyata	Hasil
Yahoo.com	*Login* berhasil.	User berhasil *login* ke halaman yahoo.com	OK

Uji coba pertama adalah *login* ke halaman yahoo.com. Dari *screenshot* yang ditampilkan dapat dilihat bahwa aplikasi berhasil melakukan *login* ke halaman yahoo.com. *Screenshot* hasil uji coba *login* ke yahoo.com dapat dilihat pada Gambar 4.



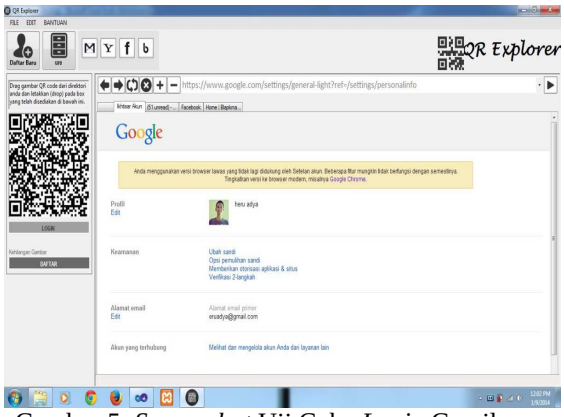
Gambar 4. *Screenshot* Uji Coba *Login* Yahoo.com

Pengujian *login* ke halaman gmail.com dapat dilihat pada Tabel 5.

Tabel 5. Tabel Pengujian *Login* Ke Halaman Gmail.com

Data Uji	Hasil Yang Diharapkan	Hasil Nyata	Hasil
gmail.com	*Login* berhasil.	User berhasil *login* ke halaman gmail.com	OK

Uji coba kedua adalah *login* ke halaman gmail.com. Dari *screenshot* yang ditampilkan dapat dilihat bahwa aplikasi berhasil melakukan *login* ke halaman gmail.com. *Screenshot* hasil uji coba *login* ke gmail.com dapat dilihat pada Gambar 5.



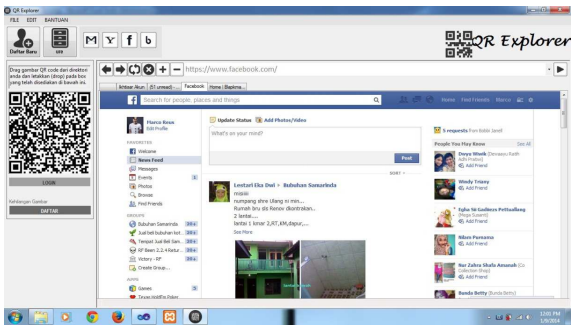
Gambar 5. *Screenshot* Uji Coba *Login* Gmail.com

Pengujian login ke halaman facebook.com dapat dilihat pada Tabel 6.

Tabel 6. Tabel Pengujian *Login* Ke Halaman Facebook.com

Data Uji	Hasil Yang Diharapkan	Hasil Nyata	Hasil
facebook.com	Login berhasil.	User berhasil login ke halaman facebook.com	OK

Uji coba ketiga adalah *login* ke halaman facebook.com. Dari *screenshot* yang ditampilkan dapat dilihat bahwa aplikasi berhasil melakukan *login* ke halaman facebook.com. *Screenshot* hasil uji coba *login* ke facebook.com dapat dilihat pada Gambar 6.



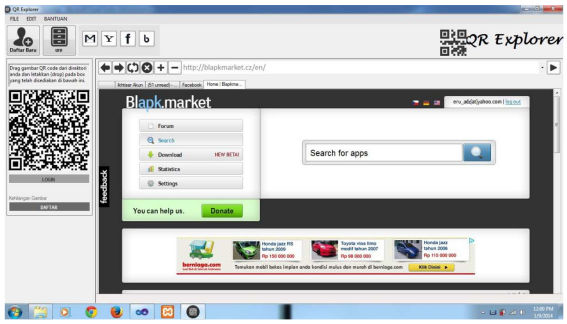
Gambar 6. *Screenshot* Uji Coba *Login* Facebook.com

Pengujian login ke halaman blapkmarket.cz dapat dilihat pada Tabel 7.

Tabel 7. Tabel Pengujian *Login* Ke Halaman Blapkmarket.cz

Data Uji	Hasil Yang Diharapkan	Hasil Nyata	Hasil
Blapkmarket.cz	*Login* berhasil.	*User* berhasil *login* ke halaman blapkmarket.cz	OK

Uji coba selanjutnya adalah *login* ke halaman blapkmarket.cz. Dari *screenshot* yang ditampilkan dapat dilihat bahwa aplikasi berhasil melakukan *login* ke halaman blapkmarket.cz. *Screenshot* hasil uji coba *login* ke blapkmarket.cz dapat dilihat pada Gambar 7.



Gambar 7. *Screenshot* Uji Coba *Login* Blapkmarket.cz

KESIMPULAN

Kesimpulan yang dapat diambil berdasarkan penelitian mengenai keamanan *login web* menggunakan metode 3DES berbasi teknologi Quick Response code yaitu metode *3DES* yang merupakan metode penyandian file teks dapat melakukan enkripsi dan dekripsi dan aplikasi dapat melakukan *encode* dan *decode* Quick Response code dengan bantuan *library* MessagingToolkit.

DAFTAR PUSTAKA

[1] Rahardjo B. 1999. *Keamanan Sistem Informasi Berbasis Internet*.PT Insan Komunikasi. Bandung

[2] Marisa. D. 2011. *Analisis Keamanan Sistem Login*. Jurnal Informatika Mulawarman. Volume 6, No.2 P : 64-65

[3] Hidayat. A. 2009. *Enkripsi Dan Dekripsi Data Dengan Algoritma 3 DES (Triple Data Encryption Standard).* Jurnal Matematika Universitas Padjadjaran.