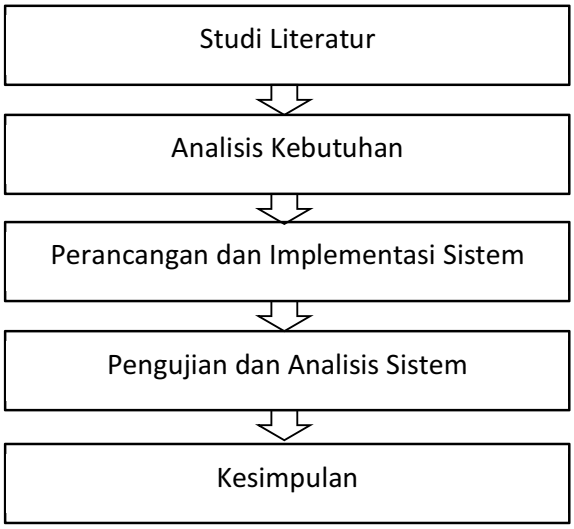
BAB 3 METODOLOGI

Dalam bab ini akan dijelaskan tentang cara sistematik yang akan digunakan untuk menyelesaikan masalah penelitian dan juga tahapan yang dilakukan dalam pengujian dan analisis dari algoritma *hash* SHA-1 dan SHA-3. Tahapan-tahapannya terdiri dari studi literatur, analisis kebutuhan, perancangan sistem, implementasi sistem, pengujian dan analisis sistem, dan kesimpulan. Tahapan-tahapan tersebut digambarkan pada Gambar 3.1.



Gambar 3.1 Diagram blok metodologi penelitian

3.1 Studi literatur

Ada beberapa hal yang harus dipelajari untuk mendukung penelitian tentang pengujian algoritma *hash* SHA-1 dan SHA-3 ini. Literatur diperoleh dari jurnal, buku dan internet. Literatur yang dipelajari adalah tentang:

a. Algoritma *hash* SHA-1

b. Algoritma *hash* SHA-3

3.2 Analisis kebutuhan

Untuk melakukan pengujian dalam penelitian ini, penulis menggunakan beberapa *hardware* dan *software*. Dalam bagian ini akan dijelaskan semua kebutuhan dan perancangan *software* dan *hardware* yang digunakan untuk pengujian.

3.3 Perancangan dan implementasi sistem

3.3.1 Perancangan sistem

Pada bagian perancangan ini penulis sudah melakukan analisis pada arsitektur awal sistem dikarenakan untuk mengembangkan sistem ini nantinya akan mengikuti arsitektur awal sistem yang sudah dikembangkan sebelumnya. Pertama penulis akan menggambarkan arsitektur awal sistem, kemudian dilakukan perancangan arsitektur yang akan dikembangkan dengan menerapkan algoritma SHA-3 pada mekanisme autentikasinya.

3.3.2 Desain tampilan

Pada bagian ini akan dijelaskan tentang rancangan tampilan yang akan digunakan pada saat implementasi nanti. Tampilan yang akan diimpelementasikan meliputi halaman *login,* halaman penambahan pengguna baru dan perubahan *password* pengguna.

3.3.3 Implementasi sistem

Pada bagian ini akan dijelaskan *pseudocode* dari beberapa potongan kode program yang berhubungan dengan mekanisme keamanan yang akan diuji, yaitu *hash password* SHA-1 dan SHA-3. Penerapannya akan dilakukan pada bagian *login,* penambahan pengguna baru dan perubahan *password* pengguna.

3.4 Pengujian dan analisis

Setelah selesai dilakukan perancangan dan analisis sistem, barulah dilakukan pengujian terhadap algoritma yang telah diterapkan tersebut. Kemudian dilakukan analisis manakah algoritma memiliki yang kinerja dan keamanan yang paling baik. Bagaimana kinerja keduanya ketika dibandingkan, apakah kelebihan dan kekurangannya.

3.4.1 Parameter pengujian

Parameter yang digunakan untuk menguji kedua algoritma *hash* yaitu SHA-1 dan SHA-3 pada penelitian ini ada 3. Yang pertama adalah waktu yang ditempuh pada saat melakukan *brute-force testing* pada kedua algoritma. Kemudian pengujian *avalanche effect* pada kedua algoritma. Dan yang terakhir yaitu waktu yang dibutuhkan saat proses *login*.

3.4.2 Skenario pengujian

Pada bagian ini akan ditentukan beberapa variasi skenario pengujian yang akan digunakan pada penelitian ini.

3.4.3 Hasil pengujian

Data-data yang didapatkan dari pengujian disajikan dalam bentuk tabel dan grafik.

3.4.4 Analisis pengujian

Setelah pengujian telah dilakukan, barulah data-data dari hasil pengujian dapat di analisis. Data-data hasil pengujian pada algoritma SHA-1 dan SHA-3 kemudian akan dibandingkan, barulah dapat dilihat algoritma manakah yang terbaik.

3.5 Kesimpulan

Setelah implementasi dan pengujian telah dilakukan, barulah dapat ditarik kesimpulan.