

IMPLEMENTASI ROLE-BASED ACCESS CONTROL (RBAC) PADA SISTEM MANAJEMEN DATA PEKERJA BERBASIS FRAMEWORK LARAVEL

Satria Kusumadewa, Azmuri Wahyu Azinar*, Sumarno, Arif Senja Fitrani

Informatika, Universitas Muhammadiyah Sidoarjo
Jalan Raya Gelam No. 250, Candi, Sidoarjo, Indonesia
azmuri@umsida.ac.id

ABSTRAK

Digitalisasi pengelolaan data sumber daya manusia perlu didukung oleh pembatasan akses agar data calon tenaga kerja, karyawan, dan dokumen pribadi tidak diakses oleh pihak yang tidak berwenang. Permasalahan dalam penelitian ini adalah perlunya sistem yang mampu mengelola data tenaga kerja secara terstruktur dengan hak akses sesuai peran pengguna. Penelitian ini bertujuan mengembangkan Sistem Informasi Sumber Daya Manusia (SI SDM) berbasis Laravel dengan menerapkan *Role-Based Access Control* (RBAC). Metode pengembangan perangkat lunak yang digunakan adalah *waterfall*, meliputi analisis kebutuhan, perancangan, implementasi, pengujian, dan pemeliharaan. Sistem dikembangkan menggunakan Laravel, PostgreSQL, Blade, Tailwind CSS, Spatie Laravel Permission, Google Form, Google Apps Script, *webhook* Laravel, dan DomPDF. Data calon tenaga kerja dikirim melalui Google Form dan *webhook*, kemudian dikelola oleh *Human Resource Development* (HRD). Hasil pengujian *black box* menunjukkan bahwa sistem dapat menampilkan menu sesuai *role*, membatasi akses data, mengelola data calon tenaga kerja, memproses calon tenaga kerja yang diterima menjadi karyawan, mengelola dokumen, serta menghasilkan *report* karyawan dalam bentuk PDF.

Kata kunci : RBAC, Laravel, SI SDM, Spatie Laravel Permission, *webhook*, *black box testing*.

1. PENDAHULUAN

Perkembangan teknologi informasi mendorong organisasi untuk mengelola data tenaga kerja secara digital. Pengelolaan data yang sebelumnya dilakukan secara manual dapat dialihkan ke sistem berbasis web agar proses administrasi menjadi lebih cepat, terstruktur, dan mudah ditelusuri. Namun, digitalisasi juga menimbulkan risiko penyalahgunaan data pribadi apabila sistem tidak memiliki mekanisme pembatasan akses yang jelas. Data seperti identitas, kontak, riwayat lamaran, dokumen KTP, ijazah, foto, dan informasi rekening termasuk data yang perlu dikelola secara hati-hati karena berkaitan dengan privasi calon tenaga kerja maupun karyawan [1].

Dalam penelitian ini, istilah pekerja merujuk pada tenaga kerja yang datanya dikelola dalam sistem, mulai dari tahap calon tenaga kerja atau pelamar, proses penelusuran dan seleksi oleh HRD, hingga menjadi karyawan setelah dinyatakan diterima.

Perlindungan data pribadi dalam sistem informasi perlu memperhatikan ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 35 huruf (a) dan (b) menegaskan bahwa pengendali data pribadi wajib menjaga keamanan data melalui langkah teknis dan operasional yang memadai [2].

Dalam konteks sistem informasi sumber daya manusia, pembatasan akses menjadi salah satu bentuk langkah teknis yang dapat diterapkan agar pengguna hanya dapat mengakses data sesuai tanggung jawabnya.

Salah satu pendekatan yang digunakan untuk mengatur hak akses adalah RBAC. RBAC mengatur

izin pengguna berdasarkan *role* sehingga pengelolaan akses menjadi lebih terstruktur, konsisten, dan sesuai prinsip *least privilege* [3] [4].

Melalui pendekatan ini, Admin hanya berfokus pada pengelolaan akun dan *role*, HRD mengelola data calon tenaga kerja atau pelamar, data karyawan, dokumen, dan *report*, Manajer hanya melihat data sesuai divisi secara *read-only*, sedangkan Karyawan hanya melihat profil dan dokumen miliknya sendiri.

Penelitian ini bertujuan mengimplementasikan RBAC pada SI SDM untuk mendukung pengelolaan calon tenaga kerja hingga menjadi karyawan dengan pembatasan akses berdasarkan *role* pengguna. Rencana penyelesaian masalah dilakukan dengan mengembangkan sistem berbasis Laravel karena mendukung pengembangan aplikasi *web* secara terstruktur dan dapat diintegrasikan dengan *package* Spatie Laravel Permission untuk pengelolaan *role* dan *permission* [5].

Sistem juga memanfaatkan Google Form dan Google Apps Script untuk menerima data calon tenaga kerja atau pelamar, *webhook* Laravel untuk menyimpan data ke *database*, serta DomPDF untuk menghasilkan *report* karyawan. Penelitian ini difokuskan pada implementasi sistem dan pengujian kesesuaian hak akses setiap *role*, bukan pada pengujian keamanan jaringan, server, maupun enkripsi data. Pengelolaan informasi perusahaan yang terstruktur juga diperlukan untuk meningkatkan keamanan data dan meminimalkan risiko penyalahgunaan informasi dalam proses administrasi organisasi [6].

2. TINJAUAN PUSTAKA

2.1. Sistem informasi sumber daya manusia

Sistem informasi sumber daya manusia merupakan sistem yang digunakan untuk mendukung pengelolaan data karyawan secara terintegrasi, mulai dari proses *input*, pemeliharaan data, hingga penyajian informasi atau laporan yang dibutuhkan pengguna [7].

Dalam penelitian ini, SI SDM difokuskan pada penelusuran calon tenaga kerja atau pelamar melalui Google Form, pemeriksaan data oleh HRD, perubahan status lamaran, pemrosesan calon tenaga kerja yang diterima menjadi karyawan, pengelolaan dokumen karyawan, serta pembuatan *report* karyawan.

2.2. Role-Based Access Control

Role-Based Access Control adalah mekanisme pengendalian akses yang menetapkan hak pengguna berdasarkan peran. Mekanisme ini membantu membatasi akses terhadap sumber daya sistem agar pengguna tidak memperoleh hak yang melebihi tanggung jawabnya [3] [4].

Dalam sistem ini, *role* terdiri dari Admin, HRD, Manajer, dan Karyawan. Admin mengelola akun dan *role*, HRD mengelola data calon tenaga kerja, data karyawan, dokumen, dan *report*, Manajer melihat data sesuai divisi secara *read-only*, sedangkan Karyawan hanya melihat profil dan dokumen miliknya sendiri.

2.3. Laravel dan Spatie Laravel Permission

Laravel digunakan sebagai *framework* pengembangan sistem berbasis *web* karena mendukung pengelolaan *routing*, *controller*, *middleware*, validasi, dan basis data. *Package* Spatie Laravel Permission digunakan untuk mengelola *role* dan *permission* sehingga pembatasan akses dapat diatur sesuai peran pengguna [5] [8] [9].

2.4. Perlindungan data pribadi

Perlindungan data pribadi menjadi aspek penting dalam sistem yang mengelola identitas calon tenaga kerja, data karyawan, dan dokumen pendukung. Pembatasan akses berbasis *role* digunakan agar data hanya dapat diakses oleh pengguna yang berwenang sesuai kebutuhan tugasnya [2] [10].

2.5. Penelitian sebelumnya

Beberapa penelitian terdahulu telah membahas penerapan RBAC, Laravel, pengelolaan dokumen digital, dan perlindungan data pribadi. Penelitian oleh Mary dan Febriyani [8] membahas peningkatan aspek keamanan sistem informasi berbasis Laravel melalui kombinasi pengaturan akses dan pembatasan penggunaan sistem RBAC. Hasil penelitian menunjukkan bahwa penerapan mekanisme tersebut mampu meningkatkan skor keamanan sistem serta menurunkan risiko akses ilegal berdasarkan pengujian *code inspection*, *security review*, dan *performance testing*.

Selanjutnya, Nasich et al. [9] membahas penerapan RBAC menggunakan Laravel dan Spatie

Laravel Permission untuk meningkatkan keamanan akses data pada sistem manajemen pelanggan dan pembayaran air berbasis *web*. Hasil pengujian *white-box* dan *black-box* menunjukkan bahwa RBAC efektif mengendalikan akses pengguna.

Penelitian lain oleh Pratama [11] membahas pengembangan sistem arsip digital berbasis Laravel untuk efisiensi penyimpanan dan keamanan data. Pengujian aplikasi menitikberatkan pada aspek fungsionalitas, dengan hasil berupa penurunan waktu pencarian *file*, penghematan kapasitas penyimpanan, serta peningkatan kepuasan pengguna. Junaedi [10] menelaah penerapan Undang-Undang Nomor 27 Tahun 2022 dalam konteks perlindungan privasi di era digital melalui pendekatan studi literatur. Pembahasan difokuskan pada perbedaan antara konsep perlindungan data pribadi dan implementasinya di lapangan, khususnya pada aspek penegakan hukum, tingkat kesadaran masyarakat, serta kesiapan lembaga pengawas.

Selain itu, Sahyudi dan Susanto [12] menganalisis penerapan RBAC pada sistem keamanan basis data menggunakan pendekatan *systematic literature review* (SLR). Hasil kajian literatur menunjukkan bahwa penerapan RBAC dapat mendukung peningkatan keamanan dan efisiensi manajemen akses.

Berdasarkan hasil kajian pustaka dan penelitian terdahulu, ditemukan bahwa sebagian besar penelitian sebelumnya telah membahas RBAC, Laravel, keamanan data, pengelolaan dokumen digital, dan perlindungan data pribadi. Namun, kesenjangan penelitian yang menjadi dasar penelitian ini adalah sebagai berikut:

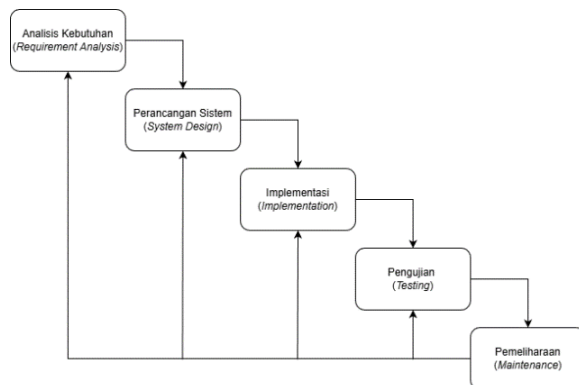
- Penelitian sebelumnya masih banyak berfokus pada keamanan sistem, kajian hukum, sistem arsip digital, sistem pelanggan, atau aplikasi ERP, sedangkan penerapan RBAC pada sistem pengelolaan data pekerja masih terbatas.
- Belum banyak penelitian yang menggabungkan RBAC berbasis Laravel dengan alur pengelolaan data calon tenaga kerja atau pelamar hingga menjadi karyawan.
- Penelitian yang mengintegrasikan penerimaan data melalui Google Form dan *webhook*, pengelolaan data karyawan, dokumen, serta pembatasan akses berdasarkan *role* pengguna masih belum banyak dibahas.

Oleh karena itu, penelitian ini berfokus pada penerapan RBAC dalam sistem pengelolaan data pekerja berbasis Laravel dengan pembatasan akses berdasarkan *role* pengguna.

3. METODE PENELITIAN

Jenis penelitian ini adalah pengembangan perangkat lunak berbasis *web*. Model pengembangan yang digunakan adalah *waterfall* karena tahapan pengembangan dilakukan secara terstruktur mulai dari analisis kebutuhan, perancangan, implementasi, pengujian, hingga pemeliharaan. Model ini dipilih

karena kebutuhan sistem telah ditentukan secara jelas, yaitu mengelola data calon tenaga kerja atau pelamar, data karyawan, dokumen, report, dan hak akses berdasarkan *role*.



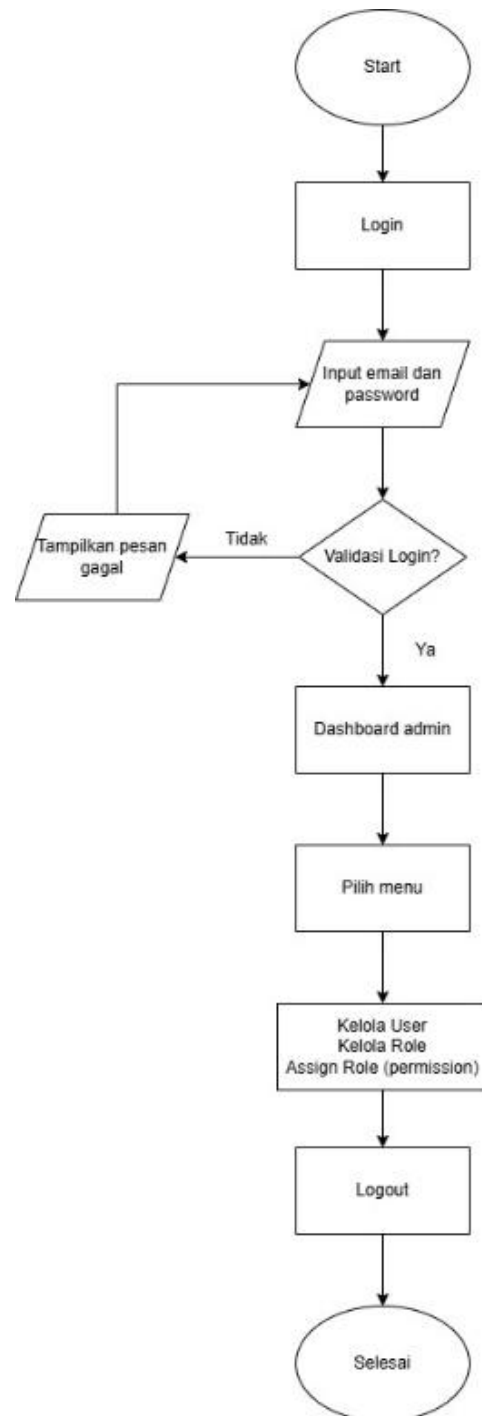
Gambar 1. Diagram *waterfall*

Gambar 1 menunjukkan tahapan *waterfall* yang digunakan pada penelitian ini. Tahapan dimulai dari analisis kebutuhan, perancangan sistem, implementasi, pengujian, dan pemeliharaan.

Analisis Kebutuhan. Tahap ini dilakukan untuk menentukan kebutuhan sistem dan pengguna. Sistem memiliki pengguna *login* yang terdiri dari Admin, HRD, Manajer, dan Karyawan. Calon tenaga kerja atau pelamar tidak termasuk pengguna *login* karena hanya mengisi data melalui Google Form. Data utama yang dikelola meliputi data calon tenaga kerja atau pelamar, data karyawan, dokumen karyawan, *user*, *role*, dan report karyawan.

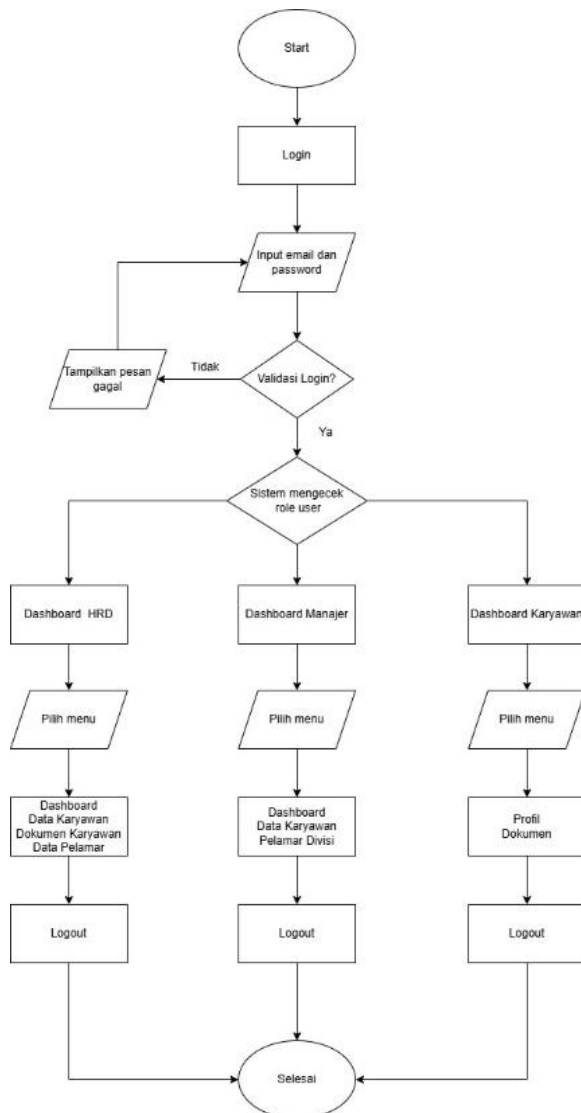
Perancangan Sistem. Perancangan dilakukan untuk menggambarkan alur kerja sistem, struktur basis data, serta pembatasan akses berdasarkan RBAC. *Flowchart* digunakan untuk menggambarkan tahapan atau alur proses sistem secara berurutan sehingga proses kerja setiap pengguna dapat dipahami dengan lebih jelas [13].

Alur utama sistem dimulai ketika calon tenaga kerja atau pelamar mengisi Google Form, kemudian Google Apps Script mengirimkan data ke *webhook* Laravel. Data tersebut disimpan ke *database* sebagai data calon tenaga kerja atau pelamar dan dapat dilihat oleh HRD. Jika calon tenaga kerja dinyatakan diterima, HRD memproses data tersebut menjadi data karyawan, melengkapi data pekerjaan dan rekening, mengelola dokumen, serta mencetak *report* karyawan.



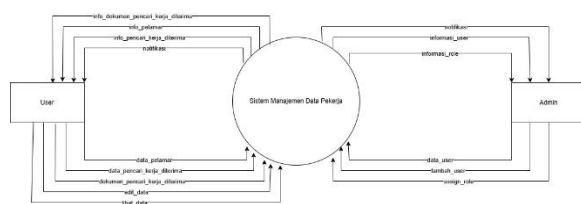
Gambar 2. *Flowchart* admin

Gambar 2 menjelaskan alur penggunaan sistem oleh Admin. Setelah *login* dan validasi berhasil, Admin masuk ke *dashboard* untuk memilih menu, mengelola *user*, mengelola *role*, menetapkan *role* kepada pengguna, kemudian *logout* setelah proses selesai.



Gambar 3. Flowchart user hrd, manajer, dan karyawan

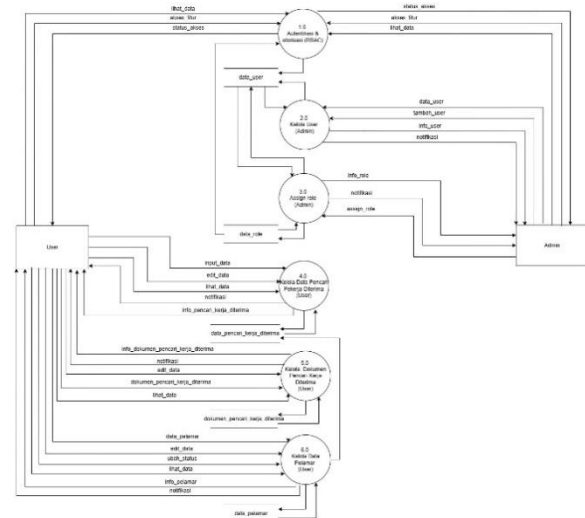
Gambar 3 menunjukkan alur penggunaan sistem oleh HRD, Manajer, dan Karyawan. Setelah login dan validasi berhasil, sistem membaca *role* pengguna, kemudian menampilkan *dashboard* dan menu sesuai hak akses. HRD dapat mengelola data pelamar, data karyawan, dokumen, dan *report*. Untuk Manajer melihat data sesuai divisi sedangkan Karyawan melihat profil dan dokumen pribadinya.



Gambar 4. DFD level 0

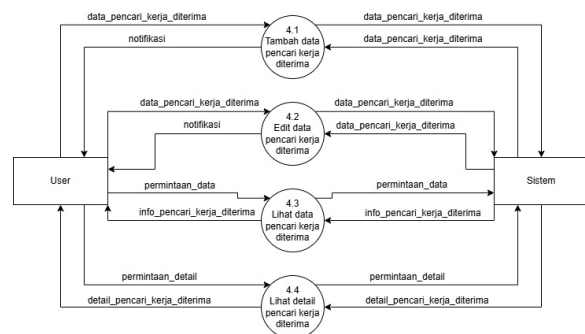
Gambar 4 menunjukkan Data Flow Diagram (DFD) level 0 atau diagram konteks yang menggambarkan hubungan sistem dengan calon tenaga kerja atau pelamar, Admin, HRD, Manajer, dan

Karyawan. Setiap entitas memiliki aliran data sesuai kewenangannya.



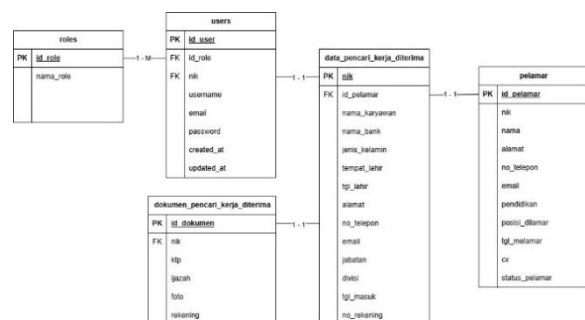
Gambar 5. DFD level 1

Gambar 5 menunjukkan DFD level 1 yang merinci proses utama sistem, yaitu pengelolaan *user* dan *role*, data calon tenaga kerja atau pelamar, data karyawan, dokumen karyawan, dan *report* karyawan.



Gambar 6. DFD level 2

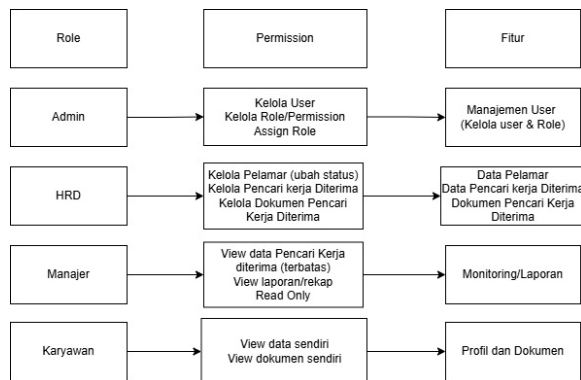
Gambar 6 menunjukkan DFD level 2 pada proses calon tenaga kerja yang diterima menjadi karyawan. Proses dimulai dari pemeriksaan data, perubahan status, pelengkapan data administrasi, hingga penyimpanan sebagai data karyawan.



Gambar 7. Entity relationship diagram

Gambar 7 menggambarkan Entity Relationship Diagram (ERD) yang digunakan untuk

merepresentasikan hubungan antar entitas, atribut, dan relasi data sebelum diimplementasikan ke dalam basis data [14]. Relasi ini digunakan agar data calon tenaga kerja yang diterima dapat dilanjutkan menjadi data karyawan.



Gambar 8. Diagram RBAC

Gambar 8 menunjukkan pembagian *role* dan *permission*. Admin mengelola user dan *role*, HRD mengelola data calon tenaga kerja atau pelamar, karyawan, dokumen, dan *report*, Manajer melihat data sesuai divisi secara *read-only*, sedangkan Karyawan hanya melihat data miliknya sendiri. Implementasi. Implementasi sistem dilakukan menggunakan Laravel 12, PHP 8.2, PostgreSQL, Blade, Tailwind CSS, dan Spatie Laravel Permission. Integrasi data calon tenaga kerja atau pelamar dilakukan melalui Google Form, Google Apps Script, *webhook* Laravel, dan Ngrok untuk pengujian lokal *webhook*. *Report* karyawan dibuat menggunakan DomPDF sehingga HRD dapat mengunduh PDF atau melakukan *print out*.

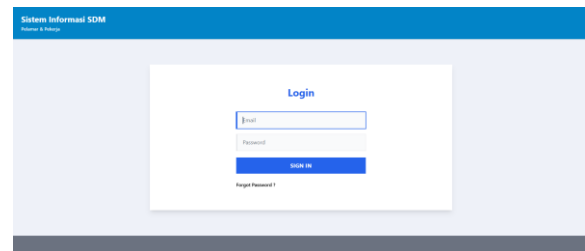
Pengujian. Pengujian dilakukan menggunakan metode *black box testing*. Pengujian difokuskan pada fungsi *login*, kesesuaian dashboard dan menu berdasarkan *role*, pengelolaan *user* dan *role*, penerimaan data calon tenaga kerja atau pelamar dari Google Form, pengubahan status calon tenaga kerja atau pelamar, pengelolaan data karyawan, pengelolaan dokumen, *report* PDF, serta pembatasan akses Manajer dan Karyawan.

Pemeliharaan. Tahap pemeliharaan dilakukan untuk memperbaiki kesalahan, menyesuaikan data, dan memastikan sistem tetap berjalan sesuai kebutuhan pengguna. Pemeliharaan tidak diarahkan pada penambahan fitur baru di luar ruang lingkup penelitian, melainkan pada stabilitas dan kesesuaian fungsi sistem.

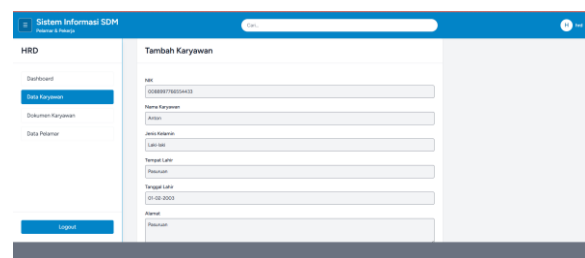
4. HASIL DAN PEMBAHASAN

4.1. Hasil implementasi sistem

Hasil dari penelitian ini adalah SI SDM dengan alur pengelolaan calon tenaga kerja hingga menjadi karyawan. Sistem digunakan untuk mengelola data calon tenaga kerja atau pelamar, data karyawan, dokumen karyawan, *user*, *role*, serta *report* karyawan. Setiap pengguna memperoleh halaman dan menu yang berbeda sesuai *role* yang diberikan.

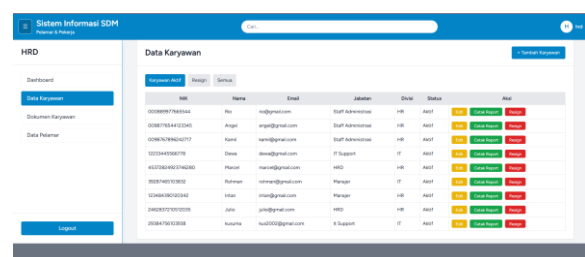
Gambar 9. Halaman *login* sistem informasi SDM

Gambar 9 menunjukkan halaman *login* sebagai awal autentikasi pengguna. Setelah *email* dan *password* diverifikasi, sistem mengarahkan pengguna ke halaman sesuai *role*.



Gambar 10. Halaman tambah karyawan

Gambar 10 menunjukkan halaman tambah karyawan yang digunakan oleh HRD untuk melengkapi data calon tenaga kerja yang telah diterima. Pada halaman ini, HRD dapat menambahkan data administrasi seperti divisi, tanggal masuk, nomor rekening, dan nama bank sebelum data disimpan sebagai data karyawan.



Gambar 11. Halaman data karyawan

Gambar 11 menunjukkan halaman data karyawan yang berisi data hasil penerimaan calon tenaga kerja. Halaman ini menyediakan fitur *edit* data, cetak *report*, dan pengubahan status karyawan.

Gambar 12. Halaman *report* data karyawan

Gambar 12 menunjukkan halaman *report* data karyawan yang berisi identitas, data pekerjaan, data rekening, kelengkapan dokumen, tanggal cetak, dan tanda tangan HRD. *Report* dapat diunduh dalam PDF atau dicetak.

4.2. Cara kerja dan penggunaan sistem

Cara kerja sistem dimulai dari calon tenaga kerja atau pelamar yang mengisi Google Form. Data yang diisi calon tenaga kerja atau pelamar dikirim oleh Google Apps Script ke *webhook* Laravel, kemudian disimpan sebagai data calon tenaga kerja atau pelamar. HRD *login* ke sistem untuk melihat daftar calon tenaga kerja atau pelamar, membuka detail, memeriksa dokumen, dan mengubah status lamaran. Jika calon tenaga kerja dinyatakan diterima, HRD memproses data tersebut menjadi data karyawan dan melengkapi data administrasi seperti divisi, tanggal masuk, nomor rekening, dan nama bank.

Admin menggunakan sistem untuk mengelola *user* dan *role*. HRD mengelola data calon tenaga kerja

atau pelamar, memproses data menjadi karyawan, mengelola dokumen, dan mencetak *report*. Manajer melihat data sesuai divisi secara *read-only*, sedangkan Karyawan hanya melihat profil dan dokumen miliknya sendiri.

Validasi data diterapkan agar data yang disimpan lebih sesuai dengan kebutuhan administrasi. NIK dibatasi angka tepat 16 digit, nomor telepon 10 sampai 15 digit, nomor rekening 6 sampai 18 digit, nama bank maksimal 50 karakter, nama karyawan dan jabatan maksimal 100 karakter, serta alamat maksimal 255 karakter. Validasi ini mendukung konsistensi data dan mengurangi kesalahan *input*.

4.3. Hasil pengujian sistem

Pengujian sistem dilakukan menggunakan *black box testing* dengan tujuan memastikan fungsi utama berjalan sesuai kebutuhan. Pengujian difokuskan pada kesesuaian *input* dan *output* sistem, terutama pembatasan akses berdasarkan *role* seperti pada Tabel 1 dan Tabel 2.

Tabel 1. Hasil pengujian *black box* admin

No	Fitur Diuji	Skenario	Hasil Yang Diharapkan	Hasil
1	Login Admin	Admin melakukan login	Sistem menampilkan <i>Dashboard</i> Admin	Sesuai
2	Kelola user	Admin menambah, mengedit, atau menghapus user	Data user tersimpan, berubah, ataupun terhapus	Sesuai
3	Kelola role	Admin membuka menu kelola <i>role</i> dan melihat daftar <i>role</i>	Sistem menampilkan <i>Role</i> dan <i>permission</i>	Sesuai
4	Assign role	Admin menetapkan <i>role</i> kepada user	Akses user sesuai <i>role</i>	Sesuai

Berdasarkan Tabel 1, seluruh fungsi utama pada *role* Admin berjalan sesuai skenario pengujian. Admin dapat melakukan *login*, mengelola *user*, melihat dan mengelola *role*, serta menetapkan *role* kepada

pengguna. Hasil ini menunjukkan bahwa fungsi pengelolaan akun dan *role* telah berjalan sesuai kebutuhan sistem.

Tabel 2. Hasil pengujian *black box* user

No	Fitur Diuji	Skenario	Hasil Yang Diharapkan	Hasil
1	Login User	User login sesuai <i>role</i>	Sistem menampilkan <i>dashboard</i> dan menu sesuai <i>role</i> pengguna	Sesuai
2	Data Pelamar (HRD)	HRD membuka Data Pelamar	Sistem menampilkan data dari <i>webhook</i>	Sesuai
3	Detail Pelamar (HRD)	HRD membuka detail pelamar	Sistem menampilkan detail data dan dokumen pendukung	Sesuai
4	Status pelamar (HRD)	HRD mengubah status calon tenaga kerja atau pelamar	Status calon tenaga kerja atau pelamar berhasil tersimpan	Sesuai
5	Proses Pelamar Menjadi Karyawan (HRD)	HRD memproses calon tenaga kerja atau pelamar yang diterima menjadi data karyawan	Data tersimpan sebagai karyawan	Sesuai
6	Data Karyawan (HRD)	HRD mengedit data karyawan	Data karyawan tampil dan dapat diperbarui oleh HRD	Sesuai
7	Dokumen Karyawan (HRD)	HRD mengelola dokumen	Dokumen tersimpan dan dapat ditampilkan melalui fitur <i>preview</i>	Sesuai
8	Report Karyawan (HRD)	HRD membuka <i>report</i> karyawan, mengunduh PDF, atau melakukan <i>print out</i>	Sistem menampilkan <i>report</i> dan menghasilkan laporan PDF/cetak	Sesuai
9	Lihat Divisi (Manajer)	Manajer melihat data karyawan divisinya	Data tampil sesuai divisi secara <i>read-only</i>	Sesuai
10	Profil (Karyawan)	Karyawan membuka profil	Data pribadi tampil secara <i>read-only</i>	Sesuai
11	Pembatasan Akses User	User login sesuai <i>role</i>	<i>Dashboard</i> dan menu tampil sesuai <i>role</i>	Sesuai

Berdasarkan Tabel 2, fungsi pada *role* HRD, Manajer, dan Karyawan berjalan sesuai skenario. HRD dapat mengelola data calon tenaga kerja atau pelamar, proses menjadi karyawan, dokumen, dan *report*. Manajer hanya melihat data sesuai divisi secara *read-only*, sedangkan Karyawan hanya melihat profil pribadinya. Hasil ini menunjukkan bahwa akses fitur telah sesuai dengan *role* masing-masing pengguna.

4.4. Pembahasan

Implementasi RBAC pada SI SDM menunjukkan bahwa pembagian hak akses berdasarkan *role* dapat membantu pengendalian akses data tenaga kerja. Admin tidak mengelola data operasional calon tenaga kerja dan karyawan, HRD menjadi pengguna utama dalam proses administrasi data, Manajer hanya melakukan pemantauan data sesuai divisi, dan Karyawan hanya mengakses data pribadinya. Pembagian tersebut membuat akses lebih terarah dan mengurangi kemungkinan data pribadi dilihat atau dikelola oleh pengguna yang tidak berwenang.

Integrasi *Google Form*, *Google Apps Script*, dan *webhook* Laravel membantu proses penerimaan data calon tenaga kerja atau pelamar tanpa menjadikan calon tenaga kerja atau pelamar sebagai pengguna *login*. Dengan demikian, sistem tetap dapat menerima data awal rekrutmen, sementara pengelolaan lanjutan tetap dikendalikan oleh HRD di dalam sistem. Fitur *report* karyawan juga mendukung kebutuhan administrasi karena HRD dapat mencetak data akhir karyawan setelah data dan dokumen dilengkapi.

5. KESIMPULAN DAN SARAN

Penelitian ini berhasil mengembangkan SI SDM berbasis Laravel dengan penerapan RBAC menggunakan Spatie Laravel Permission. Sistem mampu mengelola data calon tenaga kerja atau pelamar dari *Google Form* melalui *webhook* Laravel, memproses calon tenaga kerja yang diterima menjadi data karyawan, mengelola dokumen karyawan, serta menghasilkan *report* karyawan dalam bentuk PDF. Pembatasan akses berdasarkan *role* berjalan sesuai kebutuhan, yaitu Admin mengelola *user* dan *role*, HRD mengelola data calon tenaga kerja atau pelamar, data karyawan, dokumen, dan *report*, Manajer melihat data sesuai divisi secara *read-only*, dan Karyawan hanya melihat profil serta dokumen miliknya sendiri. Hasil pengujian *black box* menunjukkan seluruh fungsi utama berjalan sesuai skenario dan mendukung prinsip *least privilege* dalam perlindungan data tenaga kerja. Saran untuk penelitian selanjutnya adalah melakukan pengujian keamanan yang lebih luas, seperti audit keamanan aplikasi, enkripsi data, serta evaluasi performa sistem pada penggunaan dengan jumlah data yang lebih besar.

DAFTAR PUSTAKA

[1] L. A. F. Rosalinda, "Tinjauan Yuridis Terhadap Penyalahgunaan Data Pribadi oleh Oknum Tertentu dalam Aplikasi Pinjaman Online," *J.*

Commer. Law, vol. 5, no. 1, pp. 243–249, 2025, doi:

<https://doi.org/10.29303/commercelaw.v5i1.3767>.

- [2] D. E. Mahameru, A. Nurhalizah, A. Wildan, M. Haikal, and M. H. Rahmadia, "Implementasi UU Perlindungan Data Pribadi terhadap Keamanan Informasi Identitas di Indonesia," *J. Esensi Huk.*, vol. 5, no. 20, pp. 115–131, 2023, doi: <https://journal.upnvj.ac.id/index.php/esensihukum/index>.
- [3] Y. A. Prasetia and D. Manongga, "ROLE-BASED ACCESS CONTROL (RBAC) UNTUK SISTEM OTORISASI TERPUSAT BERBASIS FLASK STUDI KASUS PT. XYZ," vol. 9, no. 4, pp. 1768–1778, 2024, [Online]. Available: <https://doi.org/10.29100/jipi.v4i1.5403>
- [4] Y. Yuricha and I. K. Phan, "Penerapan Role Based Access Control dalam Sistem Supply Chain Management Berbasis Cloud," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, vol. 3, no. 2, pp. 339–348, 2023, doi: 10.57152/malcom.v3i2.1259.
- [5] M. A. Hardiansyah and B. Irawan, "Design and Development of a Web-Based Maintenance Employee Management Application Using Laravel Framework," *Technovasia*, vol. Vol 1, No.; no. 1, pp. 27–45, 2025.
- [6] A. N. Illah *et al.*, "Urgensi Enterprise Information Management pada Peningkatan Keamanan Data Perusahaan," *Khazanah J. Mhs.*, vol. 16, no. 1, pp. 32–41, 2024, doi: <https://journal.uui.ac.id/khazanah>.
- [7] Mikhriani, A. S. Wati, and N. I. H. Kunio, *Sistem Informasi Manajemen Sumber Daya Manusia: Manajemen Sumber Daya Manusia yang Terintegrasi, Produktif, dan Berdaya Saing dengan SIM SDM*, Cetakan Pe. Bandung: Widina Media Utama, 2024.
- [8] T. Mary and N. Febriyani, "Peningkatan Keamanan Sistem Informasi Berbasis Laravel 12 dengan Rate Limiting dan Role-Based Access Control (RBAC)," *J. Teknol. Dan Sist. Inf. Bisnis*, vol. 7, no. 3, pp. 473–481, 2025, doi: 10.47233/jteksis.v7i3.1976.
- [9] A. K. Nasich, S. A. Wicaksono, and M. C. Saputra, "Implementasi Role Based Access Control (RBAC) dalam Sistem Informasi Manajemen Pelanggan dan Pembayaran Air Berbasis Web (studi pada PT Tirta Wangi Sejahtera)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 9, no. 9, pp. 2548–964, 2025, [Online]. Available: <http://j-ptiik.ub.ac.id>
- [10] A. M. Junaedi, "Urgensi Perlindungan Data Pribadi Dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022," *Knowl. J. Inov. Has. Penelit. dan Pengemb.*, vol. 5, no. 2, pp. 247–257, 2025, [Online]. Available: <https://jurnalp4i.com/index.php/knowledge>
- [11] P. A. Pratama, "Pengembangan Sistem Arsip

- Digital Berbasis Website dengan Framework Laravel untuk Efisiensi Penyimpanan dan Keamanan Data,” *J. Komput. dan Teknol. Sains*, vol. 3, no. 2, pp. 9–12, 2024.
- [12] M. Sahyudi and E. R. Susanto, “Analisis Implementasi Sistem Keamanan Basis Data Berbasis Role-Based Access Control (RBAC) pada Aplikasi Enterprise Resource Planning,” *SATESI J. Sains Teknol. dan Sist. Inf.*, vol. 5, no. 1, pp. 105–116, 2025, doi: 10.54259/satesi.v5i1.3997.
- [13] K. I. Listyoningrum, D. Y. Fenida, and N. Hamidi, “Inovasi Berkelanjutan dalam Bisnis: Manfaatkan Flowchart untuk Mengoptimalkan Nilai Limbah Perusahaan Sustainable Innovation in Business: Leverage Flowcharts to Optimize the Value of Corporate Waste,” *JIPM – J. Inf. Pengabd. Masy.*, vol. 1, no. 4, pp. 100–112, 2023, doi: <https://doi.org/10.47861/jipm-nalanda.v1i4.552>.
- [14] O. Palinggi *et al.*, “Entity-Relationship Diagram Technique in Database,” *Collabits J.*, vol. 1, no. 2, pp. 102–104, 2024, doi: <https://doi.org/10.22441/collabits.v1i2.27252>.