BAB III

METODOLOGI PENELITIAN

3.1 Analisis Permasalahan

Studi kasus pada penelitian ini yaitu pada kampus STMIK PPKIA Pradnya Paramita (STIMATA), tepatnya pada bagian Pusat Kordinasi Data (PUSKORDAT). PUSKORDAT adalah unit perguruan tinggi pada kampus STIMATA yang bertugas menyediakan basis data untuk menjalankan fungsi layanan data mahasiswa dan dosen.

SIAKAD di kampus STIMATA saat ini menggunakan aplikasi berbasis mobile bagi pengguna Dosen dan Mahasiswa. Kemudian aplikasi SIAKAD berbasis website yang digunakan oleh admin di PUSKORDAT.

Pada objek penelitian ini permasalahan yang dialami hingga saat ini yaitu sebagai berikut ini.

3.1.1 Tantangan Keamanan Terkait Kemajuan Teknologi Informasi

Kemajuan teknologi informasi telah mengubah lanskap pengelolaan data mahasiswa dengan memberikan keuntungan yang signifikan dalam hal efisiensi dan responsivitas. Namun, seiring dengan perkembangan ini, muncul pula tantangan serius terkait dengan keamanan data. Ancaman serangan siber dan kompleksitas celah keamanan menjadi fokus utama yang perlu ditangani. Dengan semakin meningkatnya ketergantungan pada sistem komputer dan jaringan, risiko terhadap keamanan data mahasiswa semakin besar. Ancaman-ancaman seperti pencurian data, perusakan sistem, dan penyanderaan informasi merupakan ancaman yang

dapat berdampak serius.

3.1.2 Peran Kritis Kinerja Sistem

Kinerja sistem adalah faktor kritis yang memainkan peran utama dalam memastikan efisiensi dan responsivitas optimal dalam pengolahan data. Sistem yang tidak berkinerja optimal dapat menjadi titik lemah yang mudah dimanfaatkan oleh serangan siber. Oleh karena itu, penting untuk memastikan bahwa kecepatan dan kehandalan sistem diprioritaskan. Kecepatan sistem menjadi faktor penting untuk meminimalkan potensi kesalahan atau keterlambatan dalam pengolahan data. Begitu juga, keandalan sistem diperlukan agar proses pengolahan data dapat berjalan secara mulus dan efektif tanpa gangguan yang tidak diinginkan.

Keberhasilan dalam menjaga kinerja sistem yang optimal tidak hanya berdampak pada efisiensi operasional institusi, tetapi juga memiliki implikasi langsung terhadap keamanan data. Sistem yang lambat atau tidak responsif dapat membuka celah bagi serangan siber untuk menyerang dan merusak integritas data. Bahkan, keterlambatan dalam pengolahan data dapat meningkatkan risiko terhadap berbagai jenis serangan siber yang berpotensi merugikan institusi secara finansial maupun reputasional.

3.1.3 Penataan Menu Aplikasi yang Mudah Digunakan

Pada aplikasi SIAKAD Mobile terdapat beberapa bagian yang kurang sesuai sehingga menyulitkan pengguna. Oleh karena itu perlu penataan ulang menunya agar mudah digunakan.

3.2 Solusi yang Diusulkan

Berdasarkan permasalahan yang telah di uraikan di atas maka penulis perlu memberikan solusi yang diusulkan. Adapun dalam penyelesaikan solusi ini menggunakan metode SDLC Model Waterfall, dengan langkah-langkah sebagai berikut.

3.2.1 Tahap Analisis

Pada tahap ini, penulis akan melakukan analisis terhadap kebutuhan (SIAKAD) di (STIMATA), yaitu dengna melakukan wawancara kepada bagaian yang bertanggung jawab aplikasi (SIAKAD) di (PUSKODAT). Selain itu juga melakukan observasi terhadap aplikasi (SIAKAD) yang dilakukan di kampus (STIMATA) jalan Laksda Adi Sucipto Nomor 249A Blimbing Malang, di gedung A lantai dua ruang (PUSKODAT).

Hal yang perlu dipelajari pada aplikasi (SIAKAD) adalah sebagai berikut :

a. Keamanan Aplikasi

   Analisis akan dilakukan untuk mengidentifikasi semua potensi ancaman keamanan yang mungkin terjadi terhadap aplikasi, termasuk identifikasi data sensitif dan kebijakan keamanan yang harus diterapkan.

b. Kecepatan Respons Aplikasi

   Pada tahap ini, akan dievaluasi kecepatan respons aplikasi untuk memastikan bahwa aplikasi memberikan pengalaman pengguna yang responsif dan tanpa hambatan.

3.2.2 Tahap Design

Setelah kebutuhan dan ruang lingkup SIAKAD dianalisis, tahap selanjutnya adalah perancangan desain aplikasi. Pada tahap ini, arsitektur aplikasi akan direncanakan dengan cermat untuk memastikan bahwa setiap komponen dapat berinteraksi secara efisien.

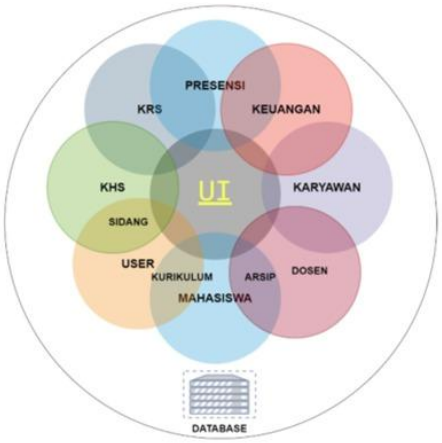
1) Arsitektur Sistem

Desain arsitektur sistem akan menetapkan kerangka kerja teknis dan infrastruktur aplikasi, termasuk pemilihan teknologi dan platform yang sesuai. Desain arsitektur sistem diantaranya sebagai berikut:

a. Indexing Query

Indeks ini berfungsi sebagai struktur data tambahan yang membantu mesin database untuk menemukan baris data yang relevan dengan lebih cepat tanpa harus memindai seluruh tabel. Dengan adanya indeks, query yang sebelumnya memerlukan waktu lama untuk diproses dapat dijalankan dengan lebih cepat, terutama pada tabel dengan jumlah data yang sangat besar.

Indeksing Query dilakukan terhadap database yang sudah tersedia dan masih digunakan di STIMATA. Gambar 3.1 merupakan Tabel-tabel dalam Database yang sudah digunakan.



Gambar 3. 1 Rancangan database

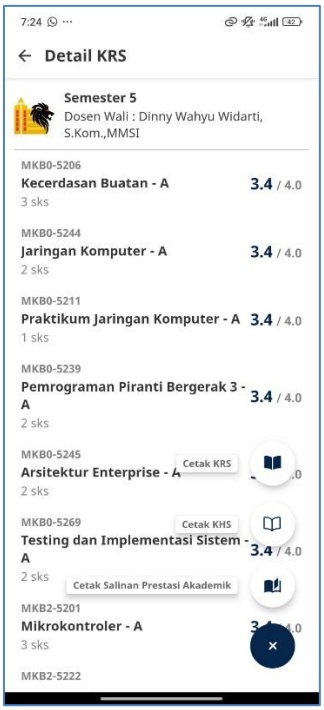
(Sumber: PUSKODAT)

b. JWT

JWT berfungsi untuk otentikasi dan otorisasi pengguna dalam aplikasi web. Setelah pengguna berhasil login, server membuat JWT yang berisi informasi seperti ID pengguna dan hak akses. Token ini digunakan untuk mengakses sumber daya tanpa perlu mengirim ulang kredensial. JWT mendukung otentikasi tanpa status (stateless) sehingga server tidak perlu menyimpan sesi pengguna. JWT juga memungkinkan pengiriman data yang aman dan mendukung komunikasi antar domain.

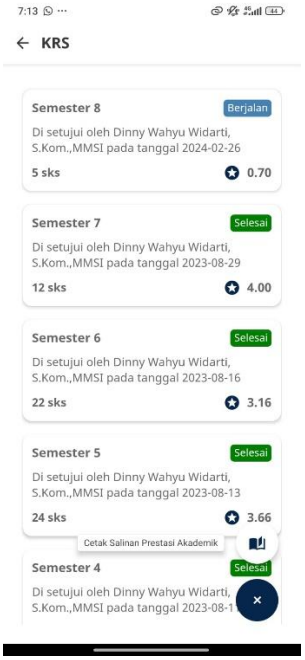
2) Antarmuka Pengguna

Pada gambar 3.2 merupakan antarmuka KRS di aplikasi SIAKAD mobile. Dimana tombol salinan nilai ada di dalam bagian detail KRS, hal ini perlu perbaikan dengan merubah tampilan agar mudah digunakan dalam pencariannya.



Gambar 3. 2 Detail KRS mahasiswa sebelum diperbaiki

Pada gambar 3.3 merupakan detail KRS yang telah diperbaiki sehingga user mudah untuk menemukan fitur cetak salinan prestasi akademik.



Gambar 3. 3 Detail KRS mahasiswa setelah diperbaiki

3.2.3 Tahap Implementasi

Tahap implementasi melibatkan pengembangan aplikasi berdasarkan rancangan yang telah dibuat sebelumnya. Tim pengembang akan mulai menulis kode menggunakan teknologi yang sudah ditetapkan seperti React Native, PHP, Laravel, dan JWT untuk implementasi keamanan.

1. Implementasi Keamanan dengan JWT

   Pada tahap ini, pengembang akan melakukan implementasi sistem keamanan menggunakan JSON Web Token JWT sebagai mekanisme otentikasi dan otorisasi pengguna. JWT adalah sebuah standar terbuka (RFC 7519) yang mendefinisikan cara yang aman untuk mentransfer informasi antara pihak-pihak dalam bentuk JSON. Dengan menggunakan JWT, pengguna akan mendapatkan token yang berisi informasi otentikasi mereka setelah berhasil login. Token ini akan digunakan untuk mengidentifikasi pengguna dan memberikan akses terhadap fitur-fitur tertentu dalam aplikasi.

   Selain itu, JWT juga memungkinkan pengembang untuk menerapkan mekanisme otorisasi yang lebih kompleks, seperti penentuan peran pengguna dan hak akses yang terkait. Dengan mengimplementasikan JWT, keamanan aplikasi akan ditingkatkan karena informasi otentikasi pengguna akan dienkripsi dan divalidasi secara aman.

2. Peningkatan Kecepatan dengan Clean Code dan Clean Query

   Dalam tahap ini, pengembang akan menulis kode dengan standar yang tinggi dan efisien untuk memastikan kinerja aplikasi yang optimal. Konsep "clean code" merujuk pada praktik menulis kode yang mudah

dipahami, dipelihara, dan diperluas. Hal ini mencakup penggunaan nama variabel yang deskriptif, pembagian kode menjadi fungsi-fungsi yang terpisah, serta penggunaan komentar yang jelas dan konsisten.

Selain itu, "clean query" mengacu pada teknik penulisan query database yang efisien dan optimal. Ini termasuk penggunaan indeks yang tepat, penghindaran penggunaan fungsi-fungsi yang membebani kinerja, dan pengoptimalan struktur query agar dapat dieksekusi dengan cepat. Dengan menerapkan prinsip clean code dan clean query, pengembang dapat meningkatkan kecepatan aplikasi dengan mengurangi beban kerja pada server dan mempercepat proses eksekusi kode. Ini akan menghasilkan pengalaman pengguna yang lebih responsif dan memuaskan, serta mengurangi kemungkinan terjadinya bottleneck dalam aplikasi.

3.2.4 Tahap Testing

Pengujian adalah tahap penting untuk memastikan kualitas dan kinerja aplikasi sebelum dirilis ke pengguna.

1. Pengujian Keamanan dengan Postman

   Metode pengujian ini akan menggunakan Postman sebagai Penguji Keamanan Otomatis untuk memverifikasi integritas dan keamanan sistem keamanan yang diimplementasikan menggunakan JWT. Postman akan digunakan untuk mengirimkan permintaan ke aplikasi dan memeriksa responnya untuk memastikan bahwa mekanisme otentikasi dan otorisasi yang diimplementasikan berfungsi dengan benar.

Selain itu, Postman juga akan digunakan untuk mengidentifikasi potensi celah keamanan yang mungkin ada dalam aplikasi. Dengan menggunakan Postman sebagai alat pengujian, tim pengembangan dapat memastikan bahwa aplikasi terlindungi secara optimal dari serangan siber dan kebocoran data.

2. Pengujian Responsif

Metode pengujian responsif waktu ini bertujuan untuk mengevaluasi seberapa cepat sistem merespons permintaan dari pengguna dalam berbagai kondisi beban dan lingkungan. Pengujian ini akan memeriksa waktu tanggapan aplikasi untuk memastikan bahwa sistem dapat memberikan respons yang cepat dan konsisten, baik dalam kondisi normal maupun saat terjadi lonjakan permintaan.

Pengujian ini dilakukan dengan mengukur waktu yang dibutuhkan oleh aplikasi untuk memproses permintaan dan mengirimkan respon kembali ke pengguna. Alat-alat seperti Postman dapat digunakan untuk mensimulasikan berbagai skenario permintaan, termasuk permintaan secara simultan dalam jumlah besar. Dengan demikian, tim pengembangan dapat mengidentifikasi potensi masalah yang mungkin menyebabkan keterlambatan dalam respon dan melakukan optimisasi yang diperlukan untuk memastikan bahwa aplikasi tetap responsif dan memberikan pengalaman pengguna yang optimal, bahkan di bawah beban yang berat.

3. Pengujian Antar Muka

Metode pengujian antarmuka ini melibatkan pengujian

langsung pada perangkat fisik untuk memastikan bahwa tampilan dan fungsionalitas antarmuka pengguna (UI) berfungsi dengan baik di berbagai jenis perangkat seperti smartphone, tablet, dan desktop. Pengujian ini bertujuan untuk memverifikasi bahwa elemen-elemen UI, seperti tombol, menu, dan formulir, tampil dengan benar dan dapat dioperasikan dengan baik pada perangkat dengan berbagai ukuran layar dan resolusi.

Dalam pengujian ini, aplikasi akan diuji secara manual pada perangkat yang berbeda untuk melihat bagaimana tampilan dan interaksinya langsung di layar perangkat. Pengujian langsung ini sangat penting untuk mendeteksi masalah yang mungkin tidak teridentifikasi dalam simulasi atau pengujian otomatis, sehingga memastikan bahwa aplikasi memberikan pengalaman pengguna yang optimal di berbagai perangkat nyata.

3.2.5 Tahap Deployment

Setelah berhasil melewati tahap pengujian, aplikasi siap untuk dirilis ke lingkungan produksi. Tahap ini melibatkan proses perilisan aplikasi yang sudah melalui serangkaian pengujian dan review oleh beberapa pengguna untuk memastikan kualitasnya sebelum diluncurkan ke publik.

3.2.6 Tahap Maintenance

Tahap pemeliharaan adalah tahap terakhir dalam siklus pengembangan perangkat lunak. Tim akan terus memonitor kinerja aplikasi, merespons masukan dari pengguna, dan melakukan pemeliharaan rutin serta peningkatan sesuai

kebutuhan untuk menjaga agar aplikasi tetap berjalan dengan lancar dan memenuhi kebutuhan pengguna secara berkelanjutan.

3.3 Rancangan Eksperimen

Bagian ini merinci rancangan eksperimen yang akan dilakukan dalam penelitian. Eksperimen ini bertujuan untuk mengumpulkan data yang relevan untuk menjawab pertanyaan penelitian atau menguji hipotesis yang diajukan. Rancangan eksperimen mencakup semua langkah yang diperlukan untuk menyusun dan melaksanakan eksperimen dengan cermat dan terkontrol.

3.3.1 Kebutuhan Perangkat

Peralatan yang digunakan untuk mengimplementasikan penelitian ini terdapat beberapa komponen sebagai berikut:

1. Perangkat Keras (*Hardware*)
    a. Laptop Lenovo Thinkpad X1 Carbon
    b. Intel i7 – 6600u
    c. Ram 16Gb
2. Perangkat Lunak (*Software*)
    a. Windows 10
    b. Visual Studio Code
    c. Laragon
    d. React Native
    e. NodeJs
    f. Android SDK

g. PHP

h. Postman

3.3.2 Kebutuhan Data

Bagian ini menyoroti aspek penting dalam penelitian, yaitu kebutuhan akan data yang digunakan sebagai bahan pengujian atau analisis. Dalam konteks ini, data yang diperlukan berasal dari dua sumber utama, yaitu data mahasiswa dari angkatan 2000 hingga 2023 dan data terbaru mengenai dosen serta data aktivitas kuliah.

Data mahasiswa ini mencakup berbagai informasi yang relevan seperti nama, nomor induk mahasiswa (NIM), program studi, nilai, dan informasi lain yang mungkin diperlukan untuk analisis. Sedangkan data dosen mencakup informasi terbaru mengenai dosen yang terlibat dalam proses pendidikan, seperti nama, jabatan, bidang keahlian, dan lain sebagainya. Data aktivitas kuliah dimulai dari data sebaran matakuliah, kartu rencana studi dan kartu hasil studi dari tahun 2020 hingga 2023. Dengan memiliki akses ke data yang relevan dan berkualitas, penelitian dapat dilakukan dengan lebih baik, memastikan validitas dan keakuratan analisis yang dilakukan serta mendukung pembuatan kesimpulan yang kuat dan dapat diandalkan. Oleh karena itu, pemilihan data yang tepat dan pemahaman mendalam tentang sumber data menjadi kunci untuk kesuksesan penelitian ini.

3.3.3 Parameter Pengujian

Terdapat beberapa parameter yang dapat digunakan untuk menguji keefektifan sistem yang telah dikembangkan dalam menyelesaikan masalah, antara lain:

1. Persepsi Pengguna terhadap Kinerja Aplikasi
    a. Peningkatan dalam persepsi pengguna terhadap kecepatan dan responsivitas sistem.
    b. Penilaian pengguna terhadap kemudahan penggunaan aplikasi.
    c. Tingkat kepuasan pengguna terhadap pengalaman menggunakan aplikasi.
2. Kemampuan Autentikasi dan Otorisasi
    a. Kemampuan sistem untuk memfasilitasi pengguna dalam melakukan autentikasi menggunakan kredensial pengguna lain.
    b. Fungsionalitas otorisasi sistem yang memungkinkan pengguna untuk mengakses sumber daya atau fitur yang sesuai dengan peran pengguna yang ditetapkan.
3. Keamanan Data
    a. Evaluasi tingkat keamanan sistem terhadap ancaman siber yang mungkin terjadi, termasuk serangan peretasan dan pencurian data.
    b. Implementasi protokol keamanan yang kuat seperti enkripsi data dan kontrol akses yang ketat untuk melindungi integritas dan kerahasiaan informasi mahasiswa.
    c. Pengujian sistem terhadap berbagai serangan siber untuk memastikan keandalan dan keamanan sistem secara menyeluruh.

3.3.4 Indikator Keberhasilan

Indikator keberhasilan adalah parameter atau metrik yang digunakan untuk mengukur pencapaian tujuan atau hasil dari suatu proyek atau inisiatif. Indikator ini membantu dalam menilai apakah suatu proyek telah mencapai hasil yang

diharapkan atau belum, serta memberikan gambaran tentang efektivitas implementasi solusi yang telah dirancang.

1. Ketersediaan Sistem

   Ketika aplikasi dapat diakses oleh pengguna tanpa ada kendala atau gangguan yang signifikan.

2. Keamanan Data
   a. Ketika sistem berhasil melindungi data mahasiswa dari akses yang tidak sah atau upaya peretasan.
   b. Ketika data mahasiswa tersimpan secara aman dan terenkripsi di dalam database.

3. Responsivitas Aplikasi:

   Ketika waktu respons aplikasi tetap di bawah batas yang telah ditetapkan, kurang dari 1000 milidetik.

4. Fungsionalitas:
   a. Ketika semua fitur yang direncanakan dalam aplikasi dapat berfungsi dengan baik dan sesuai dengan kebutuhan pengguna.
   b. Ketika pengguna dapat melakukan operasi seperti pendaftaran, pengambilan data mahasiswa, dan manajemen akun dengan lancar.

3.3.5 Lingkup Pengujian

Lingkup Pengujian merujuk pada batasan dan ruang lingkup pengujian yang akan dilakukan terhadap aplikasi atau sistem yang dikembangkan. Ini mencakup parameter-parameter pengujian seperti fungsionalitas aplikasi, kinerja sistem, keamanan data, kompatibilitas perangkat, serta kesesuaian dengan kebutuhan dan

harapan pengguna.

1. Pengujian Fungsionalitas
    a. Verifikasi fungsi-fungsi utama sistem yang mencakup pengelolaan data mahasiswa, pendaftaran, dan manajemen akun pengguna.
    b. Pengujian interaksi antarmuka pengguna untuk memastikan navigasi yang intuitif dan fungsionalitas yang sesuai dengan kebutuhan pengguna.
2. Pengujian Kinerja
    a. Evaluasi kinerja sistem dalam menangani beban kerja yang signifikan untuk memastikan responsivitas yang baik dalam kondisi beban tinggi.
    b. Pengukuran waktu respons aplikasi dan throughput untuk menilai kecepatan dan efisiensi pengolahan data.
3. Pengujian Keamanan
    a. Pengujian kerentanan terhadap serangan siber seperti SQL injection, XSS (Cross-Site Scripting), dan serangan brute force pada sistem autentikasi.
    b. Verifikasi implementasi protokol keamanan seperti SSL/TLS untuk melindungi komunikasi data.
4. Pengujian Kompatibilitas
    a. Pengujian aplikasi pada berbagai perangkat dan platform untuk memastikan kompatibilitas lintas platform yang baik.
    b. Verifikasi dukungan aplikasi pada berbagai jenis peramban web dan perangkat seluler yang umum digunakan.
5. Pengujian Penyelarasan dengan Kebutuhan Pengguna
    a. Pengujian terhadap fitur-fitur aplikasi untuk memastikan kesesuaian dengan kebutuhan dan harapan pengguna.

b. Pengujian navigasi antarmuka pengguna untuk memastikan pengalaman pengguna yang optimal dan mudah dipahami.

3.4 Benang Merah

Sistem Informasi Akademik (SIAKAD) merupakan salah satu elemen penting dalam pengelolaan data mahasiswa dan kegiatan akademik di lingkungan pendidikan tinggi. Namun, seiring dengan meningkatnya kompleksitas data dan ancaman keamanan siber, tantangan terhadap kinerja dan keamanan SIAKAD menjadi semakin signifikan.

Penelitian ini bertujuan untuk mengoptimalkan kinerja dan keamanan SIAKAD melalui penerapan teknik optimalisasi kueri (query optimization) dan praktik pengkodean aman (secure coding practices) menggunakan JWT. Penelitian ini dilakukan dengan menganalisis permasalahan kinerja dan keamanan pada SIAKAD di STMIK PPKIA Pradnya Paramita. Pengoptimalan kueri diterapkan untuk meningkatkan efisiensi pengambilan dan pengelolaan data mahasiswa, sementara penggunaan JWT bertujuan untuk memastikan integritas dan kerahasiaan data selama proses autentikasi dan pengiriman. Melalui eksperimen dan pengujian, hasil penelitian menunjukkan bahwa teknik optimalisasi kueri mampu meningkatkan kecepatan respon sistem secara signifikan. Selain itu, implementasi JWT berhasil mengurangi risiko serangan siber dan meningkatkan keamanan data.

Dengan hasil yang diperoleh, penelitian ini diharapkan dapat memberikan kontribusi praktis bagi lembaga pendidikan dalam meningkatkan kinerja dan keamanan SIAKAD, serta memberikan panduan bagi pengembang sistem dalam menghadapi tantangan serupa. Melalui pendekatan holistik ini, lembaga pendidikan dapat menjalankan operasional akademiknya dengan lebih efisien dan aman, sehingga memberikan pengalaman belajar yang lebih baik bagi mahasiswa dan staf.