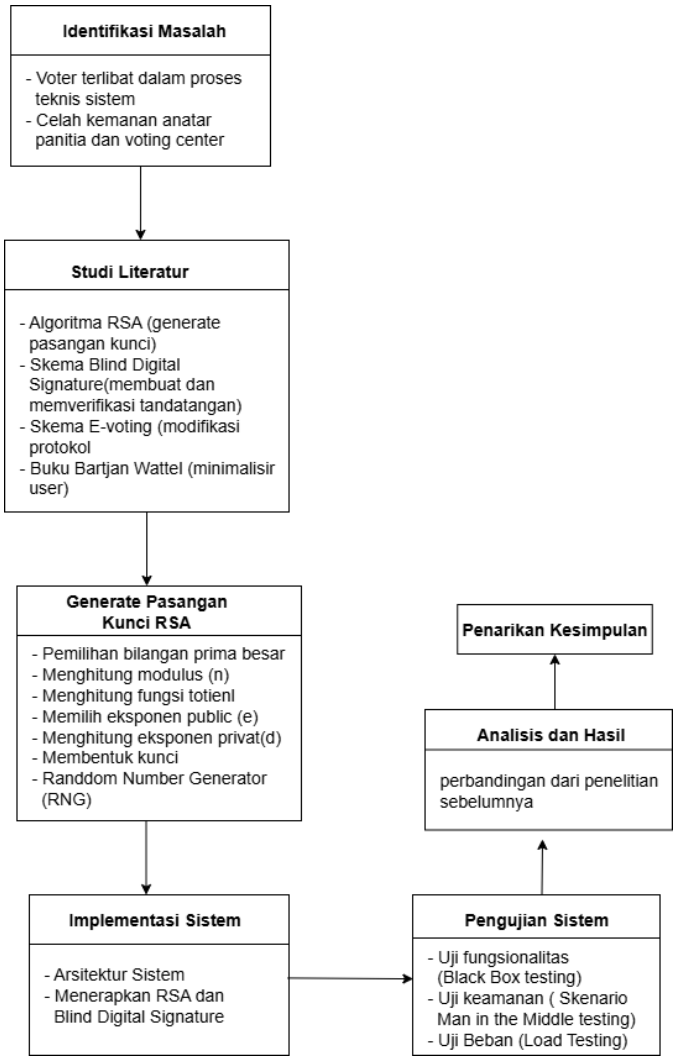
BAB III
METODOLOGI PEELITIAN

Untuk merangkum proses dalam penelitian ini akan dijelaskan pada desain penelitian sebagai berikut.

3.1 Desain Penelitian

Desain penelitian merupakan suatu tahapan yang dilakukan untuk memberikan kemudahan dalam melakukan penelitian. Desain penelitian ini ditujukan untuk mengetahui alur dalam penelitian sebagai panduan dan petunjuk yang terstruktur.



Gambar 3.1 Desain Penelitian

Penjelasan detail mengenai tahapan yang dilakukan selama penelitian adalah sebagai berikut:

1. Identifikasi Masalah

   Pada tahap identifikasi masalah dilakukan analisis terhadap penelitian sebelumnya untuk menemukan kelemahan yang ada. Ditemukan bahwa voter masih terlibat dalam proses teknis sistem, serta terdapat celah keamanan pada komunikasi antara panitia dan *voting center* yang berpotensi dimanfaatkan pihak ketiga. Dari masalah tersebut, penelitian ini difokuskan pada bagaimana meminimalisir peran teknis voter dan menutup celah keamanan tersebut.

2. Studi Literatur

   Studi literatur dilakukan untuk memperoleh dasar teori yang digunakan dalam penelitian. Literatur yang dipelajari meliputi algoritma RSA untuk menghasilkan pasangan kunci, skema *Blind Digital Signature* untuk proses pembutaan dan verifikasi tanda tangan, skema *e-voting* yang dimodifikasi agar lebih aman, serta referensi lain yang menekankan pentingnya meminimalisir peran teknis user.

3. Generate Pasangan Kunci *RSA*

   Generate pasangan kunci dibutuhkan untuk menghasilkan pasangan kunci yang akan digunakan untuk mengahsilkan *digital signature* selama proses *e-voting*, kunci tersebut terdiri dari kunci private dan kunci public. Kunci privat digunakan untuk menghasilkan tandatangan dan kunci public untuk memverifikasi tanda tangan, pasangan kunci ini akan di *generate* menggunakan *library OpenSSl* (Thangavel, Varalakshmi, Murrali, & Nithya, 2015). Berikut mekanismenya :

1) Pemilihan Bilangan Prima Besar

   OpenSSL pertama-tama membangkitkan dua bilangan prima besar secara acak, sebut saja p dan q. Bilangan ini dipilih dengan algoritma *probabilistik* (seperti *Miller-Rabin primality test*) supaya cepat tapi tetap sangat kecil peluangnya salah.

2) Menghitung Modulus (n**)**

   Dihitung nilai n = p × q. Nilai n ini nanti dipakai sebagai bagian dari kunci publik dan privat. Besarnya n (misalnya 2048 bit) yang menentukan "kuat tidaknya" kunci RSA.

3) Menghitung Fungsi Totien (φ)

   Hitung φ(n) = (p-1) × (q-1). Ini penting untuk menentukan kunci enkripsi dan dekripsi.

4) Memilih Eksponen Publik (e)

   OpenSSL memilih angka e yang relatif kecil tapi coprime dengan φ(n). Biasanya dipilih 65537 (0x10001) karena: cukup aman, cepat saat enkripsi/verifikasi sudah jadi standar de facto.

5) Menghitung Eksponen Privat (d)

   Cari nilai d sehingga: $d \times e \equiv 1 \pmod{\varphi(n)}$ $d \times e \equiv 1 \pmod{\varphi(n)}$ Dengan kata lain, d adalah inverse modular dari e terhadap φ(n). Nilai d ini hanya disimpan di kunci privat.

6) Membentuk Kunci

   - Kunci Publik = pasangan (n, e)
   - Kunci Privat = pasangan (n, d) dan juga menyimpan p dan q untuk optimasi perhitungan.

7) Random Number Generator (RNG**)**

Semua bilangan (terutama p dan q) dibangkitkan dari *cryptographically secure random number generator* yang ada di OpenSSL. Jadi setiap kali generate kunci, hasilnya beda-beda meskipun sama panjang bitnya.

4. Implementasi Sistem

Implementasi sistem dilakukan dengan mendesain alur *e-voting* yang terdiri dari entitas *voter*, panitia, dan *voting center*. Pada tahap ini juga dirancang integrasi algoritma RSA dengan *Blind Digital Signature* agar sistem mampu menjamin keamanan, privasi, dan keaslian suara, sekaligus meminimalkan keterlibatan teknis dari *voter* dan modifikasi protokol sistem *e-voting*.

5. Pengujian Sistem

Pengujian dilakukan untuk memastikan sistem berjalan sesuai harapan. Pengujian fungsional menggunakan metode *black box testing*, sementara pengujian keamanan dilakukan dengan skenario serangan *man in the middle*. Melalui pengujian ini diharapkan sistem mampu mendeteksi dan menolak manipulasi data yang terjadi selama proses komunikasi antar entitas.

6. Analisis dan Hasil

Hasil pengujian dianalisis dengan membandingkan penelitian ini terhadap penelitian sebelumnya. Analisis menunjukkan bahwa sistem mampu menutupi kekurangan dari protokol sebelumnya.

7. Penarikan Kesimpulan

Tahap akhir adalah penarikan kesimpulan berdasarkan hasil analisis dan pengujian dengan cara membandingkan hasil analisa dan evaluasi pengujian dengan rumusan masalahdan tujuan penelitian.

3.2 Alat dan Bahan

Dalam penelitian ini dibutuhkan beberapa alat dan bahan untuk menunjang keberhasilan penelitian yaitu sebagai berikut:

3.2.1 Alat Penelitian

Pada penelitian ini digunakan berbagai alat bantu untuk menunjang penelitian berupa perangkat keras dan perangkat lunak. Adapun perangkat keras yang digunakan adalah sebagai berikut:

1. Laptop Lenovo ideapad
2. Processor intel(R) Celeron(R) N4000 CPU
3. RAM 4GB
4. Mouse

Sementara perangkat lunak yang dibutuhkan adalah :

1. Laravel, PHP
2. MySQL
3. OpenSSL
4. Visual Studio Code
5. XAMPP

3.2.2 Bahan Penelitian

Bahan penelitian yang digunakan dalam penelitian ini adalah penelitian sebelumnya dan jurnal terkait yang memiliki topik serupa, tutorial, video dan dokumentasi lainnya yang didapat melalui observasi di perpustakaan dan *World Wide Web* tentang *digital signature*, *blind digital signature*, algoritma RSA, dan lain-lain.