BAB III
METODOLOGI PENELITIAN

3.1 Objek dan Subjek Penelitian

3.1.1 Objek Penelitian

Objek penelitian pada penelitian ini adalah bagaimana metode enkripsi dua tahap menggunakan kombinasi AES-256 dan RSA dapat mengamankan data pada *database* saat pengujian menggunakan serangan *SQL Injection*.

3.1.2 Subjek Penelitian

Subjek penelitian dalam penelitian ini adalah sistem keamanan database. Pada sistem yang dirancang akan diterapkan kombinasi algoritma *Advance Encryption System* (AES) dan Rivest Shamir Adleman (RSA) sebagai pengaman *database*. Sistem dibangun menggunakan model *PHP Native* dengan tambahan kode HTML dan CSS. Sistem tersimpan pada web hosting serta domain yang sudah disewa selama satu tahun kedepan sebagai bahan pengujian penelitian.

3.2 Alat dan Bahan Penelitian

3.2.1 Alat Penelitian

Alat penelitian dalam penelitian ini adalah web hosting dan juga computer penyerang dengan detail spesifikasi sebagai berikut.

3.2.1.1 Spesifikasi Web Hosting

Spesifikasi Web Hosting yang digunakan adalah sebagai berikut :

Tabel 3. 1 Spesifikasi *Web Hosting*

No.	**Aspek**	**Spesifikasi**
1.	Penyedia Jasa	Nusantara Host
2.	Penyimpanan	12 GB NVMe SSD
3.	RAM	6 GB
4.	*Processor*	2 Core CPU @2Ghz
5.	Domain	Gratis
6.	*Bandwidth*	*Unlimited*

7.	Kontrol Panel	Plesk
8.	Server Basis Data	MariaDB
9.	Jenis Basis Data	MySQL
10.	Harga Sewa Tahunan	Paket Pangeran Rp. 100.000.- (tahun pertama, perpanjangan Rp. 400.000.- per tahun)

3.2.1.2 Spesifikasi Komputer *Tester*

Spesifikasi komputer yang digunakan sebagai alat untuk melakukan pengujian serangan *SQL Injection* adalah sebagai berikut :

Tabel 3. 2 Spesifikasi perangkat *tester*

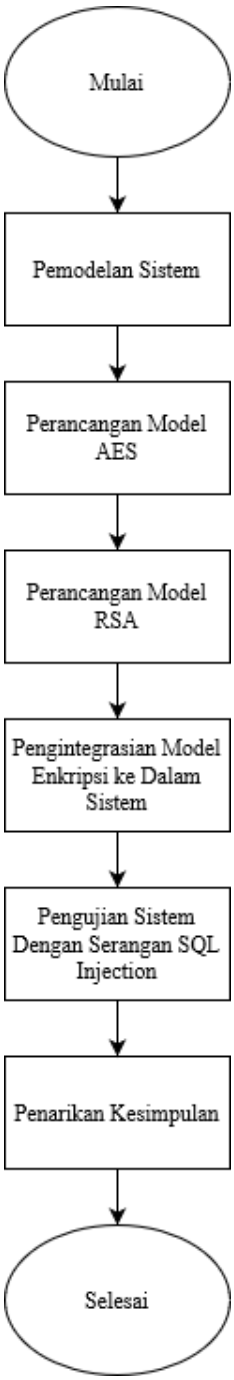
No.	**Aspek**	**Spesifikasi/Keterangan**
1.	Merek	Lenovo
2.	Tipe Perangkat	Laptop IdeaPad 320-14IKB (2017)
3.	RAM	4 GB
4.	Prosesor	Intel(R) Core (TM) i5-7200U CPU @ 2.50GHz
5.	Penyimpanan	1 TB
6.	Sistem Operasi	Kali Linux 2022.4
7.	Aplikasi *Tester*	SQL Map

3.2.2 Bahan Penelitian

Bahan penelitian yang akan digunakan oleh peneliti adalah bahan yang nantinya akan dianalisis pada penelitian ini. Bahan penelitian tersebut adalah bagaimana implementasi enkripsi AES-256 dan RSA yang difungsikan untuk mengamankan data pada *database* serta bagaimana hasil akhir dari implementasi keamanan pada *database* tersebut ketika diuji coba menggunakan serangan *SQL Injection*.

3.3 Metodologi Penelitian

Metodologi penelitian yang diterapkan dalam penelitian ini adalah studi kepustakaan, perancangan sistem, implementasi algoritma, pengujian sistem, pengumpulan data, analisis dan kesimpulan. Alur dari penelitian ini tertuang pada Gambar 3.1.



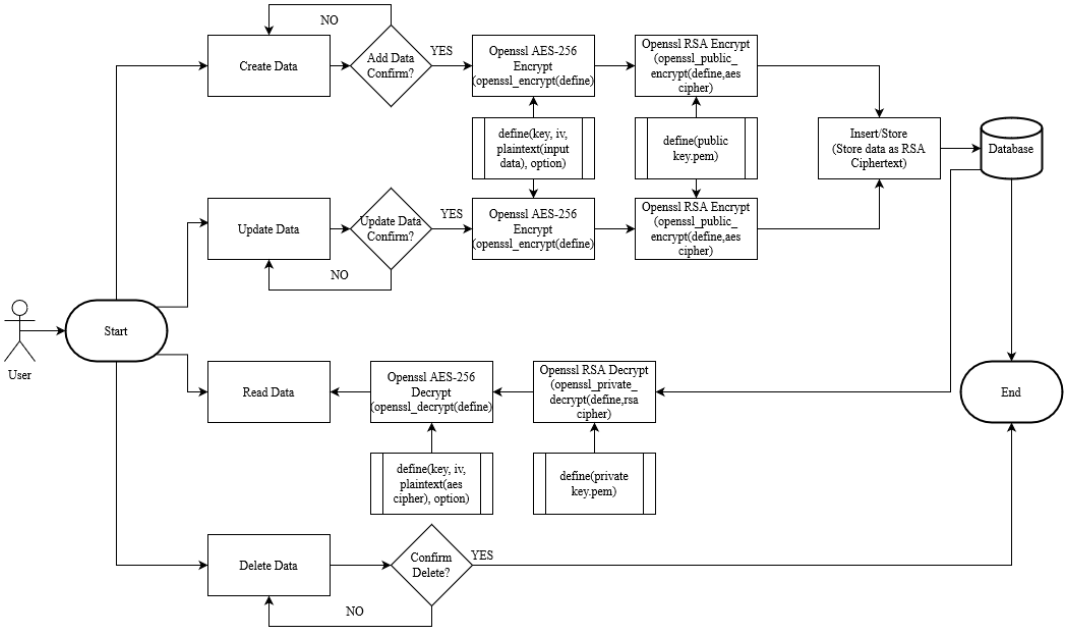
Gambar 3. 1 Metodologi Penelitian

3.3.1 Pemodelan Sistem

Pada tahap ini dilakukan perancangan skema bagaimana jalannya sistem nantinya. Perancangan mencakup bahasa pemrograman, skema basis data serta implementasi dari algoritma yang digunakan.

3.3.2.1 Perancangan Arsitektur Sistem

Pada tahap ini, dilakukan perancangan sistem yang akan digunakan sebagai objek penelitian. Perancangan sistem meliputi bagaimana sistem bekerja kaitannya dengan konsep *double encryption* yang digunakan. Desain arsitektur sistem yang dirancang tertuang pada skema Gambar 3.2.



Gambar 3. 2 Desain Arsitektur Sistem

3.3.2.2 Konfigurasi *Web Hosting*

Pada web hosting, konfigurasi fitur sistem dilakukan dengan skema seperti berikut :

Tabel 3. 3 Konfigurasi Web Hosting

Fitur	Keterangan/Status
Web Application Firewall	Non aktif
Secure Socket Layer	Non aktif
Transport Layer Security	Non akftif

HTTPS	Non aktif
Password Protected Directory	Non aktif

Konfigurasi diatur dengan menonaktifkan semua fitur keamanan pada web server dengan tujuan untuk memudahkan proses pengujian serangan *SQL Injection* pada situs web.

3.3.2.3 Pemodelan Basis Data

Pada tahap ini dilakukan konfigurasi dari basis data yang akan digunakan sebagai target pengujian sistem nantinya. Basis data dibuat dengan *PHPMyAdmin* yang sudah tersedia pada layanan *web hosting*.

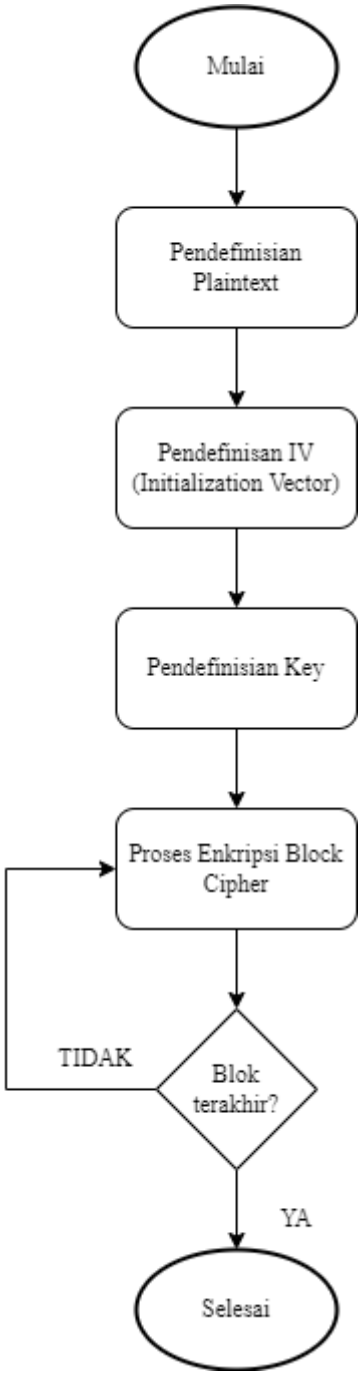
Tabel 3. 4 Konfigurasi tabel target

No.	Name	Type	Attributes	Null	Default
1.	customer (PK)	varchar(50)	-	No	None
2.	Nama	varchar(255)	-	No	None
3.	Credit	blob	-	No	None
4.	Phone	blob	-	No	None
5.	company	varchar(255)	-	No	None
6.	country	varchar(255)	-	No	None

Pada skema tabel diatas, *field* "customer" menjadi *primary key*. Semua *field* menggunakan tipe data varchar dengan pengecualian pada *field* "credit" dan "phone". Pengecualian dilakukan untuk menyimpan *ciphertext* yang nantinya terenkripsi dengan tipe data *binary* sehingga pemilihan blob (*Binary Large Object*) pada *field* tersebut sesuai dengan produk akhir *ciphertext* hasil proses enkripsi. *Field* "credit" dan "phone" nantinya adalah *field* yang akan dienkripsi pada sistem untuk diuji apakah enkripsi dan dekripsi dua tahap AES-256 dan RSA dapat diimplementasikan pada sistem.

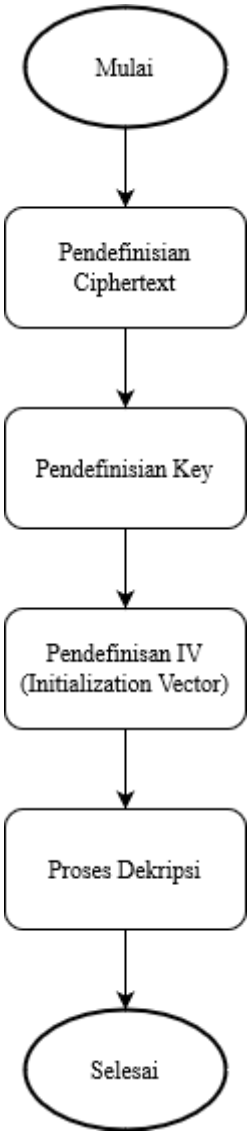
3.3.2 Perancangan Model AES-256

Pada tahap ini, dilakukan perancangan model enkripsi dan dekripsi dari kriptografi AES yang nantinya akan diintegrasikan pada sistem. Dengan memanfaatkan *library Openssl*, enkripsi dilakukan dengan mendefinisikan setiap unsur yang dibutuhkan untuk melakukan enkripsi dan dekripsi dari AES-256.



Gambar 3. 3 Pemodelan Enkripsi AES-256 CBC

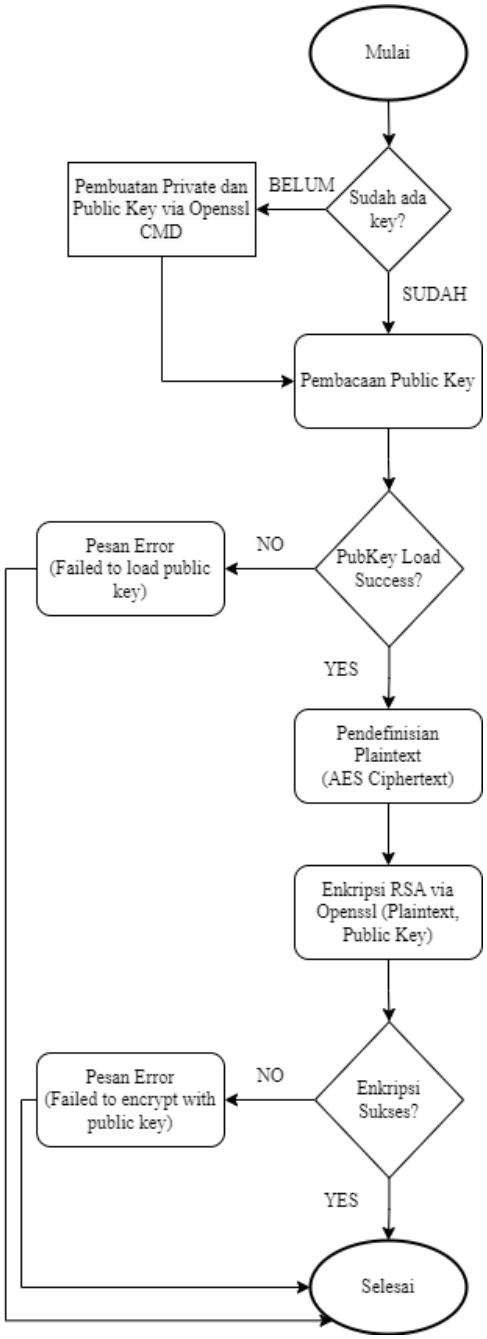
Sementara dari sisi dekripsi, skema pemodelan hanya berbeda dari sisi pendefinisian plaintext menjadi pendefinisian ciphertext.



Gambar 3. 4 Pemodelan Dekripsi AES-256

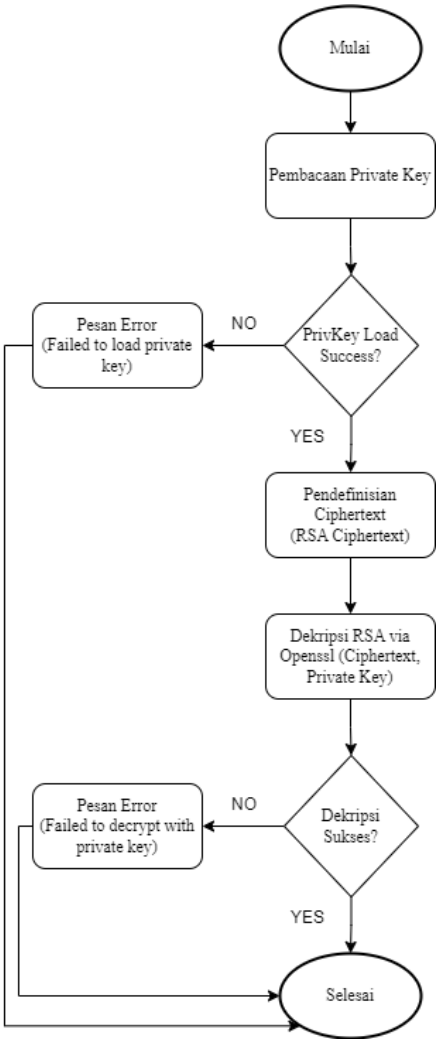
3.3.3 Perancangan Model RSA

Pada tahap ini dilakukan pemodelan untuk model kriptografi RSA. Proses RSA dilakukan dengan mengenkripsi *ciphertext* dari proses enkripsi AES-256.



Gambar 3. 5 Pemodelan Enkripsi RSA

Sementara untuk tahapan dekripsi, bagian plaintext digantikan dengan *ciphertext* yang diambil dari data yang tersimpan dengan pada *database*.



Gambar 3. 6 Pemodelan Dekripsi RSA

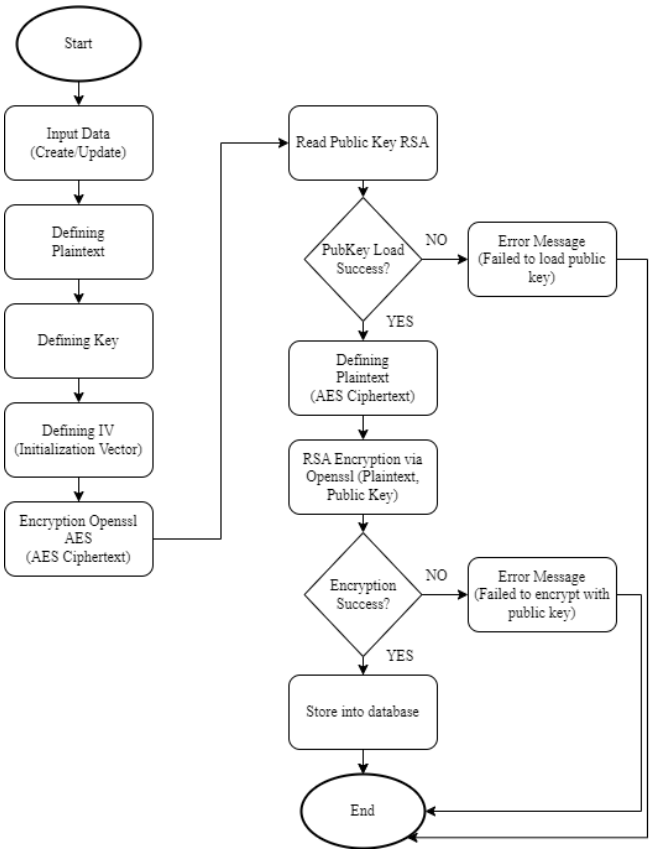
3.3.4 Pengintegrasian Sistem

Pada tahap ini dilakukan pengintegrasian antara model enkripsi dan dekripsi AES-256 dan RSA yang sudah dirancang. Pada sistem, model enkripsi AES-256 dan RSA akan diimplementasikan pada proses *create* dan *update* sementara proses dekripsi RSA dan AES-256 akan diimplementasikan pada fungsi *read* pada halaman index. Fungsi *delete* sendiri berfungsi untuk menghapus *entry* data pada sistem.

3.3.4.1 Pengintegrasian Model Enkripsi

Pada tahap ini dilakukan pengintegrasian dari model enkripsi yang sudah dibuat ke dalam sistem. Enkripsi dua tahap akan diimplementasikan pada proses

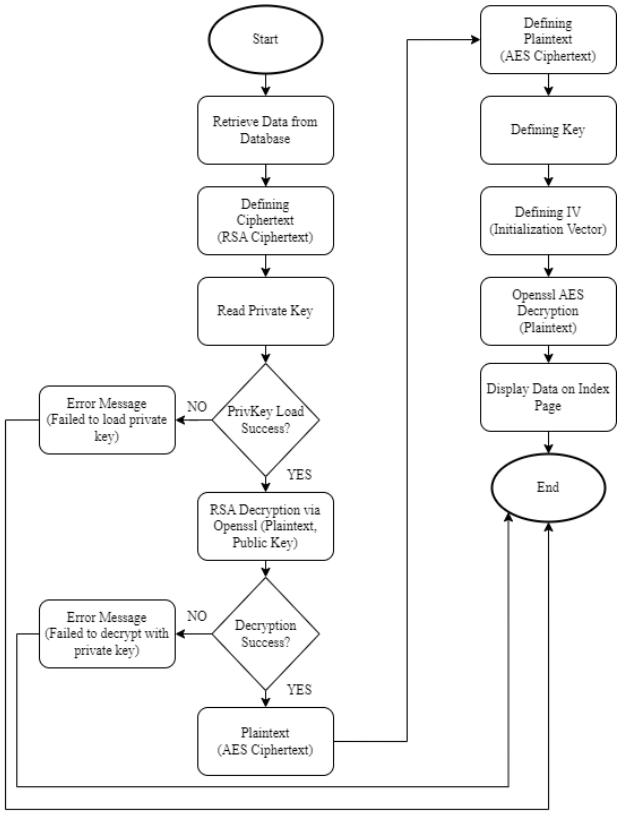
create dan *update* dimana input data dari kedua proses tersebut akan tersimpan sebagai *ciphertext* di dalam *database*.



Gambar 3. 7 Integrasi Model Enkripsi Ke Dalam Sistem

3.3.4.2 Pengintegrasian Model Dekripsi

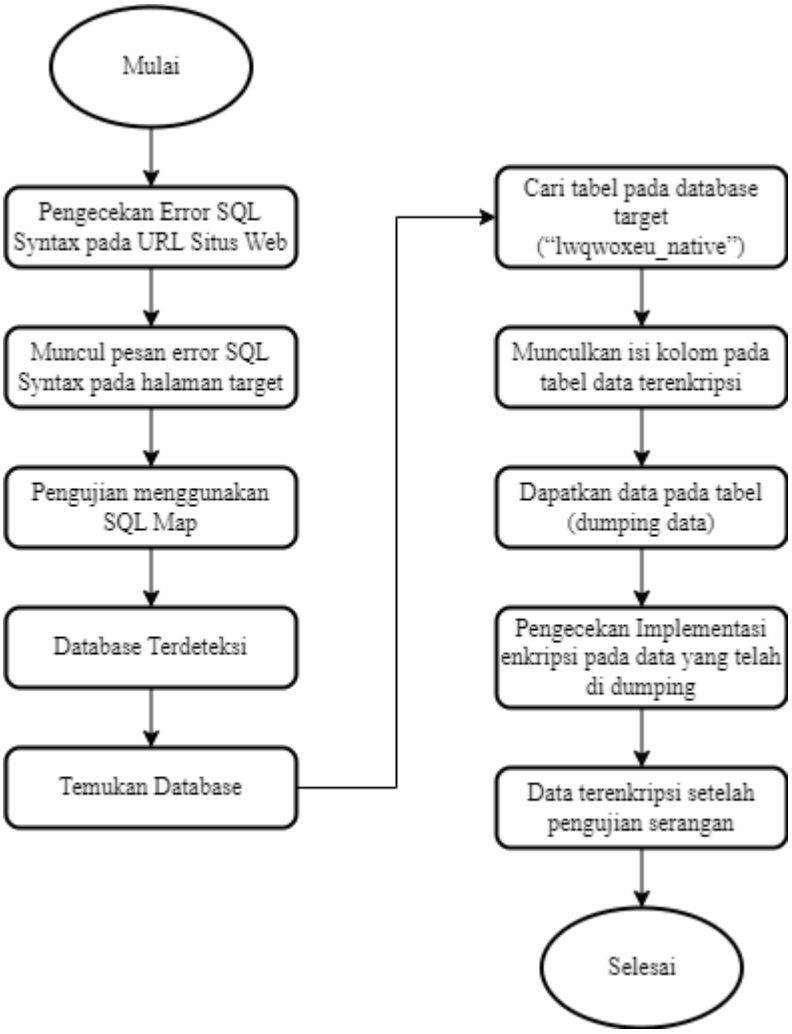
Pada tahap ini dilakukan pengintegrasian model dekripsi yang sudah dibuat ke dalam sistem. Dekripsi dua tahap akan diimplementasikan pada proses *read* dimana *output* dari proses tersebut akan muncul sebagai *plaintext* pada halaman *index*.



Gambar 3. 8 Integrasi Model Dekripsi Ke Dalam Sistem

3.3.5 Pengujian Sistem

Pengujian sistem dilakukan setelah perancangan sistem selesai dibuat. Pengujian dilakukan dengan menguji apakah algoritma enkripsi dua tahap menggunakan AES-256 CBC dan RSA dapat diimplementasikan untuk mengamankan data terhadap serangan *SQL Injection*. Skema pengujian sistem dijelaskan pada Gambar 3.9.



Gambar 3. 9 Skema Alur Pengujian Sistem

Pengujian dilakukan berdasarkan data yang sudah terenkripsi pada sistem. Implementasi dari enkripsi dua tahap dapat terlihat setelah dilakukan pengujian serangan *SQL Injection* pada situs web. Perancangan sistem dinyatakan berhasil apabila data yang muncul setelah pengujian serangan *SQL Injection* adalah data terenkripsi atau *ciphertext*.

3.3.6 Penarikan Kesimpulan

Penarikan kesimpulan merupakan tahapan akhir setelah dilakukan pengujian terhadap sistem yang telah dibuat. Kesimpulan diambil berdasarkan data yang terlah terkumpul setelah pengujian. Kesimpulan juga memuat saran untuk penelitian selanjutnya dibidang yang sama, dengan potensi adanya perbedaan

metode, objek, maupun jenis serangan yang akan diujikan di penelitian-penelitian berikutnya.