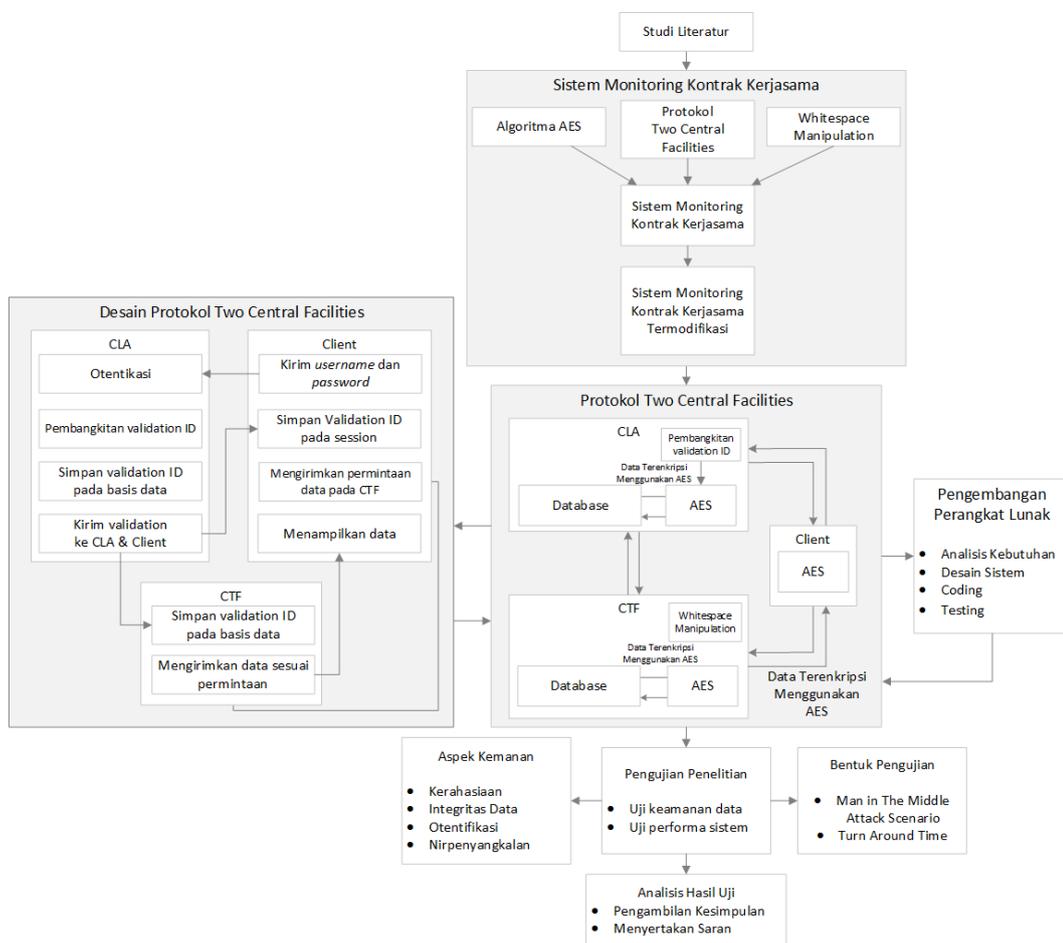


BAB III METODE PENELITIAN

3.1 Desain Penelitian

Bagian ini akan memberikan gambaran alur penelitian yang akan dijalani dalam melaksanakan penelitian ini. Tahapan penelitian ditampilkan pada gambar 3.1.



Gambar 3.1 Skema Desain Penelitian

Tahapan dari penelitian yang akan dilakukan meliputi langkah-langkah berikut:

Caesar Firdaus, 2016
**SISTEM MONITORING KONTRAK KERJASAMA DENGAN PROTOKOL TWO CENTRAL FACILITIES
 MENGGUNAKAN ALGORITMA AES DAN WHITESPACE MANIPULATION**
 Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

a. Studi Literatur

Pada tahap ini akan dipelajari algoritma kriptografi dan steganografi yang hendak diimplementasikan serta hal-hal yang mendukung terhadap kelangsungan penelitian. *Cryptography and Network Security Principle* karya William Stallings memberikan gambaran terhadap urgensi serta hal-hal esensial yang mesti dipenuhi dalam keamanan jaringan. Sumber ini juga memberikan informasi seputar algoritma AES, yang memiliki peranan penting dalam penelitian ini sebagai faktor keamanan.

Di samping buku karya William Stallings, Alfred J. Menezes dengan bukunya *Handbook of Applied Cryptography* turut dijadikan sumber pengetahuan yang solid untuk membantu membentuk pemahaman dasar dalam keamanan jaringan.

Selain itu, berbagai jurnal penunjang hasil dari penelitian yang berkaitan dengan penelitian ini turut dijadikan sebagai referensi.

b. Modifikasi Sistem Monitoring Kontrak Kerjasama

Modifikasi terhadap sistem monitoring kontrak kerjasama dilakukan dengan menyertakan *protokol two central facilities*, AES, *Information Hiding*, dan *Whitespace Manipulation*. Protokol *two central facilities* akan digunakan agar sistem hanya dapat melayani para *user* yang terdaftar serta memiliki hak akses untuk menggunakan sistem monitoring tersebut. Sedangkan algoritma *Whitespace Manipulation* digunakan untuk menyisipkan informasi bahwa berkas PDF yang dikirimkan adalah benar-benar dikeluarkan oleh pihak perusahaan serta menjaga integritas data berkas PDF tersebut. Pada sisi pengiriman data akan digunakan algoritma AES. Seperti yang telah diungkapkan pada bagian sebelumnya algoritma ini memiliki tingkat keamanan yang baik dan cocok untuk diimplementasikan pada aplikasi yang membutuhkan pengamanan lebih. Hasil dari tahap ini adalah rancangan sistem monitoring kontrak kerjasama termodifikasi.

c. Pengembangan Perangkat Lunak

Tahap pengembangan sistem dilakukan berdasarkan metode sekuensial linear yang terdiri dari tahap *analysis*, *design*, *coding*, dan *testing*. Sedangkan tahap dokumentasi akan dijalankan secara paralel seiring dengan dijalankannya ke 4 tahap yang telah disebutkan sebelumnya. Hal ini dilakukan agar dokumentasi benar-benar menggambarkan dinamika pengembangan serta manual dari perangkat lunak yang dibangun.

d. Pengujian Teori

Pada tahap ini, berbagai teori yang telah disertakan akan diuji kebenarannya. Hasil pengujian ini akan menjawab rumusan masalah.

e. Penulisan Hasil Penelitian Tahap Akhir

Pada tahap ini, kesimpulan serta saran akan dituliskan dan menandakan bahwa penelitian telah mencapai tahap akhir.

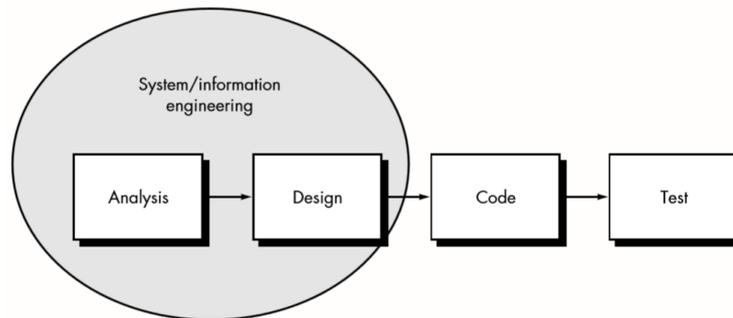
3.2 Metode Penelitian

3.2.1 Metode Pengumpulan Data

Penelitian ini akan mengumpulkan berbagai dokumen yang mendukung jalannya penelitian bersumber dari jurnal, karya ilmiah, buku, dan sumber lainnya yang terdapat di internet. Keabsahan dari informasi yang dicantumkan akan lebih dahulu ditelusuri guna menjamin keabsahan informasi yang dikandung.

3.2.2 Proses Pengembangan Perangkat Lunak

Dalam pembangunan perangkat lunak dalam penelitian ini, digunakan model sekuensial linier. Pendekatan dengan alur sistematis ini diperkenalkan oleh Winston Royce pada tahun 1970 (Pressman, 2001). Alur dari pendekatan linear sekuensial ditunjukkan pada gambar 3.2.



Gambar 3.2 Model Sekuensial Linier

Sumber: Pressman, 2001

System/information engineering dimulai dengan menentukan kebutuhan untuk semua elemen sistem lalu mengelompokkan kebutuhan tersebut ke kelompok yang lebih kecil sebagai kebutuhan perangkat lunak. Hal ini penting agar masing-masing komponen dapat berinteraksi dengan komponen lainnya.

Kegiatan analisis ditujukan pada perangkat lunak, sehingga dapat dipahami bagaimana program akan berjalan, fungsi apa saja yang dibutuhkan, bagaimana tingkah lakunya, performa, dan antarmukanya.

Pada tahap desain perhatian difokuskan pada 4 atribut penting dalam program, yaitu: struktur data, arsitektur, antarmuka, dan detail prosedur/algoritma. Pada tahap ini requirement diubah menjadi bentuk yang mewakili perangkat lunak yang dikembangkan.

Coding merupakan tahap dimana semua hasil perencanaan diterjemahkan ke dalam bahasa pemrograman, jika tahap desain diselesaikan dengan baik serta prosedur yang diperlukan terdokumentasi secara detail, maka tahap ini akan berjalan tanpa masalah.

Setelah kegiatan *coding*, maka dimulailah *testing*. Fungsi logis dari perangkat lunak akan dites sehingga dapat diketahui apakah sudah menghasilkan hasil yang sesuai atau membutuhkan perbaikan.

Tahap terakhir adalah support. Saat perangkat lunak sudah berpindah tangan ke klien maka perlu dilakukannya kegiatan pemeliharaan bersifat periodik untuk menjamin bekerjanya perangkat lunak sebagaimana mestinya.

3.3 Alat dan Bahan

Pada penelitian ini digunakan alat penelitian berupa perangkat keras dan perangkat lunak sebagai berikut:

a. Perangkat Keras

Kebutuhan perangkat keras yang digunakan adalah:

Prosesor : Intel Core i3-2348M 2.3 GHz

Memori : 4 GB RAM DDR3

Kapasitas HDD : 500 GB

b. Perangkat Lunak

Perangkat lunak hasil penelitan akan berjalan pada Sistem Operasi Windows 10 Pro 64 bit. Perangkat lunak pendukung lainnya yaitu *web browser*, *text editor*, *wireshark*, dan Oracle VM VirtualBox

Bahan penelitian yang digunakan adalah jurnal, *textbook*, *tutorial*, dan dokumentasi lainnya yang didapat melalui observasi di perpustakaan dan *World Wide Web* tentang keamanan data, protokol *two central facilities*, algoritma AES dan *digital watermark*.