BAB 1
USULAN GAGASAN

1.1 Latar Belakang Masalah

Indonesia merupakan negara yang masih berkembang dalam bidang telekomunikasi, hal ini salah satunya ditunjukkan dengan adanya perkembangan infrastruktur *Based Transceiver Station* atau yang disingkat sebagai BTS yang makin banyak tersebar bahkan sampai ke daerah pelosok di Indonesia. Hal ini juga didukung oleh pemerintah setempat dan pemerintah pusat. Salah satu contohnya adalah penambahan dan perbaikan BTS di beberapa area tertentu untuk menunjang kebutuhan komunikasi masyarakat [1].

BTS adalah infrastruktur telekomunikasi yang memungkinkan peranti komunikasi berkomunikasi dengan jaringan operator secara nirkabel. Peranti komunikasi penerima sinyal BTS termasuk telepon, telepon seluler, dan jaringan nirkabel. Operator jaringan, seperti GSM, CDMA, atau platform TDMA, juga dapat menerima dan mengirimkan sinyal radio ke perangkat mobile. Sinyal radio ini kemudian dikonversi menjadi sinyal digital untuk dikirim kembali [2].

Dengan adanya perkembangan ini, pertukaran dan akses informasi dapat dengan mudah dilakukan, namun seiring dengan perkembangan tersebut, banyak ancaman dan kejahatan yang ditimbulkan melalui penyalahgunaan infrastruktur BTS oleh pihak yang tidak bertanggungjawab , salah satunya adalah FakeBTS. FakeBTS adalah sebuah duplikat dari BTS yang sudah ada dan digunakan untuk melakukan intersepsi jaringan operator telekomunikasi tertentu disekitar BTS yang dekat dengan alat FakeBTS tersebut [3]. FakeBTS digunakan sebagai media pembobolan jaringan dan penyebaran informasi palsu [4]. Salah satu bentuk pembobolan jaringan adalah pengambilan data pada BTS yang ada dan digunakan oleh FakeBTS untuk melakukan penipuan terhadap perangkat yang tersambung. Kasus yang kerap kali terjadi pada masyarakat Indonesia adalah penyebaran SMS penipuan yang bahkan berpotensi untuk meretas dan mengumpulkan data krusial dari pengguna perangkat. Hal ini akan menjadi sangat berbahaya jika penggunaan FakeBTS sebagai pembobol jaringan dan pencurian data dilakukan pada area-area kritikal seperti kantor pemerintahan atau tempat-tempat penting yang menyimpan

data-data konfidensial, dan jika terjadi penyebaran informasi palsu pada area kritikal akan menimbulkan sebuah permasalahan yang besar.

1.2 Informasi Pendukung Masalah

Pembobolan jaringan melalui FakeBTS sudah sangat banyak terjadi pada masyarakat Indonesia. Bentuk pembobolan jaringan dibuktikan dengan penerimaan pesan berisi informasi palsu dan penipuan pada perangkat selular masyarakat. FakeBTS memancarkan frekuensi seolah-olah BTS operator, sehingga *broadcast* pesan yang diterima masyarakan terlihat seolah-olah dikirim oleh operator asli yang digunakan oleh masyarakat. Langkah yang diambil pemerintah dalam upaya menangani permasalahan penggunaan FakeBTS ini adalah mengeluarkan larangan penggunaan FakeBTS. Pelarangan tersebut tertuang dalam SIARAN PERS NO. 84/HM/KOMINFO/04/2019 mengenai Tangkal Penyebaran Konten Negatif, Kominfo Larang Jual Beli dan Penggunaan Perangkat Penyebar SMS Palsu [5].

Untuk meningkatkan efektivitas dalam mengurangi penggunaan FakeBTS di Indonesia, perlu adanya pengembangkan suatu sistem yang dapat mendeteksi keberadaan FakeBTS melalui implementasi Independent Station pada area-area kritikal.

1.3 Analisis Umum

1.3.1 Aspek Ekonomi

Banyaknya penipuan yang memakai Fake BTS menjadikan beberapa warga terkena penipuan yang bersifat keuangan

1.3.2 Aspek Keberlanjutan

Makin tidak percayanya masyarakat terhadap penyedia jasa provider yang ada di Indonesia dan kurangnya mekanisme keamanan Jaringan GSM yang langsung menyerang pengguna dengan mengirim spam dan pesan SMS penipuan.

1.4 Kebutuhan yang Harus Dipenuhi

Ada beberapa kebutuhan yang harus dipenuhi agar deteksi ini lebih lancar. Kebutuhan yang harus dipenuhi sebagai berikut.

1. Dapat mengamati dan mengontrol alat penguji jaringan fakeBTS; dan
2. Pembuatan *dashboard* sebagai media pengamatan dan *monitoring*.

1.4.1 Kebutuhan yang Harus Dipenuhi

Dalam penyelesaian masalah, kebutuhan yang harus dipenuhi peneliti pada solusi sistem yang akan dibuat yaitu:

1. Mampu mengidentifikasi BTS asli dan *fakeBTS*.
2. Membantu pengguna mengenali sinyal BTS.
3. Membantu pengguna melihat data sinyal yang telah ditangkap oleh alat ke dalam *dashboard*.

1.5 Solusi Sistem yang Diusulkan

Berikut ini adalah penjelasan terkait solusi sistem yang ditawarkan sebagai bentuk penyelesaian dari permasalahan yang telah disebutkan sebelumnya.

1.5.1 Solusi Sistem 1: Deteksi 2G

Pada solusi pertama diusulkan program Deteksi 2G yang dirancang untuk membantu pengguna dalam memantau deteksi BTS 2G.

1. Fitur Utama:

   Fungsi dari Deteksi 2G ialah untuk *scanning* BTS 2G.

2. Fitur Dasar:

   Fitur yang terdapat dalam sistem ini adalah fitur menampilkan data BTS 2G yang terdeteksi.

3. Fitur tambahan:

   Dapat mendeteksi beberapa sinyal BTS dalam waktu yang bersamaan.

4. Sifat solusi yang diharapkan:
   a. Mudah digunakan
   b. Tidak membutuhkan perawatan yang terlalu intensif
   c. Dapat digunakan di berbagai sistem operasi

1.5.2 Solusi Sistem 2: Deteksi 4G

Pada solusi kedua diusulkan program Deteksi 4G yang dirancang untuk membantu pengguna dalam melindungi dan memantau keamanan lingkungan digital.

1. Fitur Utama :

   Fungsi dari Deteksi 4G dapat melakukan pemindaian jaringan untuk mendeteksi keberadaan BTS yang mencurigakan atau palsu. Aplikasi ini dapat memantau jaringan seluler dan mengidentifikasi perangkat-perangkat BTS yang sah ataupun tidak dikenal yang dapat mengancam keamanan dan privasi pengguna.
2. Fitur Dasar :

   Fitur yang terdapat dalam sistem ini adalah fitur untuk menangkap sinyal frekuensi. Bukan hanya BTS, sistem ini juga bisa menangkap sinyal radio, dll.
3. Fitur Tambahan :

   Dapat mendeteksi sinyal beberapa BTS secara bersamaan.
4. Sifat solusi yang diharapkan :

   Mampu bmemberian alat yang kuat dan transparan untuk memeriksa dan melinndungi privasi mereka dari potensi pelacakan atau pemantauan melalui jaringan seluler.

1.5.3 Solusi Sistem 3: Dashboard Monitoring

Solusi sistem 3 merupakan sebuah *dashboard* yang memiliki fitur untuk menyimpan sebuah informasi data.

1. Fitur Utama :

   Fungsi *dashboard* bertujuan untuk mengevaluasi proses data yang sedang berjalan.
2. Fitur dasar :

   Fungsi *monitoring* adalah *Memonitoring* data yang telah didapat atau telah di identifikasi. Tujuan utamanya yaitu untuk mempermudah proses pemantauan data secara rutin dan mengidentifikasi BTS *real* atau *fake* pada sistem 2G dan 4G.

1.5.4 Skenario Penggunaan

1.5.4.1 Skema Deteksi 2G

Skema saat menggunakan DragonOS sebagai berikut. Pertama-tama dimulai dengan instalasi DragonOS kedalam device laptop. Didalam DragonOS, terdapat banyak fitur yang sudah terinstall didalamnya dan yang dipakai untuk scanning BTS 2G ialah “Deteksi 2G”. Setelah sudah masuk ke dalam DragonOS, dilanjutkan dengan membuka terminal DragonOS dan memasukkan command “Deteksi 2G_scanner -b GSM900 -v” yang dimana akan mendeteksi BTS dengan band GSM900 di sekitarnya.

1.5.4.2 Skema Deteksi 4G

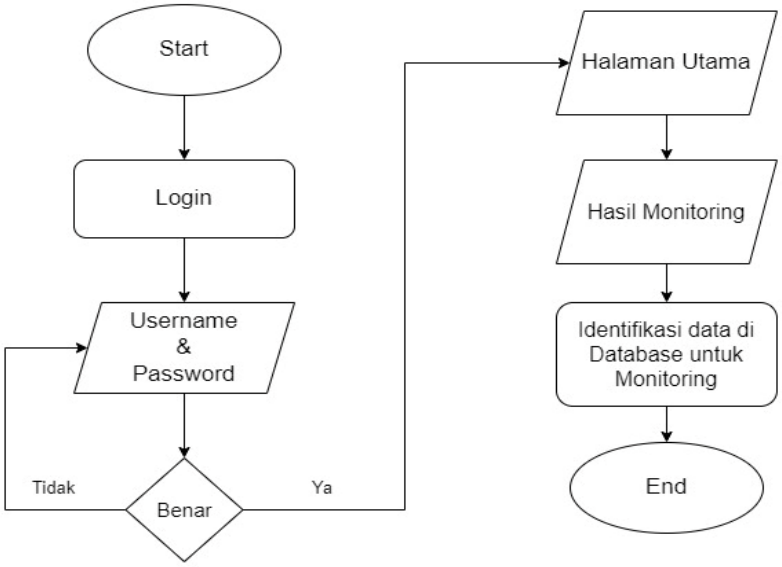
Deteksi 4G adalah aplikasi fiktif yang dirancang untuk membantu pengguna dalam deteksi dan perlindungan dari fake BTS. Beberapa skenario penggunaan termasuk pemindaian jaringan untuk mendeteksi BTS yang mencurigakan, analisis sinyal dan identifikasi karakteristik yang mencurigakan, pemantauan koneksi dan lalu lintas untuk mendeteksi perilaku mencurigakan, serta manajemen keamanan dan privasi terkait BTS. *Deteksi 4G* bertujuan untuk memberikan pemahaman umum tentang deteksi fake BTS dan melindungi pengguna dari ancaman keamanan yang terkait.

1.5.4.3 Skema *Website*

Website merupakan halaman yang mengandung kumpulan informasi tertentu yang kemudian dapat diakses melalui internet dimanapun dan kapanpun oleh siapapun. *Website* bertujuan untuk memberikan informasi tentang *Base Transceiver Station* (BTS), sedangkan *dashboard* berfungsi untuk mengevaluasi hasil data validasi 2G dan 4G yang akan di *monitoring*. Adapun skenario penggunaan produk sebagai berikut. Pertama-tama admin mengambil data hasil scanning 2G dan 4G yang akan dimasukan kedalam *database*, admin *monitoring* data, kemudian data tersebut akan ditampilkan pada halaman *dashboard*.

1.5.4.4 Skema *Monitoring*

Monitoring yang berisikan parameter data 2G dan 4G dan *monitoring* menjelaskan data yang didapat berupa data BTS real atau fake. Berikut dibawah ini merupakan skema cara kerja *monitoring*.



Gambar 1.1 Skema Monitoring

1.6 Kesimpulan dan Ringkasan CD-1

Implementasi *independent* stasion untuk deteksi fake BTS pada infrastruktur kritikal membutuhkan pendekatan komprehensif dengan fokus pada keamanan, akurasi, ketersediaan sistem, skalabilitas, integrasi, pelaporan *real-time*, dan pengelolaan yang efektif. Dalam hal ini, perlindungan data, analisis protokol jaringan, analisis sinyal, dan verifikasi tanda tangan digital menjadi kunci deteksi yang akurat. Pemilihan infrastruktur yang handal, fleksibel dalam penambahan stasiun, integrasi dengan infrastruktur yang ada, dan pemantauan sistem yang efisien juga penting. Keseluruhan implementasi ini bertujuan untuk menjaga keamanan dan integritas jaringan telekomunikasi di infrastruktur kritikal.