BAB III

ANALISIS DAN PERANCANGAN SISTEM

3.1 Analisis Sistem

Analisis sistem merupakan kegiatan penguraian suatu sistem informasi yang utuh dan nyata ke dalam bagian-bagian atau komponen-komponen komputer yang bertujuan untuk mengidentifikasikan serta mengevaluasi masalah-masalah yang muncul, hambatan-hambatan yang mungkin terjadi dan kebutuhan-kebutuhan yang diharapkan sehingga mengarah kepada solusi untuk perbaikan maupun pengembangan ke arah yang lebih baik dan sesuai dengan kebutuhan serta perkembangan teknologi.

3.2 Evaluasi Sistem

Melihat permasalahan-permasalahan yang terjadi pada website, sebagian besar disebabkan karena adanya interaksi dalam sebuah website seperti forum diskusi, pengiriman komentar dalam sebuah artikel di website, buku tamu, dan lain-lain. *Spammer* akan memasang bot-botnya untuk menyerang suatu website yang menjadi targetnya.

Untuk itu diperlukan suatu sistem keamanan untuk memblokir spam dan bot-bot spam ini, yaitu bagaimana cara agar *spammer* dan bot-bot ini tidak bisa melakukan *posting* yang nanti akan terdeteksi sebagai spam, dan juga untuk memblokir bot-bot spam ini dengan cara harus mengisi dengan benar kode keamanan yang diberikan.

3.3 Analisis Kebutuhan Sistem

Hasil evaluasi di atas menggambarkan bahwa seorang pemilik atau administrator website membutuhkan sebuah sistem keamanan untuk mengatasi permasalahan spam ini agar website dapat bersih dari spam dan bot-bot spam.

3.4 Usulan Kebutuhan Sistem

Untuk mengatasi permasalahan keamanan ini, diusulkan dengan pembuatan sistem keamanan yang dapat mengamankan website dari penyerangan bot-bot spam.

Usulan kebutuhan yang dapat diterapkan adalah dengan cara menginstalasi script PHP yang nantinya akan menjadi sebuah sistem keamanan bagi website.

3.5 Pemodelan Kebutuhan Fungsional

Sistem keamanan website ini yang berisi kode keamanan dan program untuk untuk memblokir spam dan bot-bot spam, diinstalasikan pada pengisian form, untuk melakukan *posting*. Perancangan sistem keamanan website ini meliputi:

- Perancangan sistem untuk memblokir bot
- Perancangan sistem untuk memfilter spam

Bagaimanapun juga tidak ada sistem yang sempurna dalam menangani keamanan website, tetapi yang terpenting adalah bagaimana untuk semaksimal mungkin menjaga agar website bersih dari spam dan bot spam.

3.5.1 Kebutuhan Perangkat Keras

Perangkat keras (*Hardware*) adalah seluruh komponen atau unsur peralatan yang digunakan untuk menunjang pembangunan sistem keamanan website. *Hardware* yang digunakan untuk menerapkan sistem informasi ini secara optimal memerlukan spesifikasi minimum komputer sebagai berikut :

a. *Processor* Intel core 2 duo 1.50 GHz
b. RAM 1 GB
c. *Harddisk* 120 GB
d. *Color* monitor 15”
e. CD ROM 52x
f. *Keyboard* dan *mouse*
g. Modem, RJ 45 dan *Switch Hub*

3.5.2 Kebutuhan Perangkat Lunak

Perangkat lunak (*software*) adalah program komputer yang berfungsi sebagai sarana interaksi antara pengguna dan perangkat keras. Adapun perangkat lunak yang digunakan dalam membangun sistem keamanan website ini adalah sebagai berikut:

a. Windows XP Professional SP 2
b. PHP 5
c. PHPMyAdmin – 3.0.0-dev
d. MySQL client version 5.0.32
e. Server version 5.0.32-Debian_7etch6-log

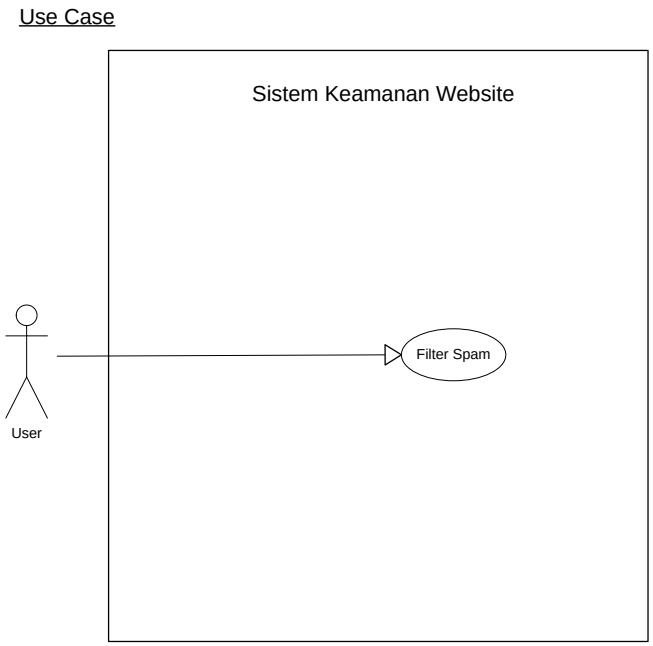
f. GD Library

g. Microsoft frontpage

h. Webhosting + Domain : skripsi.charleysakul.net

3.6 Diagram *Use Case*

Diagram *Use Case* merupakan salah satu diagram untuk memodelkan aspek perilaku sistem. Masing-masing diagram *use case* menunjukkan sekumpulan *use case*, *actor*, dan hubungannya. Diagram *use case* merupakan pusat pemodelan perilaku sistem, subsistem, dan kelas. *Use case* adalah interaksi antara *actor* dan sistem. Proses sistem tersebut di gambarkan dalam diagram *use case* sebagai berikut:



Gambar 3.1 Diagram Use Case

Dari diagram di atas, kegiatan sistem yang digambarkan oleh *Use-Case* adalah:

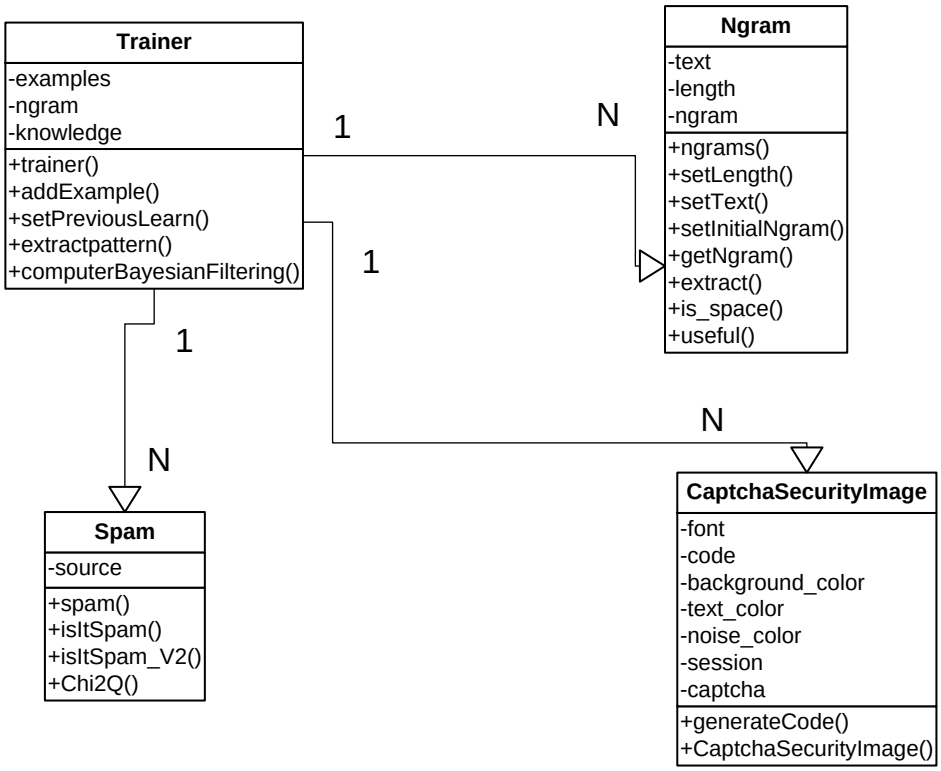
Deskripsi *Use Case* Filter Spam

Tabel 3.1 *Use Case Filter Spam*

Nama *Use Case* :	Filter Spam
Data *Input* :	Komentar User, *Security Code*
Data *Output* :	Notifikasi hasil filterisasi spam, hasil komentar bukan spam
***Actor* :**	User
Tujuan :	Menyaring komentar spam dan menampilkan komentar bukan spam
Skenario	
Actor	**Sistem**
1. User menginput security code 3. User menginput komentar	2. Sistem memverifikasi security code 4. Sistem menyaring komentar 5. Sistem menampilkan komentar yang bukan spam.

3.7 Diagram Class

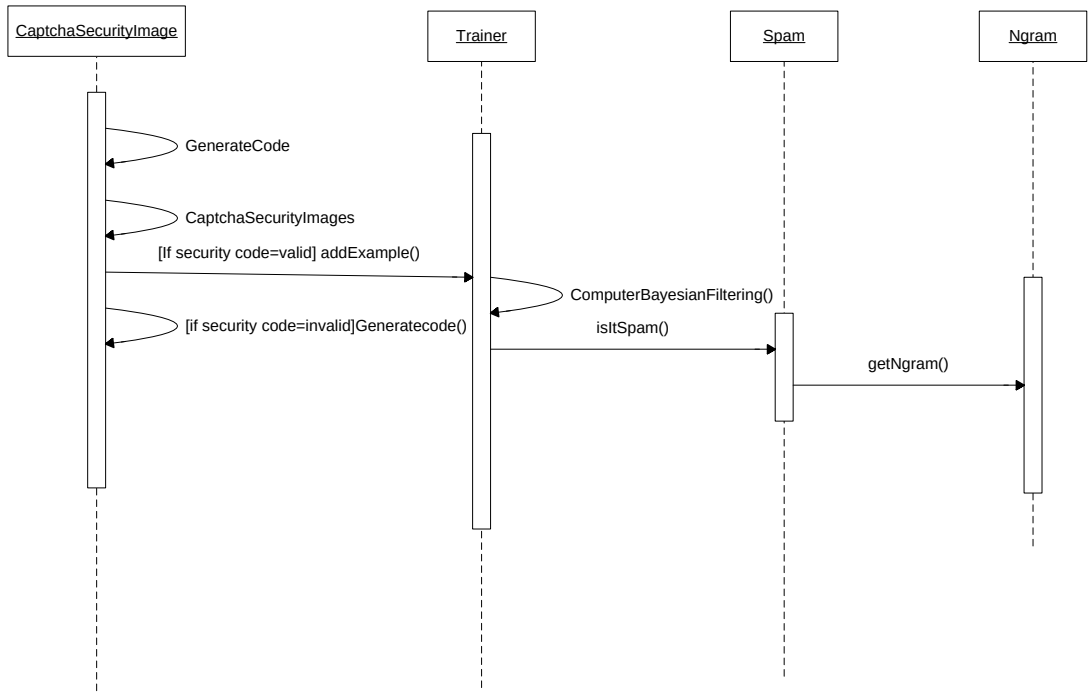
Pewarisan adalah mekanisme untuk mengekspresikan keserupaan di antara kelas-kelas, menyederhanakan pendefinisian kelas yang serupa dengan kelas yang didefinisikan sebelumnya. Pewarisan menyangkut generalisasi dan spesifikasi, menyatakan atribut dan layanan bersama (*commonality*) secara eksplisit di *hirarki* kelas. Berikut adalah gambar model objek dengan pewarisan :



Gambar 3.2 Diagram Class

3.8 Diagram Sequence

Diagram sequence digunakan untuk menggambarkan alur kerja dari fungsi-fungsi dalam sistem, seperti yang terlihat pada gambar di bawah ini:



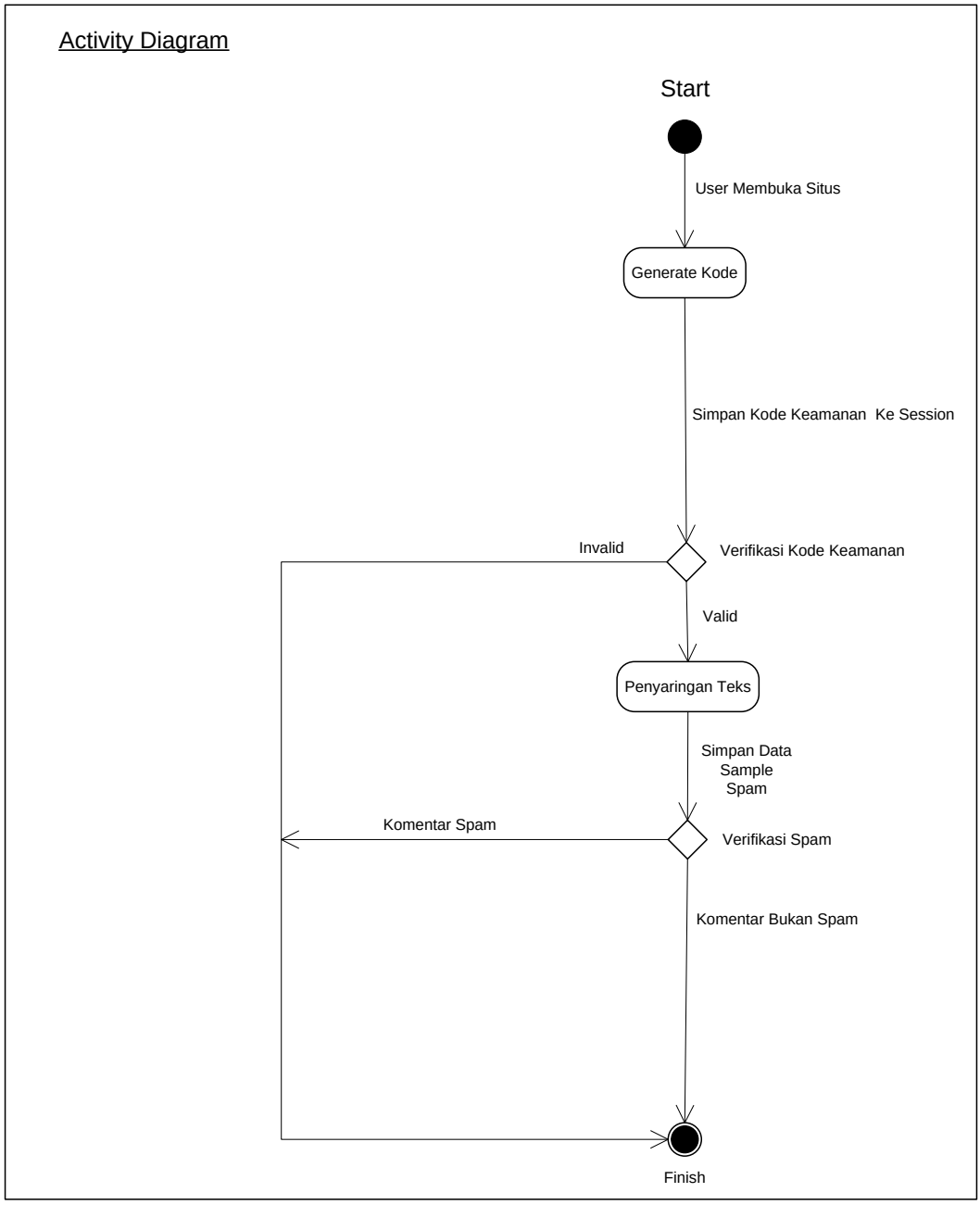
Gambar 3.3 Diagram Sequence Filter Spam

3.9 Antarmuka *(Interface)*

Antarmuka mendefinisikan batasan antara spesifikasi tentang apa itu abstraksi dan bagaimana implementasi dari abstraksi itu. Antarmuka adalah kumpulan dari operasi-operasi yang digunakan untuk menspesifikasi layanan dari suatu kelas atau objek.

3.9.1 Activity Diagram Antarmuka

Activity Diagram antarmuka menunjukkan operasi-operasi yang dilakukan oleh Actor, seperti yang terlihat pada gambar di bawah berikut ini:



Gambar 3.4 Activity Diagram

3.10 Perancangan Sistem

3.10.1 Struktur File Database

Data-data yang digunakan dalam pembangunan perangkat lunak ini disimpan dalam sebuah database *MySQL* yang terdiri dari 2 tabel yaitu tabel yang berfungsi untuk menyimpan data contoh spam (tabel *examples*) dan tabel pembelajaran komentar spam (tabel *knowledge_base*).

3.10.2 Deskripsi Tabel

1. Tabel examples

   a. Nama Tabel : examples

   b. Fungsi : Menyimpan data contoh spam

   c. Primary key : -

   d. Foreign key : -

Tabel 3.2 Tabel examples

No	Nama Field	Jenis	Ukuran	Keterangan
1	text	Text	100	Komentar user
2	state	Enum	“0”, “1”, “spam”	Pendeteksian spam

2. Tabel *knowledge_base*

   a. Nama Tabel : *knowledge_base*

   b. Fungsi : Pembelajaran komentar spam

   c. *Primary key* : *ngram, belongs*

   d. *Foreign key* : -

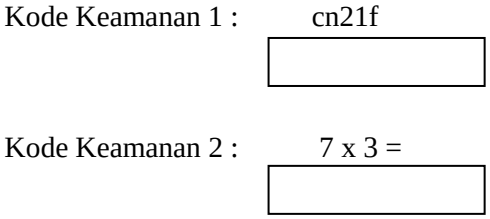
Tabel 3.3 Tabel knowledge_ base

No	Nama Field	Jenis	Ukuran	Keterangan
1	ngram	Varchar	10	Mengindentifikasi karakter
2	belongs	Varchar	10	Kepemilikan karakter
3	repite	Int	11	Pengulangan karakter
4	percent	Float	9	Persentase spam

3.11 Perancangan Antar Muka

3.11.1 Perancangan Halaman Pengecekan Bot Spam

Bot atau robot akan diblokir pada bagian pertama ini, dimana semua yang melakukan pemostingan harus memasukkan dua (2) kode keamanan dengan benar. Bila pada tahap pertama ini kode yang dimasukkan salah, maka tidak akan dilakukan pengecekan selanjutnya terhadap komentar dan otomatis pengiriman komentar gagal.



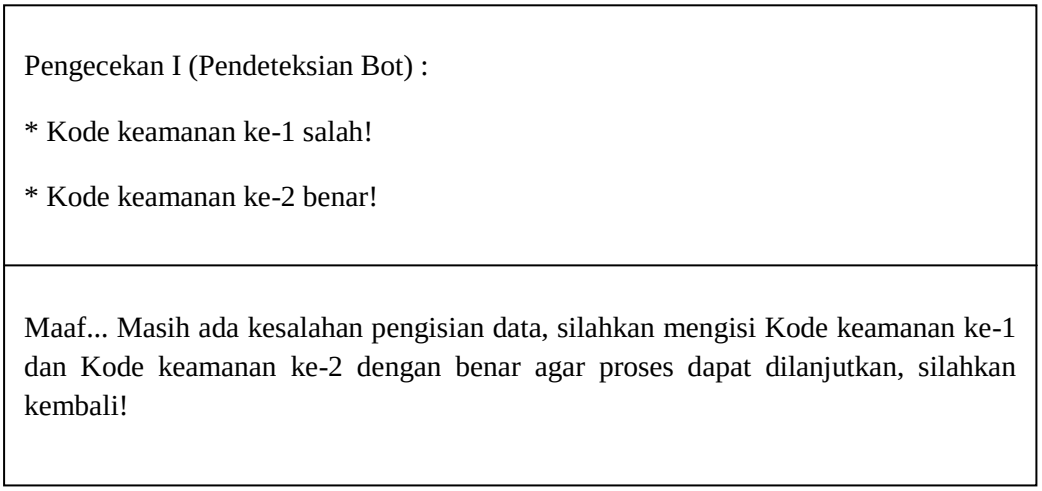
Gambar 3.5 Perancangan Kode Keamanan ke-1 dan Kode keamanan ke-2

Masing-masing kode keamanan ini selalu berganti secara random dan akan berubah setiap kali halaman ini diakses.

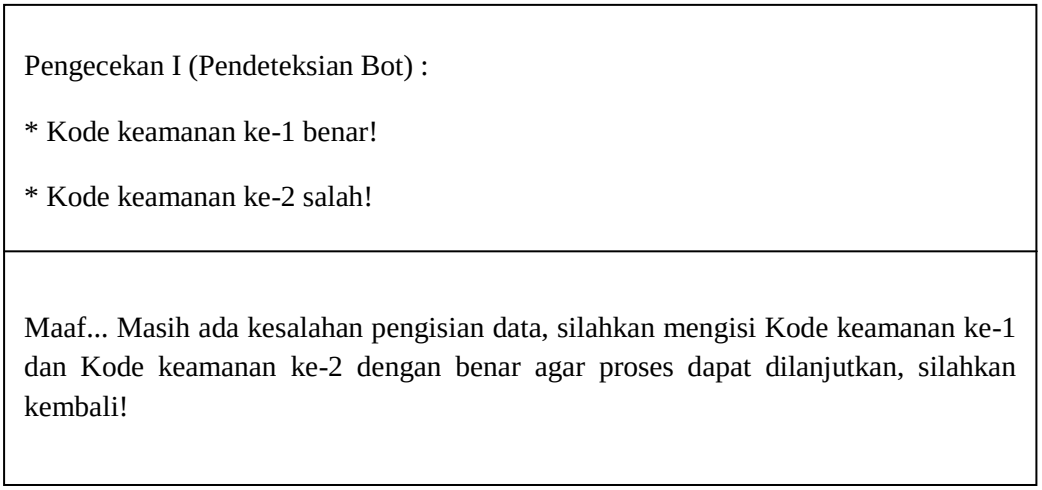
Kode keamanan ke 1 berisi gambar perpaduan 5 karakter antara huruf dan angka yang mana user harus membaca image tersebut dan memasukkan kode keamanan ini dengan benar. Contoh : cn21f, maka user harus memasukkan kode cn21f dengan benar.

Kode keamanan ke 2 berisi perhitungan angka yang mana user harus membaca image tersebut lalu menghitungnya dan memasukkan kode keamanan ini dengan benar. Contoh : 7 x 3 =, maka user harus mengisi angka 21, bila salah maka proses untuk pemostingan tidak akan dilanjutkan.

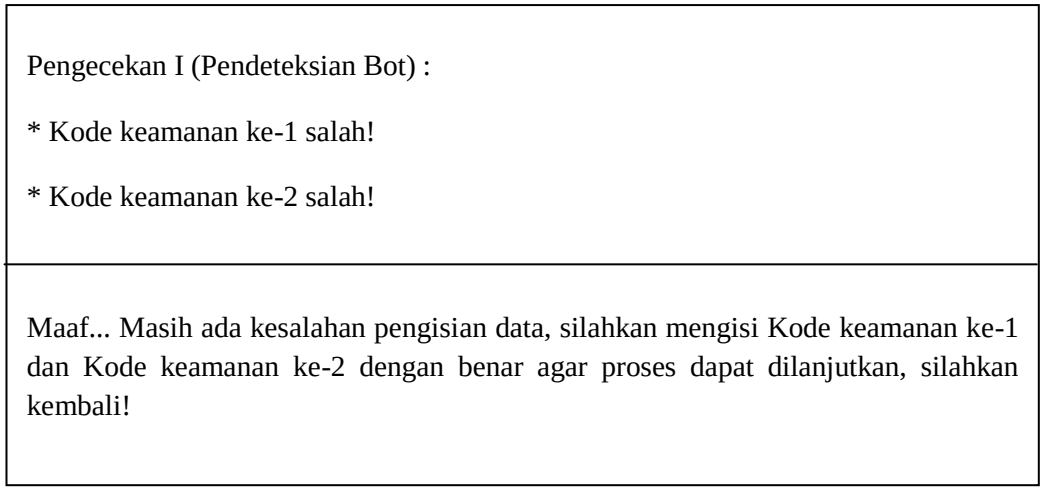
Berikut ini adalah perancangan halaman pengecekan 2 kode keamanan di atas, yang lebih ditujukan untuk pemblokiran bot (robot).



Gambar 3.6 Perancangan Tampilan Bila Kode Keamanan 1 Salah



Gambar 3.7 Perancangan Tampilan Bila Kode Keamanan 2 Salah

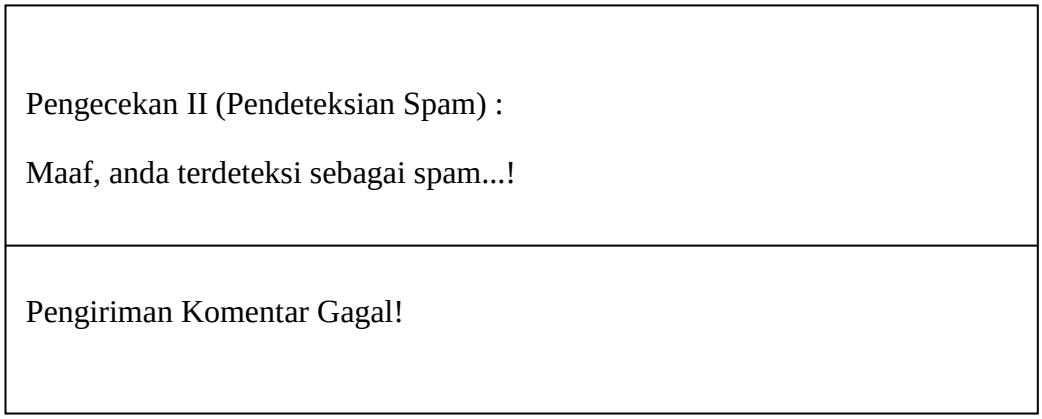


Gambar 3.8 Perancangan Tampilan Bila Kode Keamanan 1 dan 2 Salah

3.11.2 Perancangan Halaman Pengecekan Komentar

Sampai di tahap ini berarti user telah lulus melewati pengecekan I dan sekarang memasuki pengecekan II.

Pengecekan II ini adalah untuk mendeteksi semua komentar yang diisi oleh user. Pengecekan II ini menggunakan Algoritma Bayesian untuk memblokir spam.



Gambar 3.9 Perancangan Tampilan Halaman Pengecekan Komentar

3.11.3 Perancangan Halaman Sukses

Bila user memasukkan kode keamanan ke-1 dan 2 dengan benar, dan isi komentar user tersebut tidak terdeteksi sebagai spam, berarti user telah berhasil dan proses pemostingan akan dilakukan.

Berikut ini adalah perancangan halaman sukses, yaitu bila user sukses melakukan posting.

Pengecekan I (Pendeteksian Bot) : * Kode keamanan ke-1 benar! * Kode keamanan ke-2 benar!
Pengecekan II (Pendeteksian Spam) : Anda tidak terdeteksi sebagai spam…
Terima Kasih, Pengiriman Komentar Sukses! Untuk melihat hasil komentar anda, mohon tunggu sebentar, terima kasih!

Gambar 3.10 Perancangan Halaman Sukses

Setelah halaman sukses ini ditampilkan maka dalam waktu 2 detik, user akan di*redirect* ke halaman utama, dimana semua hasil pemostingan ditampilkan di halaman utama.