BAB II
KERANGKA TEORITIS

A. Landasan Teori

1. Informasi

Menurut (Rainer & Cegielsky, 2011) informasi adalah data yang telah diolah menjadi sebuah bentuk yang berarti bagi penerimanya dan bermanfaat dalam pengambilan keputusan saat ini atau saat mendatang, informasi berperan penting dalam sebuah sistem, Dalam manajemen, suatu informasi harus dapat dipercaya, tingkat kepercayaan informasi memberi dampak pada hasil keputusan yang diambil, apabila informasi yang diterima oleh pengelola merupakan informasi yang benar maka keputusan yang diambil dapat tepat dan optimal, tingkat kepercayaan informasi dapat didasarkan kepada sifat dari individu yang menjadi narasumber, informasi yang tepercaya berasal dari individu yang memiliki sifat jujur dalam menyampaikan data, sehingga informasi harus dikendalikan dan diamankan.

2. Data

Menurut (Conolly & Begg, 2015) Data merupakan komponen terpenting sebagai penghubung antara mesin (hardware) dan manusia, sehingga dalam informasi data merupakan komponen utama, sehingga data juga merupakan aspek penting dalam sebuah informasi, data-data yang terlah terbentuk menjadi informasi harus diamankan dan tidak boleh sembarangan orang dapat mengubah ataupun menghapus data ini, karena itu memberikan otorisasi merupakan jalan terbaik agar data tidak di rubah dan hilang.

3. *JWT (JSON Web Token)*

Seperti namanya, *JSON Web Token*, yang berarti token ini menggunakan *JSON (Javascript Object Notation)*, lalu token ini memungkinkan kita untuk mengirimkan data yang dapat diverifikasi oleh dua pihak atau lebih. (Muntashir, 2020). Pada otentikasi/otorisasi umumnya pengembabg *software* menggunakan session, yang mana ketika user login ke sebuah web, maka server akan menyimpan data user tersebut.

Sehingga data session yang tersimpan itu akan digunakan untuk melakukan verifikasi untuk memastikan user sudah login atau belum, dan memastikan hak akses user yang login.

4. *Feature Flag (Feature Toggle)*

Feature Toggles (sering juga disebut sebagai *Feature Flags*) adalah teknik yang kuat, memungkinkan tim untuk memodifikasi perilaku sistem tanpa mengubah kode. (Fowler, 2017). Dari pengertian tersebut singkatnya *Feature Flag* itu teknik atau metode untuk melakukan modifikasi fitur atau sistem tanpa mengubah kodenya.

Setelah melihat metode dasar yang disediakan oleh Feature Toggles (*Feature Flag*s), metode tersebut mampu mengirimkan *code* alternatif dalam satu unit yang dapat diterapkan ketika aplikasi sedang berjalan, skenario ini juga menunjukkan bahwa fasilitas ini dapat digunakan dengan berbagai berbagai konteks, dan memungkinkan metode tersebut dapat digabungkan ke dalam satu metode yang digunakan di dalam sebuah pengembangan.

Feature Toggles terdiri dari 4 Kategori yaitu:

1. *Release Toggles*

   Release toggle digunakan untuk melakukan rilis dimana aplikasi yang dikembangkan dapat di deploy secara aman tanpa mengganggu aplikasi yang telah berjalan dengan memisahkan tahap development ke dalam beberapa fitur-fitur kecil sehingga lebih mudah untuk melakukan deployment dengan skala kecil.

2. *Experiment Toggles*

   Digunakan untuk melakukan A/B Testing, dimana *Feature Toggles* tersebut yang mengatur kemana arah alur aplikasi berjalan, Sehingga memudahkan untuk melakukan penelitian dan mengambil keputusan di dalam pengembangan sebuah aplikasi.

3. *Ops Toggles*

   Digunakan untuk melakukan kontrol terhadap aspek operasional di dalam sistem, dimana tahap operasional ini dapat berubah-ubah berdasarkan keperluan produksi, *Feature Toggles* ini memudahkan pihak operasional untuk mengembangkan atau mematikan tahap operasional tertentu.

4. *Permissioning Toggles*

   Digunakan untuk melakukan kontrol terhadap aspek otorisasi di dalam sistem, dimana *Feature Toggles* ini dapat mengatur beberapa aspek dalam otorisasi sehingga pengguna dapat dengan mudah mengubah otorisasi di dalam sistem, dan kategori ini yang akan digunakan dalam proses pengembangan aplikasi pada penelitian ini.

Feature Toggles membantu dan membawa kompleksitas tambahan, dan membuat tahap development menjadi lebih mudah dengan masa yang cukup lama untuk sistem yang menggunakan metode ini.

B. Tinjauan Pustaka

Adapun penelitian serupa yang saya gunakan sebagai acuan membuat penelitian ini dengan masalah berbeda yang pernah dilakukan sebagai berikut:

1. **Rohmat Gunawan dan Alam Rahmatulloh, Tahun 2019 JSON Web Token (JWT) untuk Authenticationpada Interoperabilitas Arsitektur berbasis RESTfulWeb Service.** Permasalahan donor darah merupakan masalah disetiap negara, termasuk di Indonesia. Walaupun sudah ada sistem di Palang Merah Indonesia (PMI) namun belum bisa mengatasi permasalahan pencarian maupun distribusi donor darah. Sesuai trend sekarang di jaman gadget yaitu maraknya penggunaan Android, maka untuk mengatasi masalah ini diperlukan aplikasi berbasis Android. Sementara untuk integrasi dengan sistem yang sudah ada diperlukan web service sebagai backend system sehingga layanan donor darah dapat diakses oleh berbagai platform. Arsitektur yang digunakan pada web service menggunakan REST, namun masih ada beberapa masalah pada REST yaitu mengenai keamanan pada proses otentikasi. Pada arsitektur REST diperlukan metode otentikasi yang tidak bernegara (*stateless*), salah satunya dapat menggunakan *JSON Web Token*. Hasil penelitian ini menunjukan bahwa penggunaan *JSON Web Token Authentication* pada Web Service and Backend System Blood Donors dapat membentuk sistem yang sangat skalabel, aman, mampu berinteraksi multi-platform serta dapat diandalkan.
2. **Sopingi, Faulinda Ely Nastiti, dan Arviyan Sofyan Majid, Tahun 2019, Implementasi JSON Web Token Authentication pada Aplikasi Pembayaran Berbasis Mobile.** Alat pembayaran saat ini semakin berkembang dari pembayaran tunai menjadi pembayaran non tunai. Seperti pembayaran yang dilakukan di Universitas Duta Bangsa yang sebelumnya dilakukan dengan melakukan setor tunai langsung pada teller bank, kemudian saat ini dikembangkan ke pembayaran non tunai melalui aplikasi pembayaran berbasis mobile. Mahasiswa dapat melakukan pembayaran dari berbagai chanel pembayaran dan secara otomatis ditransaksikan di sistem informasi keuangan. Akan tetapi terdapat permasalahan keamanan data mahasiswa yang disimpan di dalam aplikasi dan proses *authentication* pada setiap proses transaksi data antara aplikasi dengan *web service* sistem keuangan. Penulis memberikan solusi berupa penggunaan *JSON Web Token (JWT)* pada proses authentication dan penerapan hash token pada setiap data yang dikirim ke server untuk memvalidasi keaslian data berasal dari aplikasi pembayaran berbasis mobile. Dalam penelitian ini penulis menggunakan metode *Rapid*

Application Development (RAD) dan melakukan pengujian teknik *User Acceptance Testing (UAT)* kepada pengguna. Berdasarkan hasil *User Acceptance Testing* diketahui bahwa aplikasi pembayaran berbasis mobile mampu melalukan *authentication* menggunakan JWT dan berhasil mengamankan data dengan penggunaan *hash token* pada setiap request ke *web service*.

3. **Pratama Abdul Karim dan Aditya, Tahun 2021, Pengujian Penetrasi Penyimpanan Token Menggunakan Cookie Storage Pada JSON WEB TOKEN.** Proses otentikasi merupakan tindakan pembuktian terhadap identitas pengguna saat akan memasuki sebuah sistem. Otentikasi berbasis token adalah jenis token yang *stateless*. Artinya ketika proses otentikasi dilakukan sama sekali tidak ada informasi tentang pengguna, karena penggunaan token dalam setiap request dilakukan dari *client* ke *server*. *Java Script Object Notation (JSON) Web Token* adalah teknik otentikasi yang menyediakan cara terbuka dan aman untuk mewakili klaim antara dua pihak, ditandatangani secara kriptografis yang dirancang untuk tidak dipalsukan. Namun, ini perlu dibuktikan aman dan tidak rentan. Tujuan dari penelitian ini adalah melakukan pengujian penetrasi keamanan penyimpanan *JSON Web Token (JWT)* pada penyimpanan cookie dengan menggunakan teknik *CSRF* dan *Brute-Force*. Skenario untuk melakukan teknik *CSRF* dan *Brute-Force* disiapkan dalam percobaan. Arsitektur sistem dan alat yang akan digunakan disiapkan sebelum percobaan dilakukan. Hasil percobaan pada penelitian ini menunjukan bahwa bagian dari atribut *cookie* yang menyematkan *flag* “seththttponly: false”, dapat diakses oleh javascript di sisi klien (*Read* dan *Write*). *Brute-force* berhasil mengetahui kunci rahasia yang sah dengan perhitungan tanda tangan dalam rentang waktu 1 menit 49 detik dan ditandai oleh status *cracked*. Teknik *CSRF* dan *Brute-force* yang dicoba dalam penelitian telah berhasil memanfaatkan token JWT yang disimpan dalam untuk mengirimkan permintaan palsu. Akhirnya akun korban digunakan dan sumber daya diambil alih.
4. **Edy, Ferdiansyah, Wahyu Pramusinto dan Sejati Waluyo, Tahun 2019, Pengamanan Restful API menggunakan JWT untuk Aplikasi Sales Order.** Perusahaan mempunyai peran penting didalam menarik perhatian pelanggan dengan mempromosikan produk dan layanannya sehingga dapat dikenal luas oleh masyarakat melalui divisi penjualan (*sales person*).Tantangan terbesar yang dihadapi oleh perusahaan sangat berkaitan dengan pemasaran, yaitu pertumbuhan pendapatan yang stabil dan berkelanjutan, serta loyalitas pelanggan. Sehingga penerapan teknologi informasi dan komunikasi

diperlukan dalam dunia bisnis sebagai alat bantu memenangkan persaingan utama dalam memasarkan produk atau jasa. Di dalam perusahaan, data pemesanan yang dilakukan *sales person* masih melalui *telephone.* Dibutuhkan aplikasi untuk mempercepat proses pemesanan produk kepada pelanggan. Untuk memecahkan permasalahan tersebut, masing-masing sales person akan menggunakan aplikasi sales order melalui perangkat *smartphone* yang akan membuat pemesanan produk. Dan data pemesanan produk akan masuk ke aplikasi berbasis web yang dijalankan admin untuk proses pembuatan invoice. Aplikasi ini dirancang menggunakan RESTful API yang merupakan salah satu model implementasi dari web service.Keamanan dalam hal pertukaran data pada aplikasi ini menggunakan *JSON Web Token*. Dengan adanya aplikasi sales order ini dapat mempermudah kinerja sales person dalam memasarkan produknya Aplikasi sales order ini berjalan baik pada web dan android sehingga proses pemesanan produk menjadi lebih mudah. Penggunaan autentifikasi json web token pada RESTful API ini membuat aplikasi menjadi lebih aman karena aplikasi tidak dapat diakses jika tidak menggunakan token.

5. **Arief Umarjati dan Arief Wibowo, Tahun 2020, Implementasi JWT pada Aplikasi Presensi dengan Validasi Fingerprint, Geotagging dan Device Checker.** Pada masa pandemi Covid-19 pemerintah membuat beberapa peraturan untuk mencegah penyebaran penyakit berbahaya tersebut. Salah satu kebijakan yang diterapkan adalah pemberlakuan Pembatasan Sosial Berskala Besar (PSBB). PSBB ini juga memberi dampak terhadap perusahaan-perusahaan di Jabodetabek termasuk PT Akses Digital Indonesia. Demi mematuhi peraturan yang diberikan pemerintah, PT Akses Digital Indonesia melakukan kebijakan Work From Home(WFH) bagi karyawannya. Selama diberlakukannya kebijakan WFH, PT Akses Digital Indonesia mengalami kesulitan untuk mengawasi kinerja dari para karyawan. Presensi adalah salah satu tolak ukur dari tingkat kinerja, terutama kedisplinan karyawan. Berdasarkan identifikasi masalah tersebut, diperlukan aplikasi web service presensi karyawan. Tentunya aplikasi ini diharuskan sama efektifnya dengan mesin fingerprint konvensional yang berada di kantor. Aplikasi ini disertai fitur validasi menggunakan geotagging, fingerprint dan device checker untuk meminimalisir adanya kecurangan saat karyawan melakukan presensi. Penelitian ini mengimplementasikan fitur keamanan RESTful API pada web services dengan menggunakan JSON Web Token (JWT) berbasis algoritma HMAC SHA-256. Seluruh tahap implementasi

diuji menggunakan metode Black Boxdan menunjukkan bahwa JWT dapat mengamankan proses autentikasi, melakukan proses request & response, dan pengamanan data. Selain itu, fitur validasi mampu memberikan data presensi dengan akurasi sebesar 90,9%..

6. **Madhiyono, Sandy Kosasi dan David, Tahun 2021, Implementasi JWT, Fingerprint Dan Algoritma Haversine Dalam Aplikasi Presensi Mahasiswa.** Sistem presensi selalu menjadi masalah baik bagi dosen maupun mahasiswa. Sistem presensi manual menggunakan lembaran yang kemudian ditandatangani oleh mahasiswa. Lembaran tersebut direkap oleh dosen setiap akhir semester yang membuat waktu dosen untuk menyiapkan materi berikutnya terbuang sia-sia. Pentingnya perubahan dan penyerderhanaan sistem presensi dapat membantu dosen juga mahasiswa dalam hal peringatan mengenai jumlah presensi. Aplikasi sistem presensi dikembangkan dengan metode prototype yang menerapkan JSON Web Token, fingerprint, dan QR Code sebagai keamanan dan keaslian data serta algoritma haversine untuk perhitungan jarak mahasiswa dengan universitas. Sistem presensi dapat diakses oleh dosen melalui website dan mahasiswa melalui mobile yang dihubungkan dengan penerapan web service berbasis REST API. Pengujian dari sistem presensi menggunakan metode black box dengan hasil hampir sesuai dengan yang diharapkan. Hasil dari penelitian ini adalah dengan diciptakannya aplikasi presensi selanjutnya dapat mempermudah dosen maupun mahasiswa dalam hal proses. Hasil dari penelitian ini juga dapat menjadi acuan untuk peneliti berikutnya mengembangkan sistem presensi.
7. **Novi Putri Octaviani, Rika Idmayanti, dan Cipto Prabowo, Tahun 2022, Aplikasi Jemput dan Donor Darah Dengan Teknologi Open Street Maps dan JWT Token Berbasis Android.** Perkembangan teknologi informasi untuk saat ini sangat pesat dan tengah mengarah pada perkembangan mobile. Dalam tugas akhir ini akan dibangun suatu aplikasi berbasis android yang berguna dalam dunia kesehatan karena membantu masyarakat yang kesulitan memperoleh pendonor dan melakukan pendaftaran untuk melakukan kegiatan donor darah, sehingga masyarakat tidak perlu mencari pendonor dengan memasang broadcast pada media sosial karena aplikasi telah membantu proses pencarian pendonor untuk melakukan donor darah. Aplikasi ini menggunakan Open Street Maps untuk mendapatkan alamat dari pendonor sehingga penerima dapat menjemput darah dan di bawa ke PMI, pada aplikasi juga menggunakan JWT Token untuk menyimpan session login dari setiap pengguna yang masuk ke dalam aplikasi. Aplikasi ini menggunakan koneksi

internet untuk berkomunikasi dengan server AWS yang sudah dipasang Mysql dan Apache di dalamnya. Aplikasi ini dibangun menggunakan bahasa pemrograman Java dan menggunakan penyimpanan data berupa Mysql. Untuk interaksi antara android dengan server dibangun sebuah API berbasis bahasa pemrograman PHP dengan metode PDO. Hasil tugas akhir ini akan menampilkan soal dan nilai yang didapatkan oleh siswa ketika selesai mengerjakan ujian pada aplikasi.

8. **Rezvan Mahdavi-Hezaveh, Jacob Dremann dan Laurie Williams, Tahun 2021, *Software development with feature toggles: practices used by practitioners*.** Menggunakan *Feature Toggle* adalah teknik yang memungkinkan pengembang untuk mengaktifkan atau menonaktifkan fitur dengan variabel dalam pernyataan bersyarat. Beralih fitur semakin banyak digunakan oleh perusahaan perangkat lunak untuk memfasilitasi integrasi berkelanjutan dan pengiriman berkelanjutan. Namun, menggunakan fitur beralih secara tidak tepat dapat menyebabkan masalah yang dapat berdampak parah, seperti kompleksitas kode, kode mati, dan kegagalan sistem. Misalnya, penggunaan kembali *Feature Toggle* lama yang salah menyebabkan Knight Capital Group, sebuah perusahaan jasa keuangan global Amerika, bangkrut karena implikasi dari perilaku sistem yang salah.
9. **Rezvan Mahdavi-Hezaveh, Nirav Ajmeri, dan Laurie Williams, Tahun 2022, *Feature toggles as code: Heuristics and metrics for structuring feature toggles*.** Menggunakan *Feature Toggle* adalah teknik untuk mengaktifkan atau menonaktifkan fitur dalam kode program dengan memeriksa nilai variabel dalam pernyataan bersyarat. Teknik ini semakin banyak digunakan oleh para praktisi perangkat lunak untuk mendukung *Continuous Integration* dan *Continuous Delivery* (CI/CD). Namun, menggunakan *Feature Toggle* dapat meningkatkan kompleksitas kode, membuat kode mati, dan menurunkan kualitas basis kode..
10. **Dita dan Wahyu Shabrina, Tahun 2020, Analisis Kinerja SECWSN berbasis RSA 2048 dan SHA1 Menggunakan Raspberry pi**. Sistem keamanan data merupakan salah satu masalah yang ada dalam jaringan Wireless Sensor Network (WSN). Berbagai serangan mencoba memanipulasi data pada jaringan WSN. Keamanan dan privasi data yang baik sangat diperlukan dalam jaringan WSN karena kondisi tersebut, maka dilakukan penelitian tentang kamanan pada jaringan WSN dengan memanfaatkan sistem kriptografi dan menyertakan fungsi hash. Sistem kriptografi merupakan sistem keamanan yang bertujuan untuk menjaga keaslian data dan keutuhan data

dengan memanfaatkan perhitungan matematika dalam bentuk key. Fungsi hash memiliki peran untuk memberikan keamanan tambahan dalam verifikasi data pada key. Dalam penelitian ini, fungsi hash akan digunakan pada sisi enkripsi dan dekripsi. Algoritma yang digunakan dalam penelitian ini menggunakan RSA2048 dan SHA-1. Raspberry Pi akan digunakan sebagai implementasi sistem kriptografi. Penelitian ini bertujuan untuk mengetahui bagaimana perbandingan kualitas keamanan pada jaringan WSN berdasarkan parameter QoS delay, dan packet loss standar ITU-T G 1010 menggunakan perangkat Raspberry Pi. Berdasarkan hasil penelitian ini diketahui bahwa perbandingan antara kedua perangkat Raspberry Pi memiliki delay dan packet loss yang baik. Hal ini ditunjukan dengan nilai delay 47.83812934 ms dan packet loss 1,61% pada perangkat Raspberry Pi A+ serta nilai delay 47.89845633 ms dan packet loss 0,72% pada perangkat Raspberry Pi B.

Berikut merupakan perbandingan dari tabel penelitian di bawah ini:

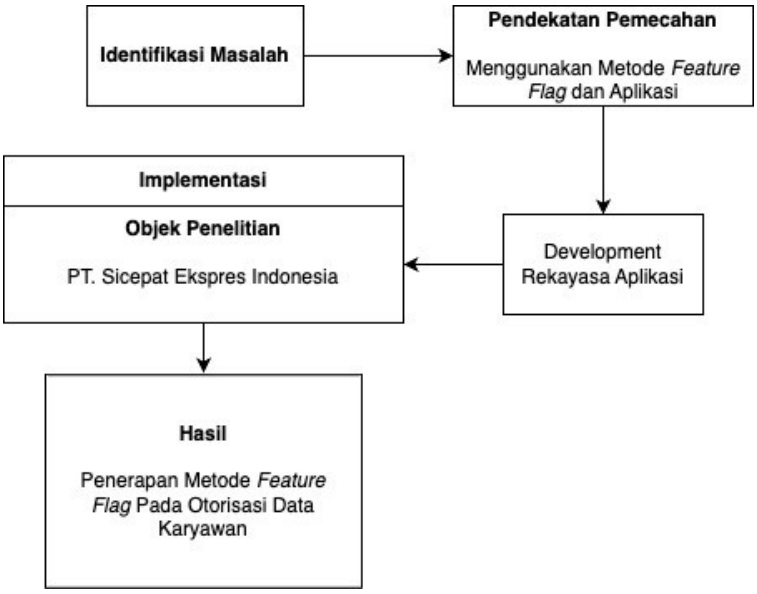
Tabel 0.1 Tinjauan Pustaka

No	Nama	Judul	Metode	Kontribusi
1	Rohmat Gunawan dan Alam Rahmatulloh, 2019	JSON Web Token (JWT) untuk Authentication pada Interoperabilitas Arsitektur berbasis RESTful Web Service	Menggunakan *JWT (JSON Web Token)*	Penggunaan JWT di Arsitektur Restful terhadap API dalam sebuah perusahaan.
2	Sopingi, Faulinda Ely Nastiti dan Arviyan Sofyan Majid, 2022	Implementasi JSON Web Token Authentication pada Aplikasi Pembayaran Berbasis Mobile	Menggunakan *JWT (JSON Web Token)*	Memperkuat kleamanan data mahasiswa yang disimpan di dalam aplikasi dan proses authentication pada setiap proses transaksi data antara aplikasi dengan web

No	Nama	Judul	Metode	Kontribusi
				service sistem keuangan
3	Pratama Abdul Karim dan Aditya, 2021	Pengujian Penetrasi Penyimpanan Token Menggunakan Cookie Storage Pada JSON WEB TOKEN	Menggunakan *JWT (JSON Web Token), CSRF,* dan *Brute Force*	Melakukan pengujian penetrasi keamanan penyimpanan JSON Web Token (JWT) pada penyimpanan cookie dengan menggunakan teknik CSRF dan Brute-Force
4	Edy, Ferdiansyah, Wahyu Pramusinto dan Sejati Waluyo, 2019	Pengamanan Restful API menggunakan JWT untuk Aplikasi Sales Order	Menggunakan *JWT (JSON Web Token)*	Mempercepat proses pemesanan produk kepada pelanggan
5	Arief Umarjati dan Arief Wibowo, Tahun 2020	Implementasi JWT pada Aplikasi Presensi dengan Validasi Fingerprint, Geotagging dan Device Checker	Menggunakan *JWT (JSON Web Token)*	Meminimalisir adanya kecurangan saat karyawan melakukan presensi
6	Madhiyono, Sandy Kosasi dan David, Tahun 2021	Implementasi JWT, Fingerprint Dan Algoritma Haversine Dalam Aplikasi Presensi Mahasiswa	Menggunakan *JWT (JSON Web Token)* dan Algoritma Haversine	Penyerderhanaan sistem presensi dalam website
7	Novi Putri Octaviani, Rika Idmayanti, dan Cipto	Aplikasi Jemput dan Donor Darah Dengan Teknologi Open Street Maps	Menggunakan *JWT (JSON Web Token)*	Membantu masyarakat yang kesulitan memperoleh pendonor

No	Nama	Judul	Metode	Kontribusi
	Prabowo, Tahun 2022	dan JWT Token Berbasis Android		
8	Rezvan Mahdavi-Hezaveh, Jacob Dremann dan Laurie Williams, Tahun 2021	*Software development with feature toggles: practices used by practitioners*	Menggunakan metode *Feature Flag*	Mengaktifkan atau menonaktifkan fitur dengan variabel dalam pernyataan bersyarat
9	Rezvan Mahdavi-Hezaveh, Nirav Ajmeri, dan Laurie Williams, Tahun 2022	*Feature toggles as code: Heuristics and metrics for structuring feature toggles*	Menggunakan metode *Feature Flag*	Mengaktifkan atau menonaktifkan fitur dengan variabel dalam pernyataan bersyarat
10	Dita dan Wahyu Shabrina, 2020	Keamanan Sistem *Wireless Sensor Network (WSN)*	Menggunakan algoritma SHA1 dan RSA 2048 dan *JWT (JSON Web Token)*	Membandingkan antara JWT dan Algoritma SHA1 Pada Implementasi Autentikasi

C. Kerangka Pemikiran



Gambar 0.1 Kerangka Pemikiran

Berdasarkan penelitian mengenai Penerapan Metode *Feature Flag* Pada Otorisasi Data Karyawan dibuat kerangka pemikiran dengan uraian sebagai berikut:

1. Identifikasi Masalah pada penelitian Penerapan Metode *Feature Flag* Pada Otorisasi Data Karyawan dibuat untuk menyelesaikan masalah belum tepatnya penerapan pengendalian atau kontrol dalam menampilkan informasi sensitif dan belum tepatnya proses otorisasi untuk mengakses informasi pada sistem informasi.
2. Pendekatan pemecahan pada penelitian dengan judul Penerapan Metode *Feature Flag* Pada Otorisasi Data Karyawan adalah Metode *Feature Flag* dan Aplikasi.
3. Development yang digunakan adalah Rekayasa Aplikasi.
4. Terdapat Model implementasi Objek Penelitian yang dilakukan di PT. Sicepat Ekspres Indonesia

D. Hipotesis Penelitian

Hipotesis berdasarkan rumusan masalah, maka hipotesis ini adalah penerapan metode *Feature Flag* di duga dapat menyelesaikan masalah dalam pengendalian informasi data karyawan pada sistem informasi