BAB I
PENDAHULUAN

1.1 Latar Belakang

Transformasi digital pada era modern menuntut setiap institusi dan organisasi untuk memiliki infrastruktur komunikasi yang responsif, terintegrasi, dan memiliki efisiensi tinggi. Komunikasi merupakan aspek fundamental yang menjamin keberlangsungan operasional, koordinasi antar divisi, serta produktivitas suatu instansi. Seiring dengan pesatnya perkembangan teknologi jaringan komputer, terjadi pergeseran paradigma dalam sistem telekomunikasi dari berbasis sirkuit analog (*Public Switched Telephone Network / PSTN*) menuju komunikasi berbasis paket data digital. Dalam konteks ini, teknologi *Voice over Internet Protocol* (*VoIP*) hadir sebagai standar solusi revolusioner untuk membangun infrastruktur komunikasi internal yang mandiri dan berkinerja tinggi.

Teknologi *VoIP* beroperasi dengan cara mengubah sinyal suara analog menjadi paket data digital yang kemudian ditransmisikan melalui protokol internet (IP). Implementasi teknologi ini memberikan keuntungan strategis yang signifikan, di mana institusi tidak perlu lagi membangun dan memelihara infrastruktur kabel telepon yang terpisah. *VoIP* dapat berjalan dan menumpang sepenuhnya pada infrastruktur jaringan area lokal (*LAN*) maupun nirkabel (*WLAN*) yang sudah beroperasi. Pendekatan ini terbukti sangat efektif dalam menyediakan fasilitas komunikasi multimedia yang cepat, serta secara drastis mampu menekan biaya operasional dan meningkatkan efisiensi komunikasi suatu institusi dibandingkan layanan seluler konvensional [1], [6].

Meskipun saat ini banyak institusi yang memanfaatkan layanan pesan instan publik, ketergantungan pada aplikasi pihak ketiga sering kali menimbulkan inefisiensi pada penggunaan *bandwidth* internet dan berisiko terhadap kedaulatan data instansi. Oleh karena itu, pembangunan *server VoIP* lokal (*on-premise*) menggunakan sistem operasi berbasis *Linux* dan perangkat lunak sentral seperti *Asterisk* menjadi sebuah urgensi infrastruktur IT. Kebutuhan ini semakin relevan jika dihadapkan pada studi kasus komunikasi antar gedung, seperti yang terjadi antara Gedung Fakultas Teknik Informatika dan Gedung C. Mengingat hambatan

jarak fisik yang memisahkan kedua area tersebut, penarikan infrastruktur kabel telepon fisik (*PSTN*) tentu membutuhkan biaya yang sangat besar dan tidak efisien. Sebagai solusi arsitektural, infrastruktur jaringan kedua gedung dapat diintegrasikan menggunakan teknologi *Virtual Private Network* (*VPN*) melalui perangkat router *MikroTik* [7]. Implementasi protokol *OpenVPN* akan menciptakan sebuah terowongan jaringan privat (*tunneling*) yang terenkripsi di atas infrastruktur jaringan kampus, sehingga perangkat pengguna di Gedung C dapat mengakses layanan *server VoIP* di Gedung Fakultas Teknik Informatika secara aman, seolah-olah berada di dalam satu jaringan area lokal (*LAN*) yang sama [2].

Namun demikian, di balik fleksibilitas yang ditawarkan, migrasi ke infrastruktur komunikasi berbasis IP membawa konsekuensi serius pada aspek keamanan siber. *Server VoIP* yang beroperasi di atas jaringan komputer mewarisi seluruh kerentanan fundamental dari jaringan data terbuka. Tanpa adanya mekanisme pengamanan jaringan yang memadai, lalu lintas data komunikasi sangat mudah dieksploitasi oleh pihak yang tidak bertanggung jawab [3]. Salah satu celah keamanan yang paling krusial terletak pada penggunaan *Session Initiation Protocol* (*SIP*), yaitu protokol utama yang bertugas menginisiasi sesi komunikasi. Sifat protokol ini menjadikan *server VoIP* sangat rentan terekspos terhadap berbagai ancaman, termasuk eksploitasi otentikasi dan serangan *Toll Fraud* yang dapat merugikan secara finansial maupun operasional [1].

Ancaman keamanan yang paling masif dan persisten terhadap infrastruktur *server IP-PBX* adalah serangan *Brute Force*. Dalam skenario ini, peretas menggunakan perangkat lunak bot otomatis untuk membanjiri *server* dengan ribuan percobaan otentikasi palsu guna menebak kombinasi username (ekstensi) dan kata sandi *SIP*. Jika hanya mengandalkan sistem *firewall* statis, penyerang pada akhirnya dapat menembus pertahanan sistem. Sebagai langkah preventif untuk menjaga integritas dan ketersediaan *server*, implementasi aplikasi pengamanan seperti *Fail2Ban* merupakan metode mitigasi yang sangat direkomendasikan [2]. *Fail2Ban* beroperasi dengan memindai file *log* pada *server* secara *real-time* untuk mendeteksi anomali kegagalan *login*, lalu meresponsnya dengan memblokir alamat *IP* penyerang secara dinamis melalui pembaruan firewall otomatis.

Selain penguatan infrastruktur keamanan di sisi *server*, keandalan sebuah

sistem komunikasi juga sangat dipengaruhi oleh perangkat lunak antarmuka di sisi pengguna (*client-side*). Selama ini, implementasi *VoIP* sering mengandalkan aplikasi *softphone* generik pihak ketiga yang tidak memberikan transparansi aliran data. Untuk memastikan bahwa seluruh lalu lintas komunikasi benar-benar terlokalisasi di dalam instansi, penelitian ini telah mengembangkan aplikasi klien mandiri. Pengembangan dilakukan menggunakan *framework Flutter*, yang memungkinkan pembuatan aplikasi lintas platform dengan antarmuka yang modern, stabil, dan responsif [17]. Aplikasi ini didesain agar terintegrasi penuh dengan *server VoIP* lokal untuk mendukung fungsionalitas komunikasi tanpa campur tangan *server* eksternal.

Berdasarkan seluruh analisis kebutuhan infrastruktur *IT* dan identifikasi kerentanan keamanan di atas, penulis telah merumuskan dan melaksanakan sebuah penelitian yang komprehensif mulai dari perancangan arsitektur *back-end* hingga perangkat lunak *front-end,* dengan mengangkat judul **"Rancang Bangun Komunikasi Internal Berbasis *Voice Over Internet Protocol (VoIP)* Dengan Pengamanan *Fail2ban* Terhadap Serangan *Session Initiation Protocol (SIP)"***. Melalui penelitian ini, telah terbangun sebuah ekosistem komunikasi internal yang tidak hanya efisien, terpusat, dan berbiaya rendah, tetapi juga memiliki ketahanan (*resilience*) yang adaptif terhadap berbagai ancaman siber masa kini.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, perumusan masalah dalam penelitian ini adalah:

1. bagaimana merancang dan membangun infrastruktur komunikasi internal berbasis *Voice over Internet Protocol* (*VoIP*) menggunakan *server IP-PBX Asterisk* yang dihubungkan melalui *Virtual Private Network* (OpenVPN) pada *router MikroTik* untuk memfasilitasi komunikasi aman antar Gedung Fakultas Teknik Informatika dan Gedung C?
2. Bagaimana membangun perangkat lunak klien telekomunikasi lintas *platform* (Android dan *Windows*) menggunakan *framework Flutter* yang mendukung panggilan suara dan video berbasis *WebRTC*, serta menjamin privasi data pengguna melalui penyimpanan riwayat komunikasi secara lokal (*SQLite*) tanpa

bergantung pada *server* pihak ketiga?

3. Bagaimana mengimplementasikan dan menguji efektivitas sistem keamanan dinamis berbasis *Fail2Ban* yang terintegrasi dengan *firewall server* dalam mendeteksi, memitigasi, dan memblokir ancaman serangan *SIP Brute Force*?

1.3 Batasan Masalah

Agar penelitian ini lebih terfokus dan terarah, batasan masalah yang ditetapkan adalah :

1. Lokasi dan Infrastruktur Jaringan**:** Implementasi dan pengujian sistem komunikasi dilakukan untuk menghubungkan Gedung Fakultas Teknik Informatika dan Gedung C di lingkungan Politeknik Negeri Bengkalis. Infrastruktur jaringan dibangun memanfaatkan teknologi *Virtual Private Network* (*OpenVPN*) pada *router MikroTik* untuk menciptakan jalur komunikasi lokal (*intranet*) antar gedung.
2. Perangkat *Server***:** Infrastruktur *server* dibangun menggunakan sistem operasi *Linux* (*Ubuntu*) dengan arsitektur hibrida. Layanan panggilan suara dan video ditangani oleh *engine IP-PBX* berbasis *Asterisk*, sedangkan layanan pertukaran pesan teks (*chat*) ditangani oleh *Web Server* (*Apache* dan *PHP*) beserta sistem manajemen basis data relasional (*MariaDB*) melalui antarmuka *REST API*.
3. Aplikasi Klien (*Client-Side*): Perangkat lunak antarmuka pengguna dibangun menggunakan *framework Flutter* yang beroperasi pada platform *Android* dan *Windows*. Fitur aplikasi difokuskan pada fungsionalitas panggilan suara (*Voice Call*) dan panggilan video (*Video Call*) dengan standar *WebRTC*, serta pengiriman pesan instan berbasis *HTTP*. Seluruh riwayat komunikasi pada perangkat klien disimpan menggunakan basis data lokal terintegrasi (*SQLite*) untuk mendukung fungsionalitas *offline-first* tanpa mengandalkan aplikasi pihak ketiga.
4. Lingkup Keamanan dan Pengujian: Fokus sistem pengamanan *server* dibatasi pada deteksi dan mitigasi serangan *SIP Brute Force*. Skenario pengujian keamanan dilakukan melalui simulasi serangan penetrasi menggunakan *tools SIPVicious* (*Kali Linux*) untuk memvalidasi tingkat respons otomatis dari *Fail2Ban*. Pengujian performa aplikasi dibatasi pada uji fungsionalitas

panggilan antar perangkat melalui *tunneling VPN MikroTik*.

1.4 Tujuan

Berdasarkan latar belakang yang telah diuraikan, terdapat beberapa permasalahan yang mendasari penelitian ini, yaitu:

1. Membangun infrastruktur komunikasi internal berbasis *Voice over Internet Protocol* (*VoIP*) yang menghubungkan Gedung Fakultas Teknik Informatika dan Gedung C menggunakan teknologi *Virtual Private Network* (*OpenVPN*) pada *router MikroTik*.
2. Mengimplementasikan sistem keamanan dinamis berbasis *Intrusion Prevention System* (*IPS*) menggunakan *Fail2Ban* pada *server IP-PBX Asterisk* untuk mendeteksi, mencegah, dan memitigasi ancaman serangan *SIP Brute Force* secara otomatis.
3. Mengembangkan perangkat lunak klien mandiri lintas *platform* (Android dan *Windows*) menggunakan *framework Flutter* yang dilengkapi fitur panggilan suara (*voice call*) dan panggilan video (*video call*) berbasis *WebRTC*, serta menjamin privasi data pengguna melalui penyimpanan lokal terpusat tanpa bergantung pada aplikasi pihak ketiga.

1.5 Manfaat

Hasil dari penelitian ini diharapkan dapat memberikan manfaat bagi beberapa pihak, di antaranya:

1. Bagi Institusi (Politeknik Negeri Bengkalis) : Memberikan kontribusi nyata berupa purwarupa (*prototype*) infrastruktur komunikasi internal antar gedung (Fakultas Teknik Informatika dan Gedung C) yang independen, aman, dan efisien. Sistem ini dapat memangkas biaya operasional telekomunikasi, meminimalisir ketergantungan pada layanan pesan publik atau penyedia seluler, serta menjamin kedaulatan dan kerahasiaan data percakapan di lingkungan kampus.
2. Bagi Lingkungan Akademik : Menjadi referensi kepustakaan yang komprehensif bagi civitas akademika, khususnya mahasiswa Program Studi D3 Teknik Informatika, terkait integrasi teknologi *IP-PBX*, *Virtual Private*

Network (*VPN*), dan implementasi *Intrusion Prevention System* (*IPS*) *Fail2Ban*. Selain itu, purwarupa ini dapat dimanfaatkan sebagai infrastruktur pendukung atau studi kasus nyata pada mata kuliah Jaringan Komputer, Keamanan Jaringan, maupun Pemrograman *Mobile.*

3. Bagi Penulis: Menjadi wadah untuk mengimplementasikan ilmu pengetahuan yang telah diperoleh selama perkuliahan ke dalam penyelesaian masalah di dunia nyata. Penelitian ini secara langsung meningkatkan kompetensi teknis penulis dalam merancang arsitektur jaringan (*routing* dan VPN), mengonfigurasi keamanan *server* berbasis Linux, hingga membangun aplikasi telekomunikasi lintas *platform* menggunakan *framework* Flutter.