JURNAL INFOTEL
Informatika - Telekomunikasi - Elektronika

Website Jurnal : http://ejournal.st3telkom.ac.id/index.php/infotel
ISSN : 2085-3688; e-ISSN : 2460-0997

Implementasi Protokol *Single Sign On* (SSO) Menggunakan *Face Recognition*

Hasan Isfahani[1], Dhidik Prastiyanto[2], Sugeng Purbawanto[3]
[1,2,3] Pendidikan Teknik Informatika dan Komputer, Fakultas Teknik, Universitas Negeri Semarang
[1,2,3]Kampus Sekaran, Gunungpati, Semarang 50229 Indonesia
Email korespondensi: hasan@students.unnes.ac.id

Dikirim 2 Mei 2017, Direvisi 8 Juli 2017, Diterima 29 Juli 2017

Abstrak – Akun (*user*) merupakan kunci dari segala sistem untuk bisa mengakses sistem tersebut. Sekarang setiap orang memiliki banyak akun dari sistem yang berbeda-beda. Semua akun tersebut harus diingat untuk bisa mengakses sistem. Untuk mengatasi hal seperti ini diperlukan perangkat pengelolaan akun yang terpusat, yaitu menggunakan protokol *Single Sign On* (SSO). Dalam penelitian ini menggunakan metode pengembangan sistem *linier sequential model*. Metode pengembangan sistem *linier sequential model* melalui empat tahapan proses, yaitu analisis, desain, pengkodean, dan pengujain. Pengujian yang dilakukan di antaranya pengujian *blackbox*, *performance testing*, *efficiency*, *portability*, *usability*, pengujian algoritma *Eigenface* untuk *face recognition*, dan pengujian *multi login* sistem. Hasil penelitian berupa tahapan-tahapan pengembangan sistem dengan hasil pengujian *blackbox*, yaitu seluruh fungsi sistem berjalan dengan baik. Pada pengujian *performance testing* menunjukkan kinerja sistem sangat baik. Pada pengujian *efficiency* menghasilkan nilai di atas rata-rata *GTMetrix*. Pada pengujian aspek *portability* menunjukkan sistem bisa diakses di 3 *browser*. Pada pengujian *usability* menunjukkan sistem layak digunakan. Dari pengujian algoritma *Eigenface* menunjukkan proses verifikasi wajah berjalan lancar tanpa terkendala. Dapat mengakses sistem dengan *login* melalui sistem yang berbeda menunjukkan uji *multi login* sistem berhasil. Simpulan yang dapat diambil dari penelitian ini adalah sistem *login SSO* dapat mempermudah pengelolaan akun untuk admin dan pengguna. Sistem *login* SSO layak diterapkan dengan menggunakan autentifikasi *face recognition*. Saran untuk pengembangan sistem lebih lanjut, yaitu diperlukan penambahan fungsi enkripsi dan pembangunan *dedicated server* sendiri untuk *face recognition*.

Kata kunci – akun, *login*, *Single Sign On* (SSO), *biometric*, *face recognition*

Abstract - Account is the key of every system in order to access the system. Nowadays, every people has some different account systems. All of these accounts must be remembered, so that they could access the system. Facing this issue, the management account devices which is centralized by using Single Sign On (SSO) protocol is needed. This research was using sequential linear system development models. The sequential linear system development through four stages, analysis, design, coding, and testing. Some tests were also performed such as blackbox test, performance test, efficiency, portability, usability, eigenface algorithm test, and multi login test. The result of the research were the stages of the system development with blackbox test of system functions were running well. Performance test shown the excellence of system performance. Efficiency test has a result above-average GTMetrix. Portability aspect test shown that system could being accessed in three browsers. Usability test shown that the process of face verification is going well without any mistakes. Accessing the system by login through some different system implied that multi login system test is successful. The conclusion could be implied from this research is SSO login system could simplify the management account for administrators and users. SSO login system needs to be applied by using face authentication recognition. Some advices for further system development are the additional function of encryption and the establishment of dedicated server for face recognition.

Keywords – account, login, Single Sign On, biometric, face recognition

I. PENDAHULUAN

Melihat perkembangan sistem atau aplikasi yang semakin banyak digunakan oleh manusia pada saat ini, menjadikan seseorang harus menghafal setiap akun dari setiap sistem yang dimiliki. Setiap sistem tersebut juga harus memiliki layanan yang aman untuk digunakan sekelompok komunitas atau perseorangan. Untuk mencapai hal ini, sistem harus menyediakan autentikasi dan otorisasi. Autentikasi *user* merupakan tugas yang sangat penting dalam layanan jaringan terdistribusi [1]. Biasanya, pengguna memiliki akun untuk setiap sistem yang dimiliki. Untuk mendapatkan akses ke sistem, seorang pengguna harus *login* dengan memasukkan *user* dan *password* yang mereka miliki. Dengan sistem yang heterogen semua pengguna harus memiliki *password* untuk setiap sistem dan *login* secara terpisah, ini bukan situasi yang ideal.

Solusi untuk masalah ini adalah *Single Sign On* (SSO) [2] Dengan *Single Sign On* pengguna hanya perlu *login* sekali dengan satu akun untuk seluruh sistem yang dimiliki. Namun masalah utama di SSO adalah *credential* yang digunakan untuk autentikasi biasanya menggunakan *credential* berbasis teks seperti *user* dan *password*. *Credential* berbasis teks dapat dengan mudah dicuri oleh orang yang tidak bertanggung jawab, sehingga ketika berhasil dicuri, penyerang dapat memperoleh akses ke banyak sistem hanya dengan satu proses autentikasi. Untuk mencegah hal ini pengguna perlu menerapkan *credential* yang unik. *Credential* unik yang sulit untuk dicuri adalah *biometric* [3]. Jadi *biometric* dapat dijadikan *credential* yang unik untuk sistem yang ada.

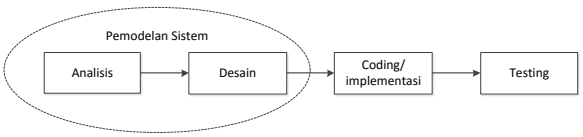
Ada 4 Autentikasi *Biometric* yaitu Finger print scans, Iris scan, Voice recognition, Facial recognition[4][5]. Setiap autentikasi *biometric* memiliki keunikan masing-masing serta kelebihan dan kekurangannya. Tampaknya tidak ada yang akan menjadi salah satu autentikasi *biometric* yang terbaik untuk memastikan autentikasi yang aman. Setiap metode yang berbeda dari autentikasi *biometric* memiliki keunggulannya masing-masing. Beberapa kurang invasif, beberapa bisa dilakukan tanpa pengetahuan tentang subjek, beberapa sangat sulit untuk dipalsukan.

Penelitian yang dilakukan oleh Patrick Telnoni yaitu mengembangkan protokol SSO menggunakan kombinasi *speech* dan *speaker recognition* [5][6][7] sedangkan dalam penelitian ini menggunakan autentikasi *Face Recognition*. Alasan penggunaan *Face Recognition* sebagai autentikasi karena belum diketemukan penelitian atau aplikasi yang memadukan antara SSO dengan autentikasi *biometric Face Recognition*. Selain itu wajah merupakan unsur yang unik dari seorang manusia, tidak ada yang menyamai walaupun itu kembar identik sekalipun [8][9][10] dan perangkat yang dibutuhkan (*webcam*) juga terjangkau, sudah tersedia di setiap laptop. Berdasarkan latar belakang masalah yang telah dijelaskan, maka perlu untuk dilakukan penelitian terhadap penggunaan protokol SSO menggunakan autentikasi *Face Recognition* dengan judul "Implementasi Protokol *Single Sign On* (SSO) Menggunakan *Face Recognition*".

Rumusan masalah dalam penelitian ini adalah bagaimana mengelola dan mengakses seluruh sistem yang dimiliki dengan satu akun menggunakan protokol SSO dan bagaimana kelayakan fungsi *login* dengan protokol SSO dan Autentikasi *Face Recognition*. Sedangkan tujuan yang ingin dicapai dari penelitian ini adalah merealisasikan kemudahan mengelola dan mengakses seluruh sistem yang dimiliki dengan satu akun menggunakan protokol SSO dan Mengetahui kelayakan fungsi *login* dengan protokol SSO dan Autentikasi *Face Recognition*.

II. METODE PENELITIAN

Metode yang digunakan adalah sistem linier sequential model melalui empat tahapan proses yaitu analisis, desain, pengkodean dan pengujian [11][12]. Pengujian yang dilakukan diantaranya pengujian *blackbox*, *performance testing*, *efficiency*, *portability*, *usability*, pengujian Algoritma *Eigenface* untuk *Face Recognition*, dan pengujian Multi *login* sistem serta *debugging*.



Gambar 1. Alur Metode Pengembangan Software Waterfall

Penelitian ini dilakukan menggunakan metode pengumpulan data observasi dan angket dengan mengamati sistem *login* yang digunakan di KPRI Handayani Semarang. Desain aplikasi yang dibuat terdiri dari UML[7], Basis Data dan Interface. Desain UML terdiri dari *Usecase* Diagram, Activity Diagram, *Class* Diagram dan Sequence Diagram. Dari hasil pengidentifikasian aktor dan *usecase* maka dibuatlah *usecase* diagram yang terdiri dari 2 aktkor dan 6 *usecase*. Aktor yang digunakan untuk identifikasi *usecase* yaitu pengguna sistem lama dan pengguna sistem baru. *Usecase* yang diiedentifikasi antara lain *Login*, *Authenticate User*, *Check Validity*, *Save Info at Server Side*, *Register New Account* dan *Register face*.

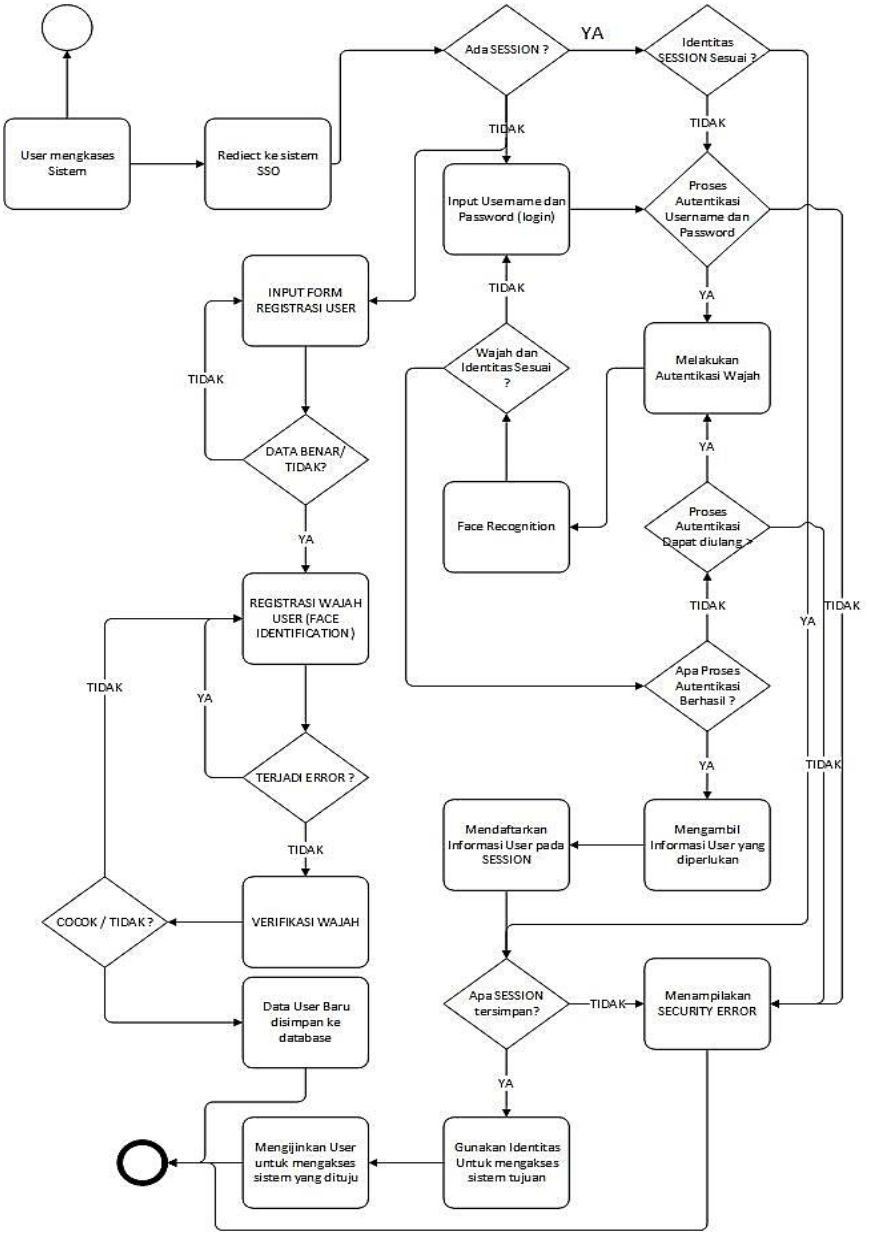
Diagram aktifitas yang ditujukan pada Gambar 2 menggambarkan proses *login* dan registrasi *user* baru yang dibuat berdasarkan *usecase* diagram. aktifitas dimulai ketika *user* ingin memasuki sistem dengan cara *login* terlebih dahulu.

User mengakses sistem yang akan dituju, sistem akan meredirect ke halaman *login* sistem SSO untuk melakukan *login*. Jika *browser* masih menyimpan session *login* maka identitas dari session tersebut akan dicocokkan dengan identitas use di *database* jika sesuai, identitas *user* tersebut dapat digunakan untuk mengakses sistem langsung.

Jika tidak ada session yang tersimpan dalam *browser* maka *user* harus memilih untuk melakukan *login* atau mendaftarkan akun baru jika belum memiliki akun. Ketika *user* memilih untuk *login* dia harus memasukkan *user*name dan *password* dalam form *login*, kemudian data *login* akan diautentikasi oleh sistem. Dalam proses autentikasi jika data *login* yang dimasukkan sesuai dengan *database* maka akan dilanjutkan proses autentikasi wajah namun jika salah maka akan muncul peringatan kesalahan *login*.

Proses autentikasi selanjutnya yaitu *Face Recognition*. Dalam proses autentikasi wajah, peragkat kamera (*webcame*) akan memotret wajah *user* yang kemudian gambar yang dihasilkan akan dicocokkan (*Face Recognition*) oleh sistem dengan *database*. Ketika wajah yang diidentifikasi sesuai dengan *database* selanjutnya informasi *user* akan disimpan ke-session dan *user* dapat mengakses sistem yang dia tuju.

Pada saat *user* belum memiliki akun maka untuk mengakses sistem dia harus mendaftarkan akun baru. Dalam *Activity Diagram* proses registrasi dimulai dengan memasukkan infromasi *user* yang diperlukkan (biodata diri ditambah dengan *user*name dan *password* yang diinginkan), kemudian jika seluruh *form* yang wajib diisi (*required*) sudah sesuai dengan *rule form* maka akan dilanjutkan dengan proses identifikasi wajah. Proses mendaftarkan wajah *user* terjadi dua proses yaitu setelah wajah berhasil diidentifikasi kemudian dilakukan verifikasi, untuk memastikan kecocokan wajah yang sudah dimasukkan ke dalam *database*. Jika verifikasi gagal proses mendaftarkan wajah akan diulangi lagi, jika berhasil maka data akan disimpan ke dalam *database* dan proses registrasi selesai.

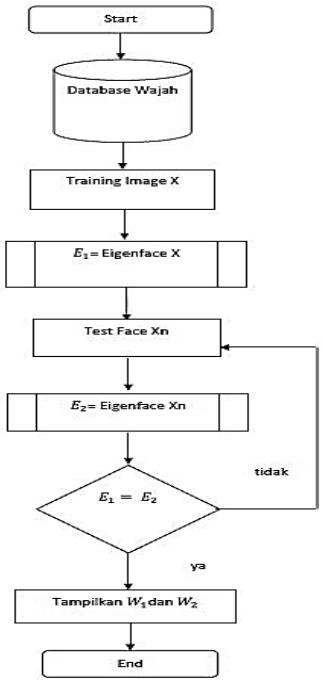


Gambar 2. *Activity Diagram* Proses *Login* dan Registrasi User

Sistem *login* SSO terdiri dari tiga *class* yang membentuk sistem *login* SSO yaitu *User*, SSO, dan *Face Recognition*. Pada tahap perancangan *database* yaitu dengan desain rancangan *database* RDMS (Relational *Database* Management System) pada sistem SSO dihasilkan lima tabel yang digunakan dalam sistem SSO yaitu *User*, *SSO*, *Face*, *Application* dan *Log*.

Dari hasil *usecase* diagram, activity diagram, serta sequence diagram dapat dibuat perancangan desain interface untuk mempermudah dalam pengkodean program. Ada 3 rancangan *interface* yaitu interface *login*, *interface Face Recognition* dan interface management *user*. Setelah proses desain dilaksanakan, maka tahap selanjutnya adalah pengkodean. Proses pengkodean adalah proses penerjemahan kode dari desain perangkat lunak yang telah dibuat sebelumnya. Proses pengkodean dalam penelitian ini menggunakan metode Pemrograman Berorientasi Objek (PBO). PBO merupakan sebuah metode yang digunakan dalam pemrograman yang disusun dari sekumpulan objek dan *class* sehingga objek dan *class* dapat dimanfaatkan kembali kapanpun programmer membutuhkan. Sedangkan Algoritma yang digunakan adalah algoritma *Eigenface* yang diterapkan dalam pengkodean *Face Recognition*.

Algoritma *Eigenface* merupakan algoritma yang digunakan sebagai autentikasi *Face Recognition* [9]. Prinsip dasar dari pengenalan wajah adalah mengutip informasi unik wajah lalu di-encode dan dibandingkan dengan hasil decode yang sebelumnya dilakukan. Dalam metode *Eigenface*, decoding dilakukan dengan menghitung eigenvector lalu direpresentasikan dalam sebuah matriks yang berukuran besar. Gambar 3 merupakan alur proses berjalannya algoritma *Eigenface*.



Gambar 3. Alur proses Algoritma *Eigenface*

Dari gambar alur kerja Algoritma *Eigenface* pada gambar 3 dapat diketahui proses pengenalan wajah dari Algoritma *Eigenface*. Tahap pertama menyiapkan data dari gambar yang sudah berupa matriks dibuat menjadi himpunan S yang terdiri dari seluruh training image dengan persamaan berikut.

$$S = \Gamma 1, \Gamma 2, \dots, \Gamma M \tag{1}$$

Setelah itu ambil nilai tengah (*mean*) dari himpunan matriks tersebut dengan persamaan berikut. *Ψ = Mean, M = Jumlah Image, Γ = Matriks (training image).*

$$\Psi = \frac{1}{M}\sum_{n=1}^{M} \Gamma_n \tag{2}$$

Selanjutnya dicari selisih antara training image denga nilai tengan (mean), apabila dihasilkan nilai dibawah nol maka diganti nilainya dengan nol, berikut persamaanya.(*Φ = Selisih, Γi = Matriks (training image), Ψ = Mean*).

$$\phi_i = \Gamma_i - \Psi \tag{3}$$

Langkah selanjutnya dihitung nilai matriks kovariannya (C) dengan persamaan:

$$\begin{aligned} C &= \frac{1}{M}\sum_{n=1}^{M} \phi_n \phi_n^T = AA^T \\ A &= \{\phi_1, \phi_2, \phi_3, \dots, \phi_n\} \\ L &= A^T A \end{aligned} \tag{4}$$

(*C = Matriks Kovarian, A = Himpunan selisih Matriks dan Mean, L = Invers Matriks Kovarian*). Pada tahap Test Face X_n akan dihitung nilai *eigenvalue* (λ) dan *eigenvector* (v).

$$CV_i = \lambda_i v_i \tag{5}$$

Setelah *eigenvector* (v) diperoleh, maka *eigenface* (μ) bisa dicari dengan :

$$\mu_i = \sum_{k=1}^{M} v_{ik} \phi_k \tag{6}$$

Sebuah *image* wajah baru atau *test face* (Γ_{new}), akan dicoba untuk dikenali, pertama terapkan cara pada tahapan pertama perhitungan *eigenface* untuk menemukan nilai *eigenface* dari image tersebut.

$$\begin{aligned} \mu_{new} &= v.(T_{new} - \Psi) \\ \Omega &= [\mu_1, \mu_2, \dots, \mu_M] \end{aligned} \tag{7}$$

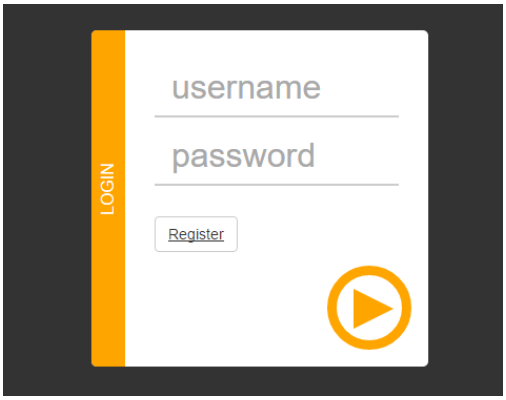
Menggunakan metode *euclidean distance* untuk mencari jarak (*distance*) terpendek antara nilai e*igenface* dari *training image* dalam *database* dengan e*igenface image test face*.

$$\varepsilon_k = \|\Omega - \Omega_k\| \tag{8}$$

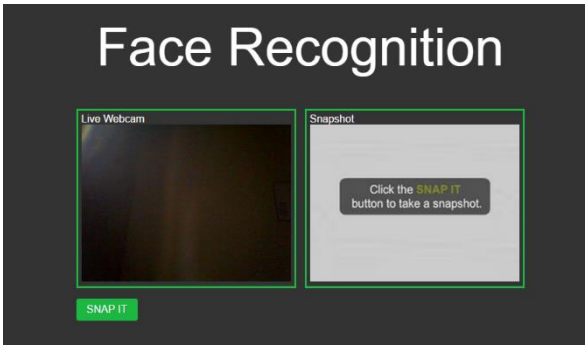
Selanjutnya pengujian sistem dilakukan dangan 3 pengujian, yaitu pengujian *blackbox*, *Performance testing*, pengujian Algoritma *Eigenface*, dan pengujian *Multi Login* Sistem serta *Debugging*. Uji *blackbox* berfokus pada persyaratan fungsional perangkat lunak yang terdiri dari 3 aspek (*efficiency, portability dan usability*). Pengujian diperlukan sebagai salah satu tahapan implementasi untuk menguji tingkat minimal kesalahan dan keakuratan perangkat lunak yang dirancang. Uji algoritma dilakukan untuk mengetahui apakah algoritma *eigenface* dapat digunakan dalam pencocokan wajah. Dalam pengujian ini dilakukan beberapa hal, yaitu dengan membandingkan wajah dari orang yang sama (*Genuine*), membandingkan wajah dengan orang yang berbeda (*impostor*), membandingkan dua pasang saudara kembar. Nilai kecocokan wajah disebut dengan *confidence* dan dalam penelitian ini menetapkan *threshold* dari nilai *confidence* yaitu 0,6. Apabila nilai *confidence* yang didapat di atas batas *threshold* maka dapat dikatakan wajah cocok, jika di bawah batas *threshold* maka dapat dikatakan wajah tidak cocok. Sistem SSO dikatakan berhasil jika dengan sekali *login* di salah satu sistem maka *user* dapat mengakses sistem lain yang terhubung dengan sistem tersebut tanpa harus *login* lagi hal ini dilakukan untuk menguji *multi login* sistem.

III. HASIL PENELITIAN

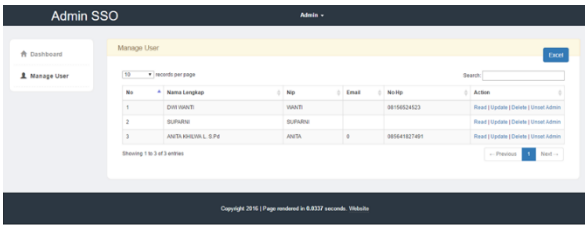
Hasil produk sistem *login* SSO berupa tampilan aplikasi yang dihasilkan dari implementasi desain perancangan sistem yang telah dibuat sebelumnya. Hasil prosuk tampilan sebagai berikut.



Gambar 4. Hasil *Interface* Halaman Login



Gambar 5. Hasil *Interface* Halaman Autentikasi Wajah



Gambar 6. Hasil *Interface* Halaman *Managemen User*

Dari hasil desain sistem dapat diperoleh data bahwa dalam pembuatan sistem ini menghasilkan 3 *frame* atau tampilan dengan ukuran ini 4,17 Mb. Dalam pengimplementasian pengkodean Protokol SSO, terdapat beberapa fungsi yang dibuat dalam tahap pengimplementasiannya, diantaranya fungsi *login(), access_token(), get_data()*. Pada sistem *client* harus menerapkan fungsi *callback()* untuk bisa menghubungkan dengan sistem SSO. Penerapan algoritma *Eigenface* untuk *Face Recognition* menggunakan OpenCV dengan menggunakan fungsi *getSimilarity()* untuk mendapatkan nilai *confidence* dari wajah yang dicocokkan.

Hasil desain data menunjukkan bahwa sistem ini mempunyai 3 *frame*, yaitu halaman *login* SSO, halaman autentikasi wajah, dan halaman manajemen *user*. Sistem ini hanya berukuran 4,2 Mb sehingga sistem ini bisa dijalankan di berbagai computer.

Pada tahap pengujian yang dilakukan dengan 8 pengujian, yaitu pengujian *blackbox*, *performance testing*, *efficiency*, *portability*, *usability*, Algoritma, Multi *Login* sistem dan *debugging*, diperoleh data bahwa dalam pengujian *blackbox* semua fungsi telah berjalan dengan baik. Pada pengujian *Performance testing* menujukkan bahwa kinerja sistem sangat baik dengan ditujukan nilai rata-rata *Grade* A. Pada pengujian *efficiency* menujukkan bahwa rata-rata waktu *page load* halaman web 0,9 detik, yang berarti sudah berada diatas rata-rata *Grade GTMetrix* yang memiliki rata-rata waktu load 6,3 detik. Kemudian *Page Size* 123,95 Kb, *Page Speed Grade* A(95%) dan *Yslow Grade* A (92%) yang berarti sudah berada di atas rata- rata *Grade Page Speed* yang memiliki rata-rata 71%, sedangkan *Grade Yslow* memiliki rata- rata 68%. Pada pengujian aspek *portability* menunjukkan bahwa sistem ini mampu di akses oleh beberapa *web browser* yang telah ada. Sedangkan pada pengujian *usability* dari 10 pertanyaan dan diberikan ke 2 responden. Hasilnya terdapat 16 pertanyaan setuju dan 4 pertanyaan tidak setuju. Pada pengujian ini masuk dalam kriteria layak. Jadi sistem ini telah memenuhi aspek *usability*.

IV. PEMBAHASAN

Pengujian Algoritma *Eigenface*, Bahan yang digunakan untuk pengujian Algoritma *Eigenface*, yaitu 4 data wajah *Genuine*, 4 data wajah *Impostor*, dan 2 pasang wajah saudara kembar. 4 data wajah *Genuine* tersebut terdiri dari 1 wajah tanpa ekspresi sebagai data master pencocokan, 1 wajah dengan ekspresi

senyum, 1 wajah dengan mata terpejam dan 1 wajah dengan menggunakan kacamata. Total keseluruhan data wajah yang digunakan untuk menguji algoritma *Eigenface* ada 13 data wajah. Berikut hasil pengujian algoritma *Eigenface*.

Tabel 1. Hasil Pengujian Algoritma

Wajah	Aspek pengujian	
	Kecepatan (detik)	*confidence*
	Genuine	
1.1	4.24	0.93
1.2	4.49	0.82
1.3	3.15	0.79
1.4	3.48	0.65
	Impostor	
2.1	4.10	0.23
2.2	4.39	0.26
2.3	3.59	0.36
2.4	3.40	0.33

Terkait pengujian Algoritma *Eigenface* pada pengujian wajah *genuine*, seluruh wajah dapat diidentifikasi dengan benar yang menghasilkan nilai *confidence* di atas batas *threshold* seperti yang tertera pada tabel 1 menunjukkan kecocokan pada wajah yang diuji. Pada pengujian wajah *impostor* seluruh wajah menghasilkan nilai *confidence* dibawah batas *threshold*, yaitu 0,6 yang mana berarti wajah dari orang yang berbeda dapat dibedakan. Dalam pengujian wajah kembar identik mendapatkan nilai *confidence* 0,59 yang berarti selisih dengan batas *threshold* adalah 0,1 menunjukkan bahwa algoritma mampu membedakkan wajah yang kembar sekalipun walaupun nilai *confidence* yang dihasilkan mendekati batas *threshold*, yaitu 0,59 jadi wajah kembar hampir dianggap sama.

Dalam Pengujian algoritma juga dihitung nilai FAR (*False Acceptance Rate*) dan FRR (*False Rejection Rate*) dengan menggunakan 4 data wajah sebelumnya (*genuine*) sebagai wajah asli dan 4 data wajah tambahan yang berbeda (*impostor*) dengan penentuan batas *threshold* adalah 0,6. Berikut hasil penghitungan nilai FAR dan FRR.

Tabel 2. Nilai FAR dan FRR

F	f	FAR
0	1,389	0%
G	g	FRR
0	3,277	0%

Keterangan :

f = Identitas palsu yang melebihi batas *threshold*
F = Jumlah seluruh identitas palsu
g = Identitas asli yang kurang dari batas *threshold*
G = Jumlah seluruh identitas asli

Hasil dari pengujian multi *login* sistem, yaitu tiga sistem yang terhubung dengan sistem *login* SSO dapat diakses cukup dengan sekali *login* di salah satu sistem saja. Pada proses *debugging* dilakukan untuk memperbaiki fungsi/proses/tampilan yang salah/ kurang diterima dengan baik dari pengujian *blackbox* yang telah diujikan. Ada beberapa fungsi yang kurang dalam pengujian *blackbox* yang kemudian diperbaiki, yaitu penambahan tampilan *snapshot* dari wajah yang diambil untuk melihat wajah yang baru diambil.

Sistem *Login* SSO adalah sebuah sistem yang dibangun dengan tujuan memudahkan pengguna dalam mengakses berbagai sistem dengan satu akun dan memudahkan pengguna dalam pengelolaan akun. Sistem ini menggunakan metode *Single Sign On* dan *Face Recognition* sebagai metode autentikasi *login*. Pengujian selanjutnya, yaitu pengujian Multi *Login* Sistem, dimana dalam pengujian ini menunjukan hasil bahwa sistem *login* SSO yang dikombinasikan bersama autentikasi *Face Recognition* sudah berjalan dengan baik.

V. PENUTUP

A. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat diambil kesimpulan bahwa Sistem *Login* menggunakan protokol *Single Sign On* (SSO) dan Autentikasi *Face Recognition* dapat dirancang dengan baik dan layak diterapkan di tiga sistem yang dimiliki oleh KPRI Handayani Semarang yaitu sistem toko, sistem arisan, dan sistem undian. Dibuat dengan metode pengembangan perangkat lunak linier sequential model yang terdiri dari analisis, desain, pengkodean dan pengujian.

Pengelolaan *user* oleh admin menjadi lebih terpusat dalam satu *database*. Pengguna tidak harus masuk satu persatu ke setiap sistem dengan akun yang berbeda, hanya cukup *login* melalui satu sistem pengguna langsung bisa mengakses ke seluruh sistem yang terhubung dengan sistem *login* SSO.

User tidak perlu melakukan *login* lagi untuk masuk ke sistem yang berbeda dari sistem yang terhubung. Algoritma *Face Recognition* dalam sistem SSO, yaitu algoritma *Eigenface*. Dapat diketahui dari hasil pengujian bahwa setiap pengujian pencocokan wajah menggunakan algoritma *Eigenface* menunjukkan nilai *confidence* yang sesuai sehingga algoritma ini dapat diterapkan untuk autentikasi *Face Recognition* pada sistem SSO.

B. Saran

Sistem *Login* SSO memiliki performa yang baik dilihat dari hasil performance testing yang telah dilakukan. Perlu ditambahkan fungsi enkripsi pada file foto wajah untuk lebih meningkatkan keamanan autentikasi.

DAFTAR PUSTAKA

[1] Cynthia L Knott, G. Steube, Student Perceptions Of *Password* Security And Maintenance. International Journal of Management & Information Systems F, 2012.

[2] D. Richard Kuhn,Vincent C. Hu W. Timothy Polk, Shu-Jen Chang. Introduction to Public Key Technology and the Federal PKI Infrastructure. NIST SP 800-32, 2001.

[3] J. Wayman, 1999. Technical testing and evaluation of *biometric* identification devices, in A. Jain, et al. (eds) *Biometric*s: Personal Identification in Networked Society. Kluwer Academic Press.

[4] Michael Zimmerman. *Biometric*s and *User* Authentication. SANS Institute. M.Zimmerman, "Biometrics and User Authentication," SANS Institute, 2002.

[5] Patrik telnoni. 2014. SAML single sign-on protocol development using combination of speech and speaker recognition. International Conference on Advanced Informatics: Concept, Theory and Application, ICAICTA.

[6] Jani Hursti. 1997. Single Sign-On. Helsinki University of Technology .

[7] Madhavi A. Indalkar, Prof. Ram Joshi. 2014, Efficient and Secure *Single Sign On* Mechanism for Distributed Network, Int. Journal of Engineering Research and Applications.

[8] Jeaf Wang. 2013. Spatially Enhanced Local Binary Patterns for Face Detection and Recognition in Mobile Device Applications. Department of Electrical and Computer Engineering University of Toronto.

[9] M. A. Turk and A. P. Pentland. 1991. *Face Recognition* Using *Eigenface*s.

[10] Divyarajsinh N. Parmar, Brijesh B. Mehta. 2013. *Face Recognition* Methods & Applications. Int.J.Computer Technology & Applications,Vol 4 (1),84-86, ISSN:2229-6093.

[11] Pressman, Roger S. 2002. Rekayasa Perangkat Lunak :Pendekatan Praktisi (Buku 1). Yogyakarta : Andi.

[12] Jain, Shreya. 2011. 10 Best Tools for Test Automation. On line at: http://www.toolsjournal.com/[diakses pada hari Sabtu, 10 September 2016].