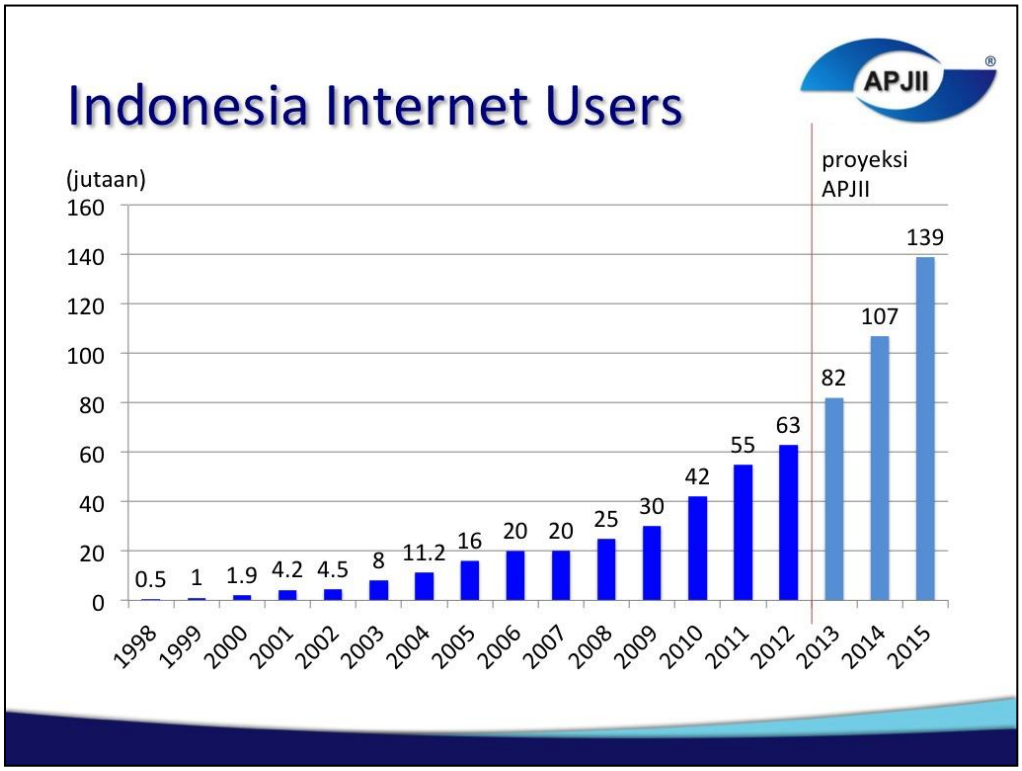
# BAB I

# PENDAHULUAN

## 1.1. Latar Belakang Masalah

Internet merupakan kemajuan teknologi informasi yang sangat nyata dan berpengaruh besar dalam kehidupan, namun dampak negatif dari internet turut berkembang, diantaranya adalah konten negatif yang terus bertambah seiring pertumbuhan situs internet dan peningkatan jumlah pengguna layanan internet pada setiap tahunnya. Berdasarkan informasi dari data yang disajikan oleh APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) bahwa pengguna layanan internet khususnya di Indonesia terus bertambah, seperti ditunjukkan pada diagram grafik di bawah ini :




Gambar 1.1. Grafik jumlah pengguna internet di Indonesia tahun 1998-2012 versi APJII

Dengan pertumbuhan domain yang sangat pesat dan konten negatif yang tidak terkendali, diiringi jumlah pengguna layanan internet yang terus meningkat maka akan menimbulkan banyak kerugian diantaranya :

1. Spam : mengakibatkan ketidaknyamanan pengguna.
2. Situs Porno : mengakibatkan gangguan kesehatan mental dan tindakan criminal.
3. Perjudian *online* : mengakibatkan kerugian material dan spiritual.
4. Isu SARA : mengakibatkan perpecahan persatuan dan kesatuan bangsa.

Untuk mencegah dampak negatif tersebut maka diperlukan sistem keamanan yang diterapkan pada jaringan internet. Hal ini sesuai dengan tugas dan peran serta Internet Service Provider (ISP) dalam melindungi bangsa dari dampak negatif internet. Sebagai penyedia layanan internet diharapakan mampu memberikan layanan jaringan internet yang aman dan sehat bagi masyarakat. ISP harus mampu menerapkan sistem keamanan yang memadai agar masyarakat merasa nyaman tanpa hadirnya konten negatif ketika memanfaatkan layanan intenet.

Untuk mewujudkan sistem keamanan pada jaringan internet, ISP dapat menerapkan beberapa metode proteksi diantaranya *blocking* situs dan *redirect. Blocking* situs bertujuan untuk melakukan pencekalan terhadap situs yang mememuat konten negatif, sehingga tidak dapat diakses. Sedangkan *redirect* bertujuan untuk mengalihkan ke situs lain.

Metode *blocking domain* merupakan strategi untuk membuat sulit bagi pengguna untuk menemukan domain tertentu atau situs web di internet. Metode ini pertama kali diperkenalkan pada tahun 1997 sebagai sarana untuk memblokir email spam dari alamat IP yang diketahui. Namun seiring pertumbuhan situs yang semakin banyak, makan *blocking domain* saat ini diterapakan tidak hanya untuk memblokir email spam melainkan situs-situs yang mengandung unsur porno, isu SARA, perjudian online, dan lain sebagainya.

Sedangkan sistem keamanan internet dengan metode *redirect* yaitu dengan mengarahkan pengguna ke situs lain yang sudah didaftarkan pada DNS. Salah satu contoh ketika pengguna mencoba untuk akses www.spam.com dan situs tersebut berada didaftar blok DNS, maka akan diarahkan ke situs lainnya, misalnya situs yang sudah disiapkan dengan halaman yang menyatakan bahwa domain yang diminta tidak diizinkan diakses karena mengandung unsur konten negatif.

## 1.2. Identifikasi Masalah

PT Telkom bekerjasama dengan Dinas Komunikasi dan Informatika (Diskominfo) melakukan *blocking* terhadap situs-situs yang memuat *content negative.* Proses *blocking* dilakukan berdasarkan alamat domain atau situs website. Alamat domain tersebut diperoleh dari hasil *research*, laporan langsung dari masyarakat atau hasil identifikasi situs-situs yang diakses oleh pelanggan.

Saat ini daftar situs yang akan dilakukan *blocking* diinput secara manual oleh administrator ke database server, dan ada tiga lokasi server DNS Telkom yaitu Batam, Jakarta dan Surabaya. Kondisi ini mengakibatkan pekerjaan menjadi tidak efektif dikarenakan :

1. Harus dilakukan di masing-masing DNS yang berlokasi di 3 *node* yang berbeda.
2. Setiap ada penambahan data domain yg di-*blacklist* harus dihapus terlebih dahulu kemudian dimasukkan total semua data terbaru.
3. Perkembangan domain yang cukup tinggi menuntut Telkom untuk menyiapkan tim khusus sebagai *researcher* untuk mencari domain-domain yang berisi konten negatif.
4. Tidak ada *evident* yang bisa dilampirkan di DNS untuk referensi apabila suatu saat dibutuhkan. Contoh: tidak ada capture yang menyatakan domain tersebut berisi konten negatif

tidak ada data siapa yang request bahwa domain tersebut harus diblok, tidak ada waktu kapan domain tersebut mulai diblok.

5. Menambah load proses di DNS

## 1.3. Lingkup Tugas Akhir

Adapun ruang lingkup tugas akhir adalah sebagai berikut :

1. Studi kasus hanya dilakukan di jaringan internet yang disediakan oleh PT Telkom.
2. Pengujian sistem dilakukan secara simulasi dengan membuat *server dummy* yang dikonfigurasi pada *Virtual Machine* (WMware Workstation), secara lokal.
3. Optimasi yang dilakukan hanya sebatas untuk manajemen data *content negative.*
4. Protokol yang digunakan untuk pengiriman data adalah RPZ *(Response Policy Zone)*.
5. DNS yang digunakan adalah BIND 9.
6. Sistem Optimasi Administrasi *Blocking* Domain dimaksud mempermudah dan meningkatkan efektifitas kerja pengelola layanan internet dalam melakukan blocking domain yang dianggap mengandung konten negatif.
7. Tidak membahas pembuatan perangkat lunak yang diterapkan.

## 1.4. Tujuan Tugas Akhir

Tujuan Tugas Akhir adalah “Membangun Sistem Optimasi Administrasi *Blocking Domain* secara terpusat sehingga dapat membantu meningkatkan efektifitas kerja dan mengoptimalkan infrastruktur yang ada.

Fitur yang akan disediakan pada Sistem Optimasi Administrasi *Blocking Domain* dimaksudkan untuk :

1. Memudahkan dalam melakukan pekerjaan *blocking domain*.
2. Network DNS eksisting dapat dijaga dari koneksi dan konfigurasi secara langsung.
3. Membuat proses pekerjaan update data *blocking domain* menjadi lebih mudah karena hanya dilakukan di server RPZ master sehingga tim operasional Telkom tidak perlu melakukan update data ke setiap DNS server pada masing-masing lokasi.
4. Adanya *evident* yang bisa di lampirkan di DNS untuk referensi apabila suatu saat dibutuhkan.
5. Mewujudkan layanan internet yang sehat bagi masyarakat.

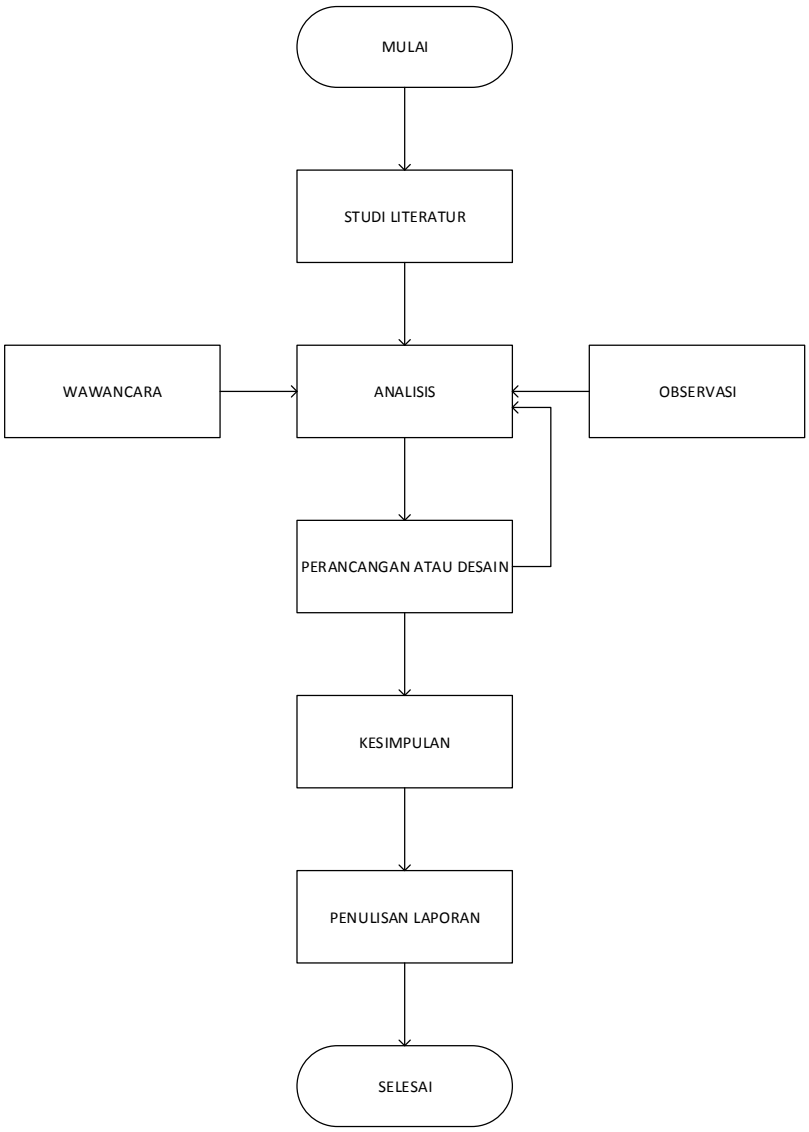
## 1.5. Metodologi Tugas Akhir

Metodologi ini mencakup semua kegiatan pengumpulan data yang dilakukan sebagai bahan untuk identifikasi dan pemecahan masalah yaitu :

1. Melakukan tanya jawab dan diskusi dengan ahli telekomunikasi yang memahami sistem manajemen DNS khususnya yang diterapkan pada jaringan internet ISP.
2. Studi Literatur tentang administrasi *Domain Name Server (DNS)*.

Mengumpulkan data tertulis dan mengidentifikasi pengolahan *cache* yang tersimpan pada DNS, mencatat permasalahan yang terjadi, menganalisis data yang diperoleh untuk menetukan rancangan sistem optimasi yang efektif yang sesuai dengan kebutuhan pengguna. Mencari beberapa informasi dari internet untuk mengetahui gambaran secara lebih detail mengenai perencanaan sistem optimasi administrasi DNS.

3. Melakukan Observasi terhadap sistem keamanan internet yang diterapkan pada jaringan Telkom. Observasi dilakukan di STO Telkom Jatinegara.
4. Melakukan analisis terkait dengan fungsional dari sistem, koneksi jaringan, dan *respons time* yaitu waktu tanggap yang diberikan oleh interface ketika user melakukan permintaan.
5. Melakukan proses perancangan Sistem Optimasi Administrasi Blocking Domain.
6. Membangun aplikasi untuk menajemen data.
7. Menguji hasil analisis dan perancangan di laboratorium komputer.
8. Menyusun laporan dari hasil perancangan sistem.




Gambar 1.2 Metodologi Tugas Akhir

## 1.6. Sistematika Penulisan

Untuk lebih memudahkan dalam memahami Tugas Akhir ini, maka disusun dengan sistematika penulisan sebagai berikut :

**Bab I Pendahuluan**

Berisi tentang latar belakang masalah, identifikasi masalah, lingkup tugas akhir, tujuan tugas akhir, metodologi, dan sistematika penulisan tugas akhir.

**Bab II Landasan Teori**

Berisi tentang teori yang menjelaskan dasar jaringan internet, arsitektur jaringan internet, protokol yang sering digunakan, skema pengalamatan IP, fungsi DNS, struktur database DNS, cara kerja DNS, optimalisasi DNS, klasifikasi sistem keamanan internet, konsep dalam mengamankan sistem jaringan internet yang digunkan oleh publik dengan mekanisme *Response Policy Zone (RPZ)*.

**Bab III Analisis dan Perancangan**

Berisi tentang kerangka tugas akhir, analisis sistem yang berjalan yang mencakup mekanisme blocking domain, kelemahan dan kelebihan dari sistem yang ada saat ini, dan solusi terhadap permasalahan dari sistem. Menjelaskan konsep dari pembangunan sistem baru yang mencakup perancangan topologi jaringan, interoperability dan diagram *flow chart*.

**Bab IV Implementasi dan Pengujian**

Berisi tentang perancangan Sistem Optimasi Administrasi *Blocking Domain* dalam bentuk simulasi pada *Virtual Machine*. Dalam bab ini juga dibahas pengujian sistem setelah melalui tahap simulasi.

**Bab V Penutup**

Berisi tentang kesimpulan dan saran.