UNIVERSITAS PANCASAKTI TEGAL

2025

DOKUMENTASI & MANUAL

NetCrypt: Aplikasi VPN dengan Enkripsi AES-256

Pencipta dan Pemegang Hak Cipta:

1. Muhammad Zidan (662260102)
2. Hikmal Falah Agung Maulana (6622600087)
3. Hanna Maulidina (6622600089)
4. Muhammad Faizal (6622600016)
5. Gunawan, S.E., M.Kom

Fakultas Teknik dan Ilmu Komputer

Tegal

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena berkat rahmat dan karunia-Nya, penulis dapat menyelesaikan laporan proyek pengembangan aplikasi NetCrypt. Laporan ini merupakan dokumentasi teknis sekaligus pedoman penggunaan dari aplikasi yang dirancang untuk memberikan solusi keamanan jaringan pribadi berbasis VPN.

Dokumentasi dan manual aplikasi yang berjudul "**NetCrypt: Aplikasi VPN dengan Enkripsi AES-256**" ini disusun sebagai bentuk pendokumentasian teknis dari proses pengembangan aplikasi serta sebagai syarat pengajuan Hak Kekayaan Intelektual (HKI).

Aplikasi ini dikembangkan oleh:

1. Muhammad Zidan (6622600102)
2. Hikmal Falah Agung Maulana (6622600087)
3. Hanna Maulidina (6622600089)
4. Muhammad Faizal (6622600016)

Di bawah bimbingan Gunawan, S.E., M.Kom, pada Fakultas Teknik dan Ilmu Komputer, Universitas Pancasakti Tegal.

Aplikasi NetCrypt dikembangkan dengan tujuan utama untuk meningkatkan kesadaran dan kemudahan dalam menggunakan jaringan virtual pribadi secara aman melalui pendekatan teknologi enkripsi yang kuat. Terima kasih kepada semua pihak yang telah memberikan dukungan dan motivasi selama pengembangan aplikasi ini.

Penulis menyadari bahwa laporan ini masih jauh dari sempurna, oleh karena itu segala bentuk kritik dan saran sangat penulis harapkan demi perbaikan di masa mendatang.

ABSTRAK

NetCrypt adalah sebuah aplikasi berbasis web yang memungkinkan pengguna menghasilkan konfigurasi VPN secara otomatis dan aman. Aplikasi ini menggunakan metode enkripsi AES-256 untuk melindungi file konfigurasi OpenVPN agar tidak mudah disalahgunakan oleh pihak yang tidak berwenang.

Dibangun menggunakan framework Flask dalam bahasa pemrograman Python dan Booststrap sebagai framework CSS, NetCrypt menyediakan antarmuka sederhana yang memungkinkan pengguna untuk melakukan registrasi, login, dan mengelola konfigurasi VPN mereka sendiri. Aplikasi ini cocok digunakan oleh pengguna individu yang ingin membangun koneksi VPN pribadi dengan perlindungan tingkat tinggi tanpa tergantung pada layanan pihak ketiga.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

I. PENDAHULUAN

1.1 Latar Belakang

Kebutuhan akan keamanan dan privasi di dunia maya semakin meningkat. Penggunaan *Virtual Private Network* (VPN) menjadi salah satu solusi populer untuk menghindari penyadapan dan pembatasan akses internet. Namun, penggunaan VPN publik memiliki risiko tersendiri karena pengguna harus mempercayakan data mereka kepada penyedia layanan VPN.

NetCrypt hadir sebagai solusi untuk menciptakan layanan VPN pribadi dengan keamanan tinggi, di mana pengguna sendiri yang menghasilkan dan mengelola konfigurasi jaringan mereka. Dengan memanfaatkan teknologi enkripsi AES-256, aplikasi ini memastikan bahwa konfigurasi hanya dapat digunakan oleh pengguna yang sah.

1.2 Rumusan Masalah

a. Bagaimana membangun aplikasi VPN personal yang mudah digunakan dan aman?
b. Bagaimana menerapkan enkripsi pada file konfigurasi OpenVPN untuk menjaga kerahasiaan data pengguna?
c. Bagaimana mengelola pengguna dan file konfigurasi OpenVPN secara efisien dalam aplikasi??

1.3 Tujuan

a. Mengembangkan aplikasi berbasis web untuk menghasilkan konfigurasi OpenVPN secara otomatis.
b. Mengimplementasikan sistem enkripsi AES-256 untuk melindungi file konfigurasi.
c. Menyediakan antarmuka pengguna yang intuitif dan mudah dioperasikan.

1.4 Manfaat

a. Meningkatkan keamanan dan privasi pengguna internet.
b. Memberikan kontrol penuh kepada pengguna atas koneksi VPN mereka.
c. Menjadi alat bantu pembelajaran dalam memahami dasar keamanan jaringan dan enkripsi.

II. DASAR TEORI

2.1 Deskripsi Algoritma

NetCrypt menggunakan algoritma kriptografi simetris, khususnya *Advanced Encryption Standard* (AES) dengan panjang kunci 256-bit dan mode operasi *Cipher Block Chaining* (CBC). AES merupakan standar enkripsi yang ditetapkan oleh *National Institute of Standards and Technology* (NIST) dan saat ini menjadi algoritma kriptografi simetris yang paling banyak digunakan secara global karena keamanannya yang tinggi dan performa yang efisien.

a. Prinsip Kerja AES-256

AES-256 bekerja dengan cara membagi data menjadi blok-blok sebesar 128-bit dan mengenkripsi setiap blok dengan serangkaian transformasi yang kompleks menggunakan kunci sepanjang 256-bit. Proses enkripsi melibatkan beberapa ronde (putaran), dan setiap ronde terdiri dari empat tahap utama:*SubBytes* – Proses substitusi *byte* menggunakan S-box non-linear.

1. *ShiftRows* – Pergeseran baris untuk menyebarkan data.
2. *MixColumns* – Proses pencampuran data antar kolom untuk difusi.
3. *AddRoundKey* – XOR antara data dan kunci dari ronde saat ini.

Pada mode CBC, setiap blok plaintext di-XOR dengan ciphertext dari blok sebelumnya sebelum dienkripsi, yang meningkatkan keamanan dengan membuat pola yang berbeda meskipun plaintext-nya identik.

3. Implementasi di NetCrypt

Dalam kode `utils/crypto.py`, algoritma ini diimplementasikan dengan menggunakan pustaka `cryptography` di Python. Data yang akan dienkripsi terlebih dahulu dilakukan *padding* agar ukurannya sesuai kelipatan 16 *byte* (karena AES bekerja pada blok 128-bit), kemudian dienkripsi menggunakan kunci dan IV *(Initialization Vector)* yang unik. Hasilnya disimpan dalam bentuk base64 agar mudah ditransmisikan atau disimpan sebagai teks.

2.2 Alasan Pemilihan Algoritma

Pemilihan AES-256 CBC sebagai algoritma inti dalam NetCrypt didasarkan pada pertimbangan sebagai berikut:

a. Keamanan Tinggi

AES-256 menawarkan tingkat keamanan yang sangat kuat dan belum pernah berhasil ditembus secara praktis. Mode CBC juga membantu mengaburkan pola pada plaintext.

b. Standar Industri

AES diakui sebagai standar internasional dan digunakan oleh organisasi besar seperti pemerintah, bank, dan perusahaan besar.

c. Ketersediaan Pustaka Python
   Pustaka `cryptography` menyediakan antarmuka aman dan efisien untuk mengimplementasikan AES dengan sedikit kemungkinan terjadinya kesalahan implementasi.

d. Performa Efisien
   Walaupun menggunakan kunci 256-bit, performa AES tetap baik bahkan pada sistem dengan spesifikasi menengah.

e. Kesesuaian dengan File Konfigurasi
   File konfigurasi OpenVPN sering kali memuat informasi sensitif seperti sertifikat dan private key. AES sangat cocok untuk mengamankan file ini karena dapat mengenkripsi data dalam ukuran besar secara efisien dan aman.

2.3 Studi Terkait

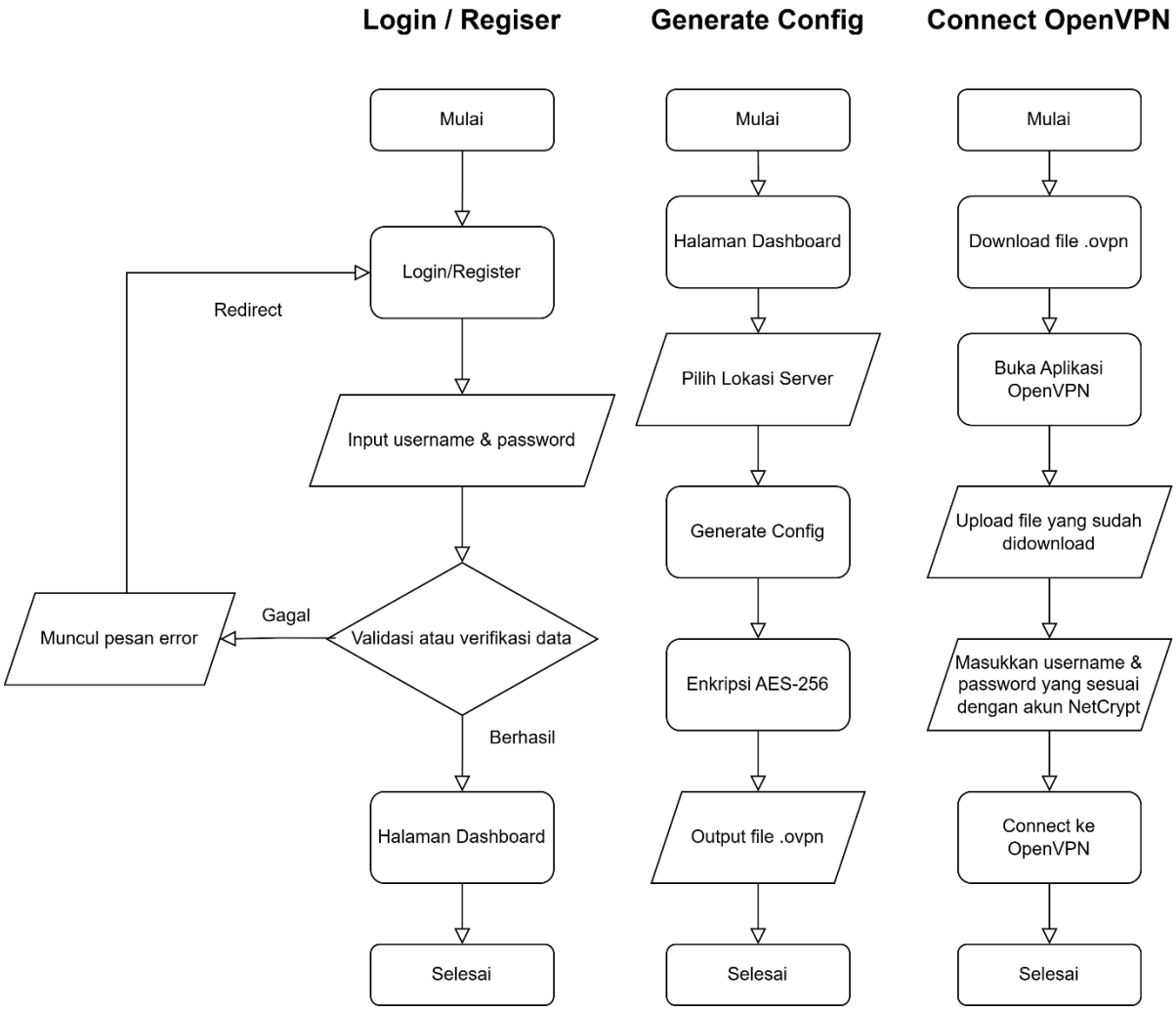
Beberapa penelitian dan implementasi di dunia nyata menunjukkan bahwa penggunaan AES untuk mengenkripsi file konfigurasi atau data sensitif telah menjadi praktik umum dalam sistem keamanan:

a. Penelitian oleh Ferguson dan Schneier (2003) menyatakan bahwa AES-CBC tetap aman jika digunakan dengan IV acak dan padding yang tepat.
b. Implementasi OpenVPN sendiri juga mendukung penggunaan AES sebagai bagian dari channel enkripsi.
c. Dalam proyek serupa seperti Algo VPN atau PiVPN, distribusi konfigurasi client tetap menjadi titik lemah. NetCrypt menawarkan pendekatan yang lebih kuat dengan menambahkan lapisan enkripsi tambahan untuk file konfigurasi yang dihasilkan, menjadikannya lebih sulit untuk disalahgunakan.

Dengan mengadopsi pendekatan ini, NetCrypt meminimalisir kemungkinan kebocoran data dan memberikan ketenangan bagi pengguna bahwa konfigurasi VPN mereka tidak dapat digunakan oleh pihak ketiga.

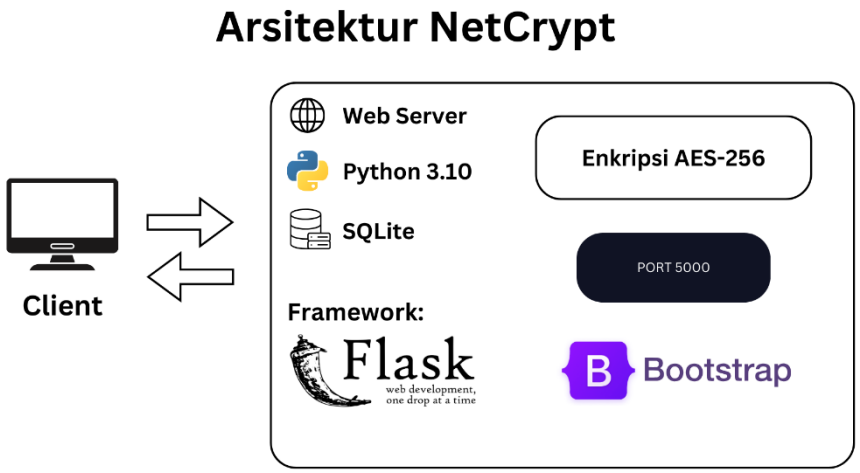
III. DIAGRAM DAN ARSITEKTUR SISTEM

3.1 Diagram Alur Proses

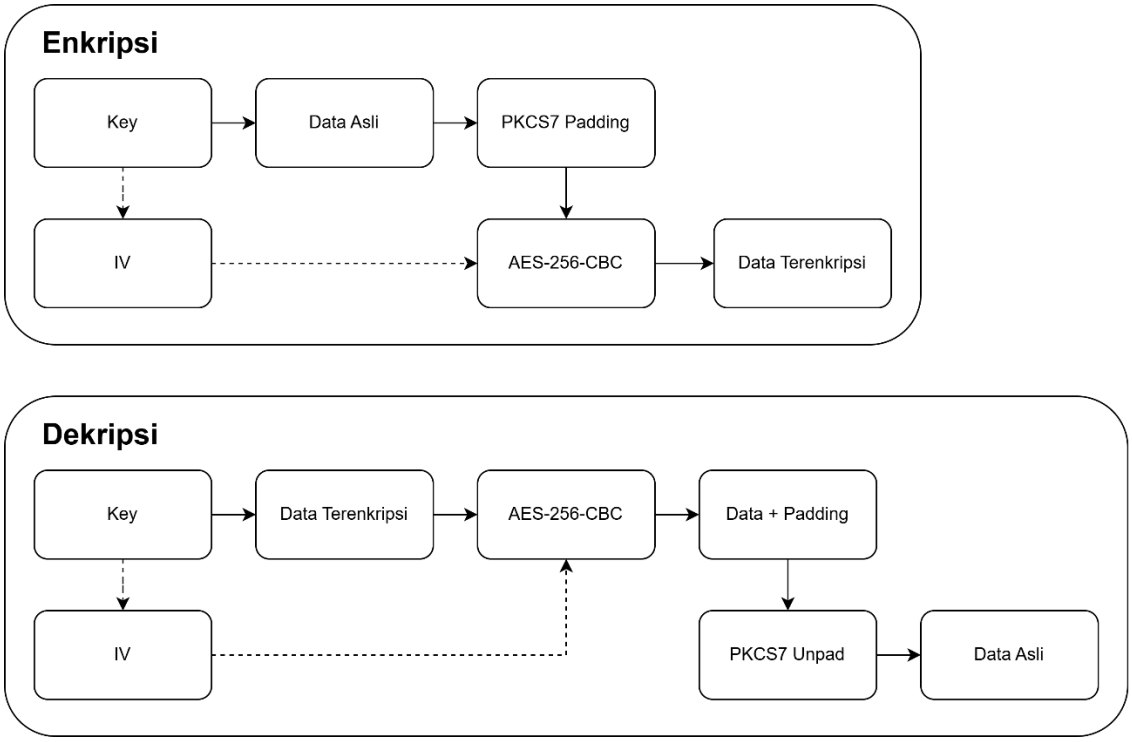


Gambar 3.1.1 Flowchart NetCrypt

3.2 Arsitektur Aplikasi

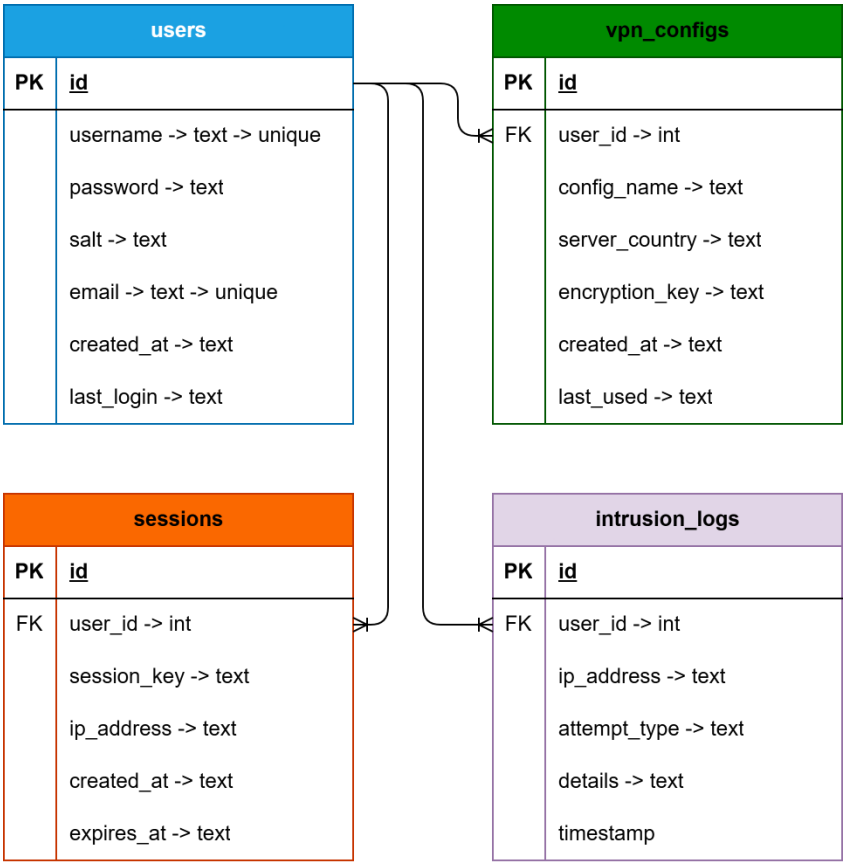


Gambar 3.2.1 Arsitektur NetCrypt



Gambar 3.2.2 Arsitektur Enkripsi dan Dekripsi

3.3 Entity Relationship Diagram



Gambar 3.3.1 ERD NetCrypt

IV. SPESIFIKASI TEKNIS APLIKASI

4.1 Teknologi yang Digunakan

a. Bahasa Pemrograman**:** Python 3.10
b. Framework: Flask dan Bootstrap
c. Basis Data: SQLite
d. Enkripsi: AES-256 (`pycryptodome`)
e. Frontend: HTML, CSS, Javascript
f. Server: Gunicorn / Flask built-in server
g. Lingkungan: Localhost, dapat di-deploy ke VPS

4.2 Platform dan Kebutuhan Sistem

a. OS: Windows, Linux, atau macOS
b. Python 3.x
c. OpenVPN
d. Browser modern (Chrome, Firefox, Edge)

V. ANTARMUKA DAN FUNGSIONALITAS APLIKASI

5.1 Struktur Navigasi Aplikasi

NetCrypt dikembangkan menggunakan framework Flask yang ringan namun fleksibel, dengan struktur navigasi yang sederhana, efisien, dan mudah dipahami oleh pengguna dari berbagai tingkat keahlian. Terdapat beberapa halaman utama yang menjadi inti dari interaksi pengguna dengan sistem, yaitu:

a. Halaman Home
   Halaman ini adalah halaman pertama pada saat pengguna mengakses website NetCrypt. Halaman ini berisi tentang NetCrypt, fitur yang disediakan, *resources,* dan panduan cara penggunaannya.

b. Halaman Login dan Registrasi
   Pengguna yang belum memiliki akun dapat mendaftar dan mengisi formulir pendaftaran. Setelah pendaftaran berhasil, pengguna akan di arahkan ke halaman login, lalu pengguna dapat login menggunakan akun yang telah dibuat sebelumnya.

c. Halaman Dashboard
   Setelah berhasil login, pengguna akan di arahkan ke halaman dashboard. Pada halaman ini, pengguna dapat melihat daftar konfigurasi VPN yang pernah dibuat, serta dapat membuat dan menghapus konfigurasi VPN.

d. Pembuatan Konfigurasi VPN
   Pengguna dapat memilih server VPN dan sistem akan secara otomatis menghasilkan file konfigurasi VPN yang telah dienkripsi.

e. Unduh File Konfigurasi
   Setelah file dienkripsi, file konfigurasi akan didekripsi dan siap diunduh oleh pengguna.

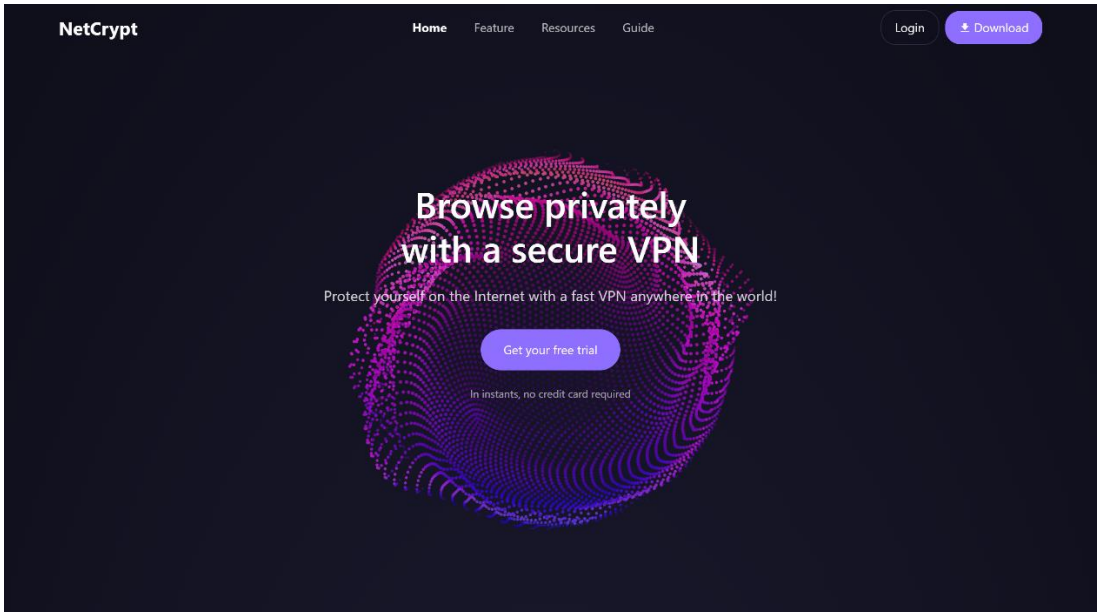
f. Logout
   Aksi logout disediakan di setiap halaman untuk mengakhiri sesi pengguna dengan aman.

Navigasi antar halaman diatur melalui sistem routing Flask yang memisahkan setiap *endpoint* berdasarkan fungsinya, seperti `/`, `/login`, `/register`, `/dashboard`, `/create_config`, dan `/download_config`, `/delete_config`, `/intrusion_logs`.

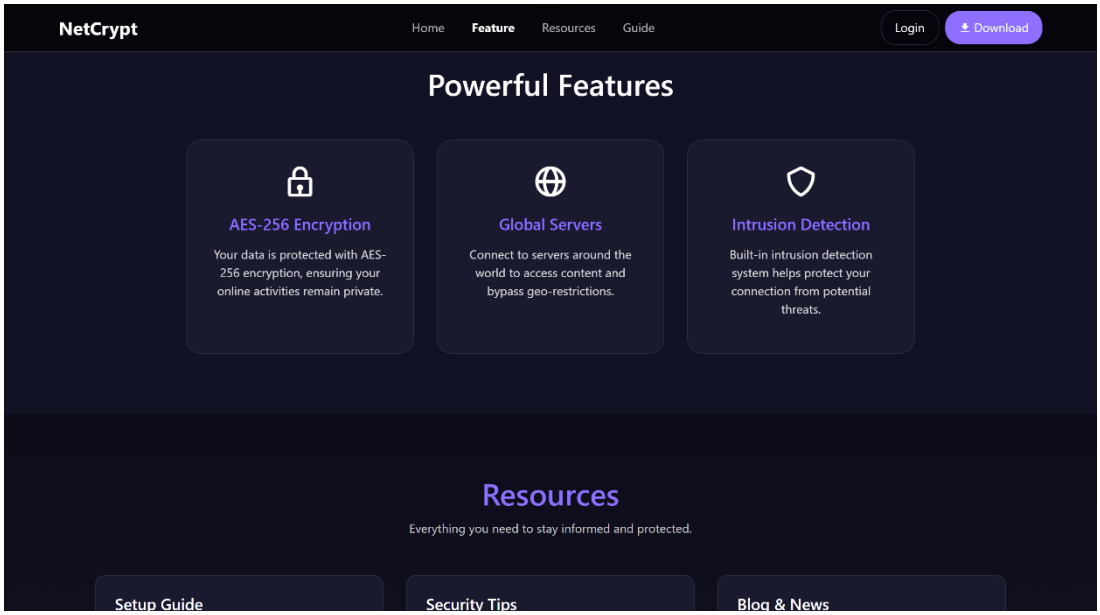
5.2 Tangkapan Layar dan Penjelasan Antarmuka

a. Halaman Home
   Halaman Home pada website NetCrypt merupakan halaman utama yang dirancang untuk memberikan gambaran umum mengenai layanan dan manfaat yang ditawarkan oleh platform ini.

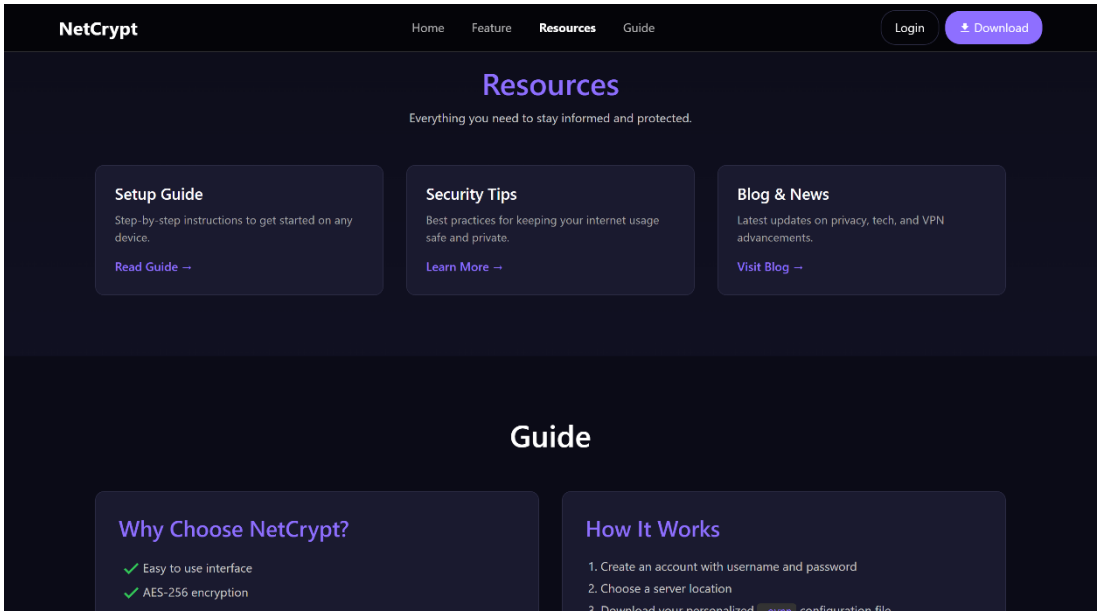
Tampilan halaman ini disusun secara informatif dan terstruktur agar pengguna dapat dengan mudah memahami fungsi serta fitur utama dari NetCrypt. Halaman ini terdiri dari informasi tentang NetCrypt, fiur yang disediakan, *resources*, dan panduan cara penggunaannya.



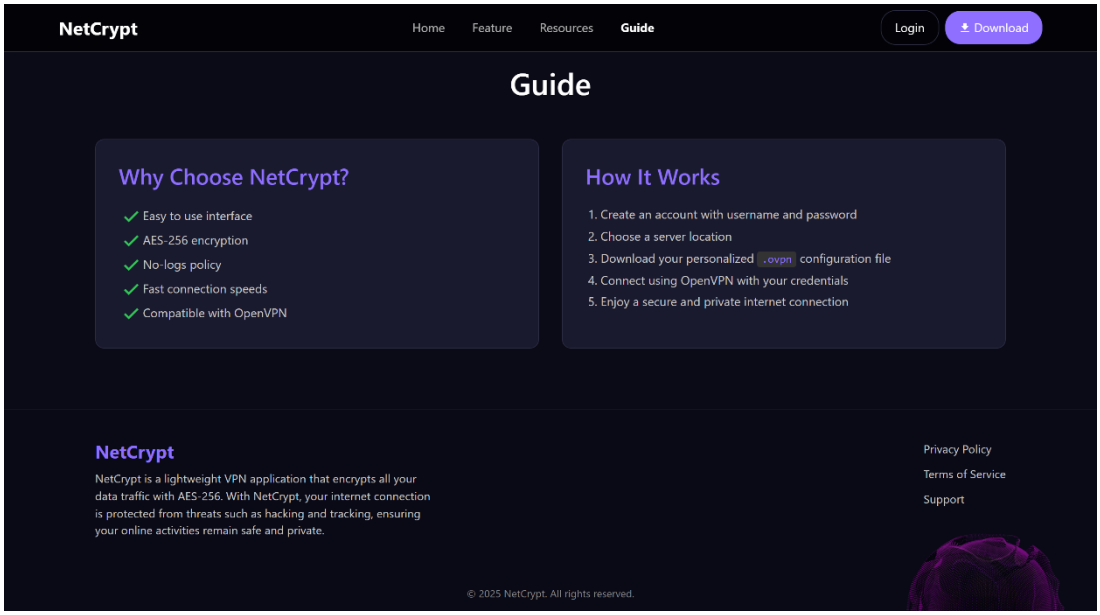
Gambar 5.2.1 Halaman Home



Gambar 5.2.2 Halaman Features



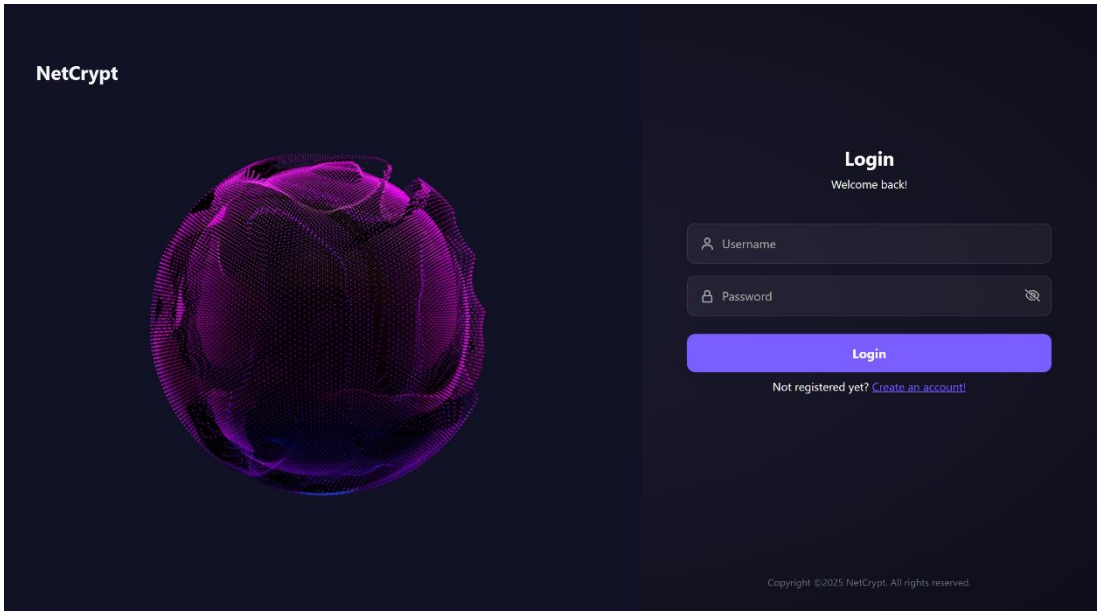
Gambar 5.2.3 Halaman Resources



Gambar 5.2.4 Halaman Guide

b. Halaman Login

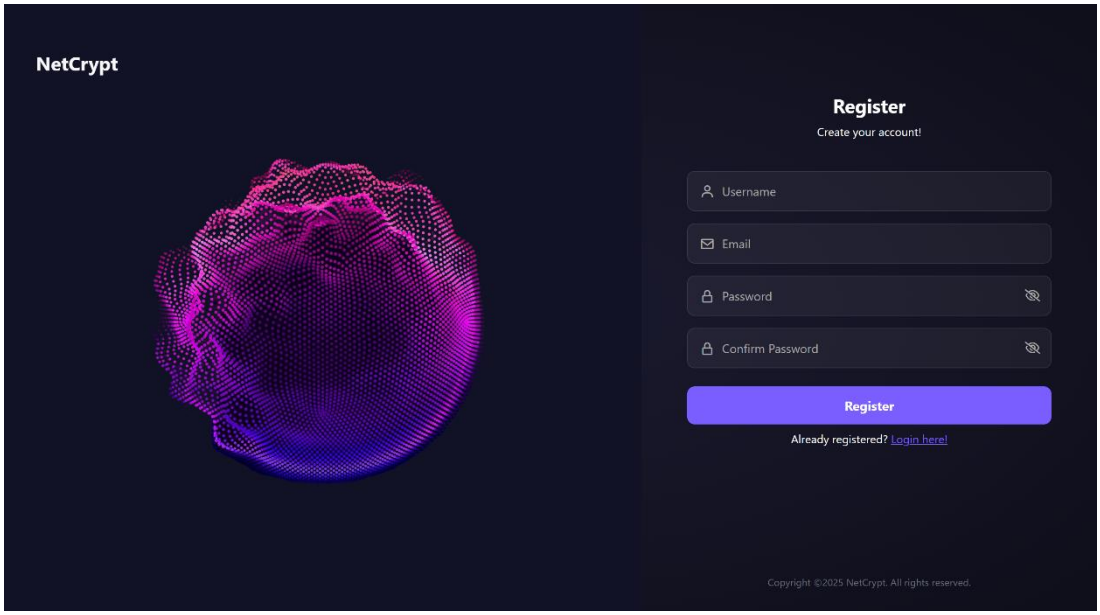
Halaman Login terdiri dari dua input utama yaitu *username* dan *password.* Tombol login akan akan mengautentikasi pengguna terhadap *database,* jika terjadi kesalahan seperti *username* atau *password* tidak sesuai maka sistem akan menampilkan pesan error yang informatif.



Gambar 5.2.5 Halaman Login

c. Halaman Registrasi

Halaman ini berisi formulir registrasi yang mencangkup username, email, dan password. Sebelum mendaftar sistem akan melakukan validasi data untuk mencegah duplikasi akun. Setelah berhasil mendaftar, pengguna akan diarahkan ke halaman login.

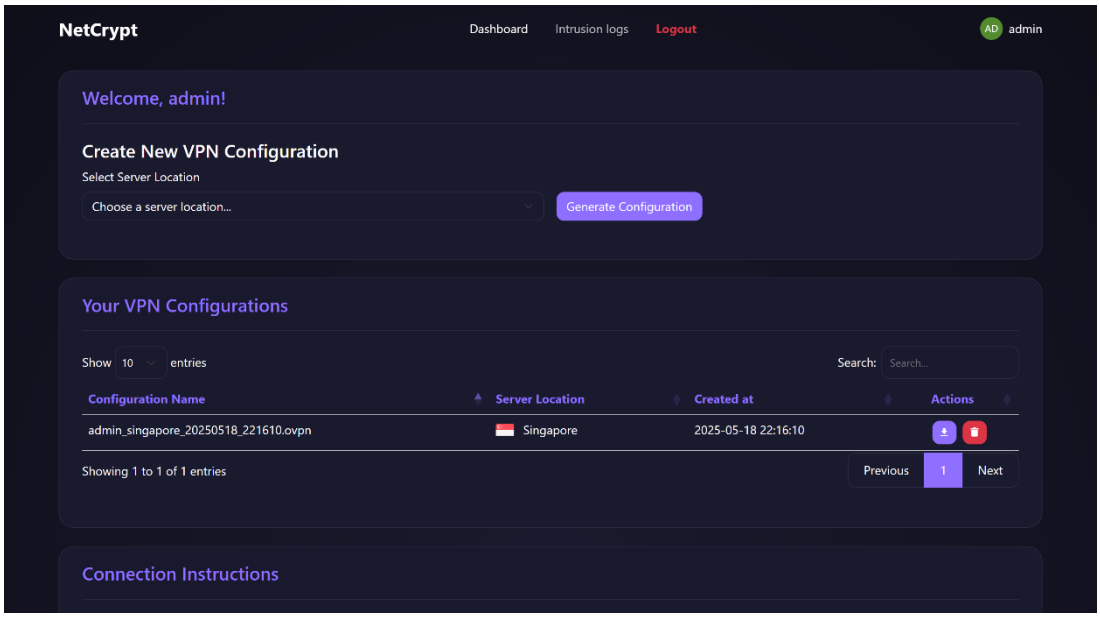


Gambar 5.2.6 Halaman Registrasi

d. Halaman Dashboard

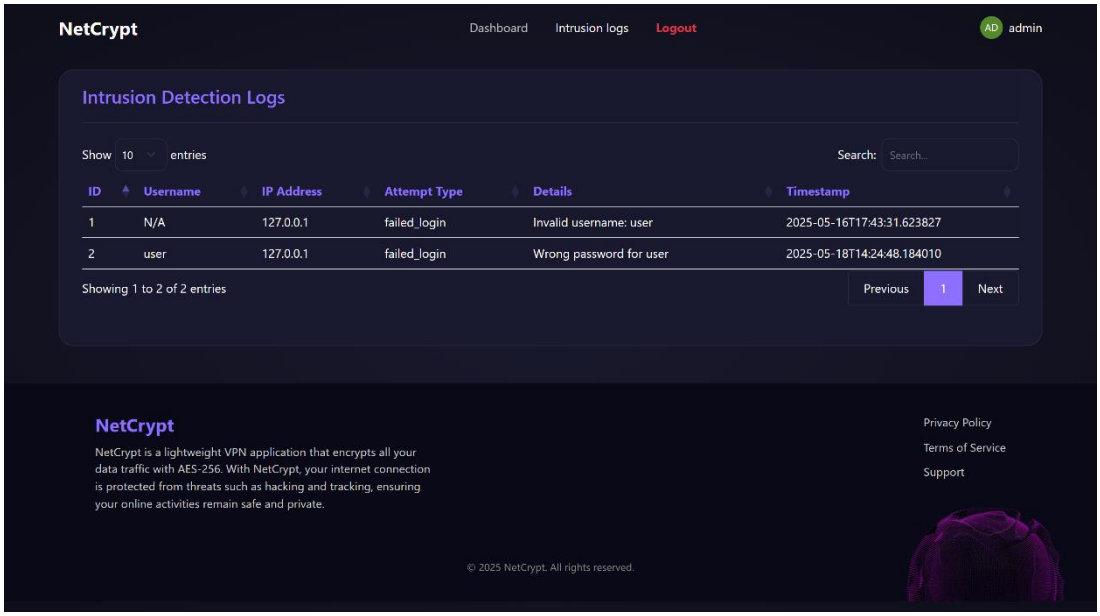
Halaman dashboard adalah halaman yang bersisi sambutan selamat datang, manajemen konfigurasi VPN seperti membuat, download, dan menghapus konfigurasi VPN. Pada halaman ini juga terdapat inturksi cara mengkoneksikan file .ovpn yang telah

didownload. Untuk membuat file konfigurasi pengguna akan memilih server VPN yang sudah disediakan lalu menekan tombol “Generate Configuration”, lalu sistem akan membuat sertifikat OpenVPN dan mengenkripsi file konfigurasi menggunakan AES-256. Sebelum pengguna mengunduh file konfigurasi yang telah dibuat, sistem akan mendekripsi file tersebut lalu file yang telah didekripsi akan ditampilkan di tabel “Your VPN Configurations”.



Gambar 5.2.7 Halaman Dashboard

e. Halaman Intrusi
Halaman ini berfungsi untuk memantau kegagalan yang terjadi pada sistem NetCrypt.



Gambar 5.2.8 Halaman Intrusi

5.3 Fungsionalitas Utama Aplikasi

NetCrypt dikembangkan dengan mengedepankan keamanan, kemudahan penggunaan, dan kemampuan untuk berkembang di masa depan. Fungsionalitas utama yang mendukung operasional aplikasi ini dijelaskan sebagai berikut:

a. Manajemen Autentikasi

NetCrypt menerapkan sistem autentikasi yang aman untuk memastikan bahwa hanya pengguna yang telah terdaftar yang dapat mengakses fitur-fitur utama aplikasi. Setiap pengguna wajib melakukan login terlebih dahulu, dan data kredensial seperti *password* disimpan dalam bentuk terenkripsi menggunakan algoritma hashing seperti SHA-256. Dengan sistem ini, *password* tidak pernah tersimpan dalam bentuk *plaintext* sehingga memberikan perlindungan yang lebih tinggi terhadap potensi pencurian data.

b. Enkripsi File

Salah satu fitur inti dari NetCrypt adalah kemampuan untuk mengenkripsi file secara aman. NetCrypt menggunakan algoritma AES-256 *(Advanced Encryption Standard)* yang telah diakui secara internasional sebagai metode enkripsi yang sangat kuat dan andal. File konfigurasi VPN yang bersifat sensitif akan dikunci menggunakan algoritma ini, dan aplikasi tidak akan pernah menyimpan data dalam bentuk asli *(plaintext).*

c. Otomatisasi Proses Sertifikat VPN

Seluruh proses sertifikasi VPN (CA, server cert, client cert) dilakukan otomatis di *backend*. Ini menyederhanakan proses yang biasanya kompleks menjadi hanya satu klik bagi pengguna.

d. Distribusi Aman

Setelah proses enkripsi dan konfigurasi selesai, distribusi file hasil enkripsi dilakukan secara aman. Akses terhadap file hanya diberikan kepada pengguna yang telah login, dan tidak ada jalur publik yang dapat digunakan untuk mengakses file secara bebas. Setiap file pengguna disimpan secara terpisah dan hanya bisa diakses oleh pemiliknya, menjaga privasi dan kerahasiaan data. Selain itu, pengguna juga diberikan opsi untuk menghapus file mereka secara permanen melalui fitur pengelolaan riwayat file, memastikan kontrol penuh terhadap data pribadi.

e. Skalabilitas

NetCrypt dirancang dengan arsitektur yang mendukung skalabilitas, memungkinkan aplikasi untuk tumbuh dan menangani jumlah pengguna serta server VPN yang lebih banyak di masa

mendatang. Sistem *backend* memungkinkan penambahan server VPN secara fleksibel, dan seluruh manajemen dapat dilakukan secara terpusat tanpa perlu melakukan konfigurasi ulang pada setiap node. Selain itu, aplikasi ini juga telah dioptimalkan sebagai *Progressive Web App* (PWA), memungkinkan pengguna untuk mengakses aplikasi secara instan melalui perangkat seluler maupun desktop. Fitur PWA memungkinkan aplikasi dapat dipasang seperti aplikasi *native* sehingga hal ini akan memberikan pengalaman pengguna yang lebih cepat, responsif, dan nyaman.

VI. MANUAL PENGGUNAAN APLIKASI

6.1 Panduan Enkripsi

Proses enkripsi pada aplikasi NetCrypt berlangsung secara otomatis saat sistem membuat dan menyimpan konfigurasi OpenVPN untuk setiap pengguna. Sistem memanfaatkan algoritma AES-256 dengan mode CBC *(Cipher Block Chaining)* yang merupakan salah satu bentuk enkripsi simetris terkuat yang tersedia saat ini. Berikut langkah-langkah penggunaannya:

a. Pengguna mendaftar dan masuk ke NetCrypt.
b. Setelah berhasil login, pengguna memilih server VPN yang tersedia.
c. Sistem akan secara otomatis membuat sertifikat dan kunci klien VPN.
d. Komponen sertifikat tersebut dienkripsi dengan kunci AES-256 secara internal.
e. Data yang sudah terenkripsi disimpan dalam *database*.
f. Tidak ada input manual dari pengguna dalam proses enkripsi, menjadikan sistem ini aman dari kesalahan pengguna.

6.2 Panduan Dekripsi

Proses dekripsi juga dilakukan secara otomatis ketika pengguna melakukan permintaan unduh konfigurasi. Berikut prosesnya:

a. Sistem membaca data konfigurasi terenkripsi dari penyimpanan atau *database*.
b. Menggunakan kunci enkripsi yang telah disimpan, sistem melakukan dekripsi.
c. Konfigurasi yang telah didekripsi dikemas dan ditawarkan kepada pengguna dalam bentuk file .ovpn.

Dekripsi ini aman karena hanya dapat dilakukan oleh sistem *backend* dengan otorisasi yang tepat. Seluruh proses ini menjaga keamanan informasi pengguna dari akses yang tidak sah.

6.3 Tips Keamanan Penggunaan

Untuk memastikan keamanan maksimal dalam penggunaan aplikasi NetCrypt, berikut adalah beberapa rekomendasi:

a. Gunakan password yang kuat dan unik saat mendaftar.
b. Jangan bagikan file konfigurasi VPN Anda kepada orang lain.
c. Selalu unduh file konfigurasi dari antarmuka resmi NetCrypt.
d. Logout setelah selesai menggunakan aplikasi untuk menghindari pembajakan sesi.

VII. PENGUJIAN DAN EVALUASI APLIKASI

7.1 Metode Pengujian

Pengujian dilakukan untuk memastikan bahwa seluruh fungsi utama aplikasi berjalan dengan baik, aman, dan sesuai dengan tujuan perancangannya.

a. Pengujian Unit (Unit Testing)
Pengujian pada fungsi-fungsi seperti `generate_vpn_certificate_components()`, `test_generate_vpn_config()`, `test_store_vpn_config()`, `test_get_user_config()`, `test_delete_vpn_config()`, `encrypt_data()`, `decrypt_data()`, untuk memastikan bahwa enkripsi, dekripsi, dan pembuatan sertifikat berjalan sesuai harapan.

Gambar 7.1.1 Hasil Unit Testing

b. Pengujian Fungsional (Functional Testing)
Tahap pengujian ini dilakukan dengan menggunakan metode *BlackBox Testing* dengan mengakses seluruh halaman aplikasi dan menguji fitur seperti registrasi, login, dan pengunduhan konfigurasi.

1. Pengujian Login

Tabel 7.1.1 Proses Pengujian BlackBox Login

No	Skenario	Hasil Pengujian	Hasil yang Diharapkan	Ket
1.	Username dan password benar	Masuk ke halaman dashboard	Masuk ke halaman dashboard	Valid
2.	Username atau password salah	Muncul pesan “Invalid username or password”	Muncul pesan “Invalid username or password”	Valid
3.	Username dan password kosong	Muncul pesan “Username and password are required”	Muncul pesan “Username and password are required”	Valid
4.	Hanya username atau hanya password yang diisi	Muncul pesan “Username and password are required”	Muncul pesan “Username and password are required”	Valid

2. Pengujian Registrasi

Tabel 7.1.2 Proses Pengujian BlackBox Registrasi

No	Skenario	Hasil Pengujian	Hasil yang Diharapkan	Ket
1.	Username (belum digunakan), email (belum digunakan) password & konfirmasi password diisi	Di arahkan ke halaman login dan muncul pesan "Registration successful! You can now log in."	Di arahkan ke halaman login dan muncul pesan "Registration successful! You can now log in."	Valid
2.	Username atau email (sudah digunakan) password & konfirmasi password diisi	Muncul pesan "Username already exists" atau "Email already exists"	Muncul pesan "Username already exists" atau "Email already exists"	Valid
3.	Username, email, password, atau konfirmasi password kosong	Muncul pesan "All fields are required"	Muncul pesan "All fields are required"	Valid
4.	Password dan konfirmasi password tidak cocok	Muncul pesan "Passwords do not match"	Muncul pesan "Passwords do not match"	Valid

3. Pengujuan Konfigurasi VPN

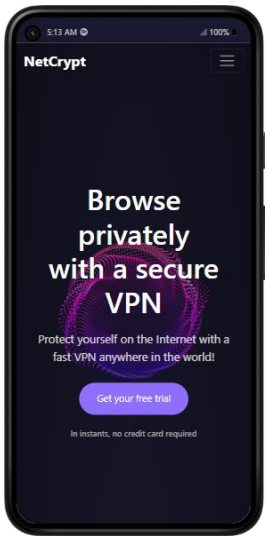
Tabel 7.1.3 Proses Pengujian BlackBox Konfigurasi VPN

No	Skenario	Hasil Pengujian	Hasil yang Diharapkan	Ket
1.	Buat Konfigurasi VPN dengan memilih server	File konfigurasi dapat dibuat	File konfigurasi dapat dibuat	Valid
2.	Buat Konfigurasi VPN tanpa memilih server	Muncul pesan "Please select an item in the list."	Muncul pesan "Please select an item in the list."	Valid
3.	Download file konfigurasi	File berhasil diunduh dan dienkripsi menggunakan AES-256	File berhasil diunduh, sudah ada *certificate* dan dienkripsi menggunakan algoritma AES-256	Valid

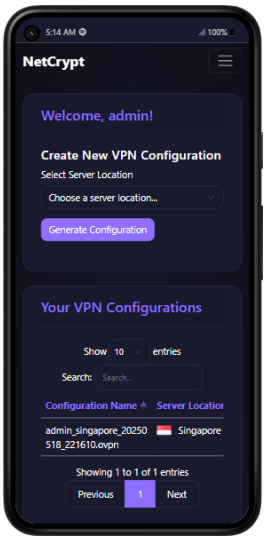
No	Skenario	Hasil Pengujian	Hasil yang Diharapkan	Ket
4.	Hapus file konfigurasi	File konfigurasi berhasil dihapus	File konfigurasi berhasil dihapus	Valid

c. Pengujian Kompabilitas Platform

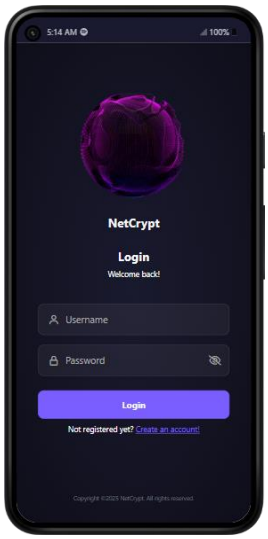
NetCrypt menggunakan framework Bootstrap untuk memastikan tampilan antarmuka yang responsif di berbagai ukuran layar dan perangkat, seperti *desktop*, *tablet*, dan *smartphone*. Selain itu, aplikasi ini dilengkapi dengan fitur *Progressive Web App* (PWA) yang memungkinkan pengguna untuk mengakses aplikasi secara optimal di berbagai platform, termasuk browser *desktop* dan *mobile*.



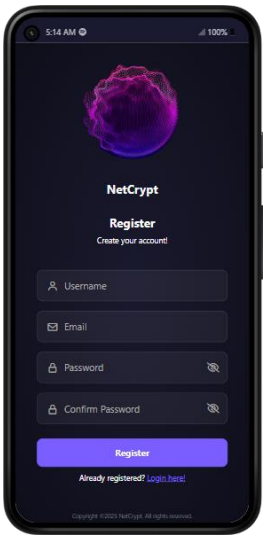
Gambar 7.1.2 Halaman Home Mobile



Gambar 7.1.3 Halaman Dashboard Mobile



Gambar 7.1.4 Halaman Login Mobile



Gambar 7.1.5 Halaman Register Mobile

7.2 Evaluasi Hasil

Hasil pengujian menunjukkan bahwa:

a. Semua fitur dapat dijalankan tanpa error yang signifikan.
b. Proses enkripsi dan dekripsi data dapat dilakukan dengan baik tanpa adanya kesalahan.
c. File konfigurasi yang dihasilkan valid dan dapat digunakan oleh klien OpenVPN.
d. Tidak ditemukan kebocoran informasi atau konfigurasi dalam bentuk *plaintext*.

Evaluasi ini juga menyarankan adanya mekanisme audit dan logging yang lebih detail untuk pemantauan potensi penyalahgunaan akun pengguna.

VIII. PENUTUP

8.1 Kesimpulan

NetCrypt berhasil memenuhi tujuannya dalam menyediakan platform pengelolaan dan distribusi file konfigurasi VPN secara aman. Dengan penerapan algoritma kriptografi AES-256 dan arsitektur berbasis Flask, sistem mampu melakukan enkripsi dan dekripsi secara efisien dan otomatis. Integrasi sistem ini dapat meminimalkan potensi kebocoran data konfigurasi VPN dan memberikan perlindungan tambahan kepada pengguna akhir.

8.2 Saran Pengembangan

Beberapa saran untuk pengembangan ke depan antara lain:

a. Penambahan autentikasi dua faktor (2FA) untuk meningkatkan keamanan akun pengguna.
b. Peningkatan antarmuka pengguna (UI/UX) agar lebih responsif dan modern.
c. Integrasi dengan email untuk notifikasi otomatis kepada pengguna tentang aktivitas akun mereka.
d. Membuat fitur rotasi otomatis sertifikat setiap periode tertentu untuk meningkatkan keamanan jangka panjang.

DAFTAR PUSTAKA

Flask Documentation – https://flask.palletsprojects.com
NetCrypt Repository - https://github.com/Superior231/NetCrypt
OpenVPN – https://openvpn.net
PyCryptodome Documentation – https://pycryptodome.readthedocs.io

LAMPIRAN