Perancangan Infrastruktur Jaringan Aman dan Implementasi Kriptografi pada Sistem "FinTech SecureCorp"

Anggota Kelompok:

Daffa Wardhanaditya Junaidi – 2702750703

Kevin Sebastian – 2702746012

Joshua Verbiano Inkiriwang – 2702745501

Name of Lecturer : Dr. Rojali, S.Si, M.Si. & Dr.Eng. Nico Surantha, S.T., M.T.

Topic : Network and Cyber Security

Class : Network and Cyber Security

BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan layanan keuangan berbasis teknologi (*Financial Technology* / FinTech) telah mendorong peningkatan kebutuhan akan infrastruktur jaringan yang andal dan aman. Sistem pembayaran digital, aplikasi keuangan, serta pengelolaan data nasabah menuntut ketersediaan layanan yang tinggi sekaligus perlindungan terhadap data sensitif. Di sisi lain, sektor keuangan merupakan salah satu target utama serangan siber, seperti *Distributed Denial of Service* (DDoS), SQL *Injection* (SQLi), dan *data breach*, yang dapat berdampak langsung pada kepercayaan pengguna dan keberlangsungan bisnis.

Dalam konteks tersebut, keamanan jaringan tidak lagi dipandang semata-mata sebagai isu teknis, melainkan sebagai bagian dari strategi Teknologi Informasi dan Komunikasi (TIK) yang berperan penting dalam mendukung operasional dan tata kelola organisasi. Oleh karena itu, diperlukan suatu perancangan infrastruktur jaringan yang tidak hanya memenuhi kebutuhan fungsional, tetapi juga mampu menerapkan prinsip keamanan secara sistematis dan terukur. Studi kasus pada penelitian ini menggunakan perusahaan fiktif FinTech SecureCorp, yang merepresentasikan sebuah organisasi FinTech dengan kebutuhan pemisahan jaringan antara layanan publik, jaringan internal pengguna, dan *server* dengan tingkat sensitivitas tinggi. Perancangan dilakukan untuk menghasilkan desain jaringan yang aman, terstruktur, serta dapat divalidasi melalui simulasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah pada penelitian ini difokuskan pada satu pertanyaan utama sebagai berikut:

> Bagaimana merancang infrastruktur jaringan yang aman dan tersegmentasi untuk mendukung layanan FinTech, serta memitigasi ancaman keamanan jaringan melalui penerapan kebijakan keamanan dan kriptografi?

Rumusan masalah ini dipilih secara terfokus agar pembahasan dapat diarahkan pada aspek perancangan jaringan dan strategi keamanan, tanpa melebar ke implementasi operasional skala produksi.

1.3 Tujuan dan Keluaran

Tujuan dari *project* ini adalah sebagai berikut:

1. Merancang topologi jaringan yang menerapkan segmentasi keamanan menggunakan konsep *Demilitarized Zone* (DMZ), *Virtual LAN* (VLAN), dan *Server Farm*.
2. Menyusun skema pengalamatan IP dan *subnetting* yang efisien menggunakan metode *Variable Length Subnet Mask* (VLSM).
3. Menganalisis dan merekomendasikan mekanisme keamanan jaringan untuk memitigasi ancaman siber berlapis (*Defense in Depth*) menggunakan *firewall*, *Access List* (ACL), *Intrusion Detection System* (IDS), dan Kriptografi (AES-256 & TLS 1,3).
4. Memvalidasi desain jaringan melalui simulasi menggunakan Cisco Packet Tracer untuk memvalidasi desain.

Adapun keluaran (*output*) yang dihasilkan dari *project* ini meliputi:

- Dokumen perancangan infrastruktur jaringan dan kebijakan keamanan
- *File* simulasi jaringan menggunakan Cisco Packet Tracer
- *Source code* yang merepresentasikan penerapan kriptografi pada sistem aplikasi
- Media presentasi dan dokumentasi pengujian

1.4 Batasan Masalah

Agar *project* ini tetap terarah dan sesuai dengan tujuan pembelajaran, maka ditetapkan beberapa batasan masalah sebagai berikut:

1. Perancangan jaringan difokuskan pada desain logis dan strategis, bukan implementasi fisik di lingkungan produksi.
2. Simulasi jaringan dilakukan menggunakan Cisco Packet Tracer dengan keterbatasan fitur yang dimiliki oleh perangkat simulasi.

3. Mekanisme keamanan yang dibahas mencakup segmentasi jaringan, *firewall* berbasis *Access Control List* (ACL), *Network Address Translation* (NAT), serta penerapan kriptografi dasar.
4. Deteksi serangan dan ancaman dibahas pada tingkat konseptual dan simulatif, tanpa implementasi penuh sistem IDS/IPS nyata.
5. Studi kasus menggunakan organisasi fiktif sebagai representasi lingkungan FinTech.

Dengan batasan tersebut, penelitian ini diharapkan dapat memberikan gambaran yang jelas dan terfokus mengenai perancangan infrastruktur jaringan yang aman dalam konteks sistem FinTech.

BAB 2

PERANCANGAN JARINGAN DAN TOPOLOGI

2.1 Pendekatan Perancangan Jaringan

Perancangan infrastruktur jaringan pada studi kasus FinTech SecureCorp menggunakan pendekatan topologi hierarkis yang terdiri dari lapisan *edge*/perimeter, *distribution,* dan *access*. Pendekatan ini dipilih karena mampu meningkatkan skalabilitas, kemudahan pengelolaan serta mendukung penerapan kebijakan keamanan secara terstruktur. Dalam konteks keamanan jaringan, topologi hierarkis juga memudahkan penerapan prinsip *defense in depth* dengan membagi jaringan ke dalam beberapa zona keamanan yang memiliki fungsi dan tingkat risiko berbeda. *Firewall Router* berperan sebagai *edge router* yang menjadi gerbang utama antara jaringan internal perusahaan dan jaringan eksternal (Internet). Seluruh lalu lintas masuk dan keluar jaringan perusahaan dikendalikan melalui perangkat ini, sehingga kebijakan keamanan dapat diterapkan secara terpusat.

2.2 Segmentasi Jaringan dan Zona Keamanan

Untuk mengurangi *attack surface* dan membatasi pergerakan penyerang (*lateral movement*), jaringan FinTech SecureCorp dibagi ke dalam beberapa zona keamanan sebagai berikut:

1. Zona Eksternal (Internet)

Zona ini merepresentasikan jaringan publik yang tidak dapat dipercaya. Akses dari zona ini hanya diperbolehkan menuju layanan tertentu yang berada di DMZ melalui mekanisme *firewall* dan NAT.

2. Zona DMZ (*Demilitarized Zone*)

Zona DMZ digunakan untuk menempatkan layanan publik seperti *Web Server* dan *Mail Server*. Zona ini dapat diakses dari jaringan eksternal, namun tidak memiliki akses langsung ke jaringan internal perusahaan. Pemisahan ini bertujuan untuk melindungi jaringan internal apabila terjadi *incident* pada layanan publik.

3. Zona Internal (*User Network*)

Zona ini digunakan oleh karyawan perusahaan dan dipisahkan kembali menggunakan *Virtual LAN* (VLAN) berdasarkan fungsi kerja, yaitu *Finance &* HR, *General Staff* dan IT *Administration*. Segmentasi ini bertujuan untuk membatasi akses antar divisi dan mengurangi risiko kebocoran data sensitif.

4. Zona Server Farm (*Secure Zone*)

Zona ini berisi server dengan tingkat sensitivitas tinggi, seperti *Database Server* dan *Application Server*. Akses ke zona ini sangat dibatasi dan hanya diperbolehkan dari segmen tertentu sesuai dengan kebijakan keamanan yang telah ditentukan.

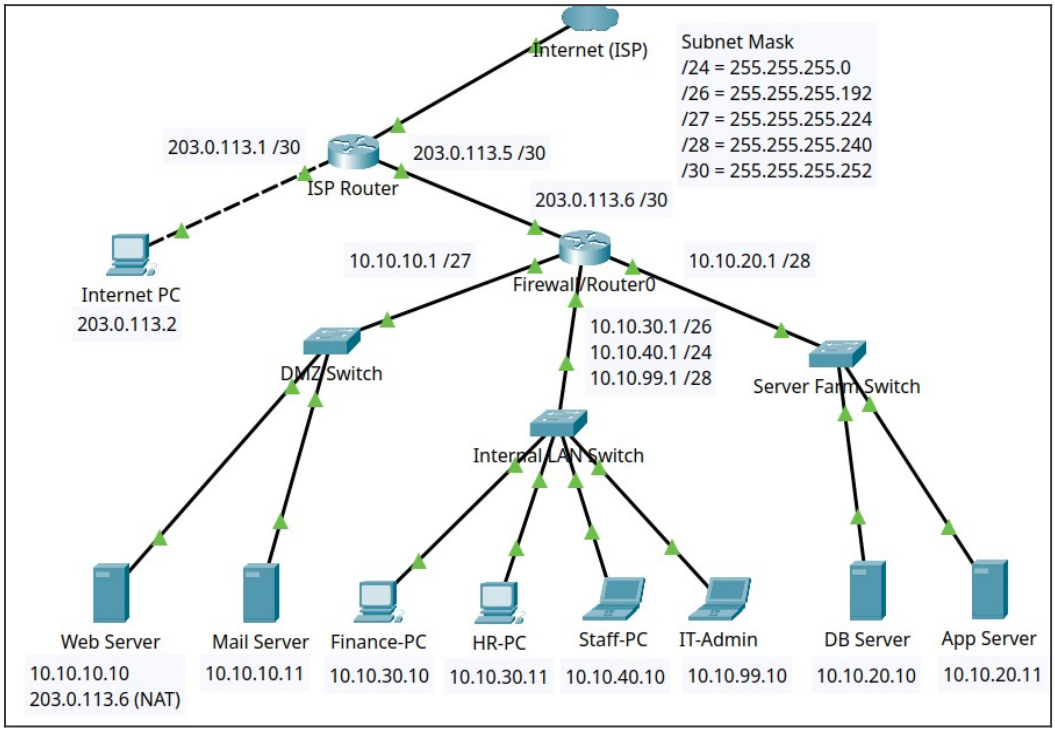
2.3 Desain Topologi Logis Jaringan

Topologi jaringan dirancang secara logis dengan memisahkan setiap zona menggunakan perangkat jaringan yang terhubung ke *firewall router*. Seluruh komunikasi antar zona harus melewati *firewall*, sehingga dapat diawasi dan di*filter* menggunakan aturan keamanan seperti ACL dan NAT.

Penggunaan topologi ini memungkinkan :

- Isolasi layanan publik dari jaringan internal
- Pengendalian akses antar segmen jaringan
- Kemudahan monitoring dan pengelolaan trafik
- Peningkatan keamanan secara menyeluruh

Gambar 2.1 menunjukkan topologi logis jaringan FinTech SecureCorp yang diimplementasikan menggunakan Cisco Packet Tracer.



Gambar 2.1 Topologi Logis Jaringan dan Segmentasi Keamanan FinTech SecureCorp

2.4 Perancangan IP *Address* dan *Subnetting*

Skema pengalamatan IP menggunakan alamat privat kelas A 10.0.0.0/8 dengan penerapan *Variable Length Subnet Mask* (VLSM). Metode ini dipilih untuk meningkatkan efisiensi penggunaan alamat IP sekaligus menyesuaikan ukuran *subnet* dengan kebutuhan masing-masing segmen jaringan.

Tabel 2.1 Penentuan IP Address untuk masing-masing segmen

Nama Segmen	Subnet	Range IP Address	Keterangan
DMZ	/27	10.10.10.1 - 10.10.10.30	*Web* & *Mail Server*
Server Farm	/28	10.10.20.1 - 10.10.20.14	*Database* & *App Server*
Finance & HR	/26	10.10.30.1 - 10.10.30.62	Divisi Sensitif
General Staff	/24	10.10.40.1 - 10.10.40.254	Karyawan Umum
IT Administation	/28	10.10.99.1 - 10.10.99.14	Admin & *Monitoring*

Pemilihan ukuran *subnet* didasarkan pada jumlah perangkat, tingkat sensitivitas data, serta kebutuhan keamanan masing-masing segmen. Segmen dengan data sensitif seperti *Server Farm* dan IT *Administration* menggunakan *subnet* yang lebih kecil untuk meminimalkan *exposure* jaringan.

2.5 Desain *Routing* dan Akses Jaringan

Firewall router menggunakan *default route* (0.0.0.0/0) untuk meneruskan seluruh trafik yang tidak ditujukan ke jaringan internal menuju ISP. Pendekatan ini mencerminkan desain nyata pada jaringan *enterprise*, dimana *edge router* tidak menyimpan seluruh informasi *routing internet*, melainkan bergantung pada *upstream* ISP. Seluruh komunikasi antar zona dikontrol menggunakan kebijakan *routing* dan ACL, sehingga hanya trafik yang diizinkan yang dapat melintas. Dengan desain ini, jaringan FinTech SecureCorp memiliki struktur yang jelas, aman, dan mudah dikembangkan di masa depan.

BAB 3

ANALISIS DAN REKOMENDASI KEAMANAN

3.1 Identifikasi Ancaman Keamanan Jaringan

Berdasarkan karakteristik layanan FinTech dan arsitektur jaringan yang dirancang, terdapat beberapa ancaman keamanan utama yang berpotensi menyerang sistem FinTech SecureCorp. Ancaman tersebut berasal baik dari pihak eksternal maupun internal, serta dapat menargetkan lapisan jaringan maupun aplikasi. Ancaman keamanan yang diidentifikasi antara lain:

1. Serangan terhadap layanan publik

Layanan yang berada di zona DMZ, seperti *web server*, berpotensi menjadi target serangan DDOS, *port scanning* dan eksploitasi kerentanan aplikasi web seperti SQLi.

2. Akses tidak sah ke *server* internal

Apabila segmentasi jaringan tidak diterapkan dengan baik, penyerang yang berhasil mengompromi layanan publik dapat melakukan *lateral movement* menuju *server* internal, khususnya *database server* yang menyimpan data sensitif nasabah.

3. Ancaman dari jaringan internal *(insider threat)*

Pengguna internal dengan hak akses terbatas berpotensi melakukan akses yang tidak semestinya ke segmen jaringan lain apabila tidak terdapat pembatasan berbasis kebijakan jaringan.

4. Penyadapan dan manipulasi data

Data yang ditransmisikan tanpa mekanisme pengamanan dapat disadap atau dimodifikasi oleh pihak yang tidak berwenang, terutama pada komunikasi antara klien dan *server* aplikasi.

3.2 Analisis Mekanisme Keamanan Jaringan

Untuk memitigasi ancaman tersebut, desain jaringan FinTech SecureCorp menerapkan beberapa mekanisme keamanan utama yang saling melengkapi.

3.2.1 Segmentasi Jaringan dan DMZ

Penerapan segmentasi jaringan menggunakan VLAN dan zona DMZ bertujuan untuk membatasi ruang lingkup serangan. Layanan publik ditempatkan pada zona DMZ yang terisolasi dari jaringan internal, sehingga kompromi pada layanan publik tidak secara langsung memberikan akses ke *server* internal. Segmentasi ini mendukung prinsip *defense in depth*, di mana kegagalan pada satu lapisan keamanan tidak serta-merta menyebabkan kompromi seluruh sistem.

3.2.2 *Firewall* dan ACL

Firewall router digunakan sebagai mekanisme pengendali lalu lintas antar zona jaringan. Kebijakan keamanan diterapkan melalui ACL untuk menentukan jenis trafik yang diperbolehkan maupun ditolak. Sebagai contoh, trafik dari jaringan pengguna umum dibatasi agar tidak dapat mengakses *server farm* secara langsung. Sebaliknya, akses dari *web server* di DMZ ke *database server* hanya diperbolehkan pada *port* dan protokol tertentu sesuai kebutuhan aplikasi. Pendekatan ini menerapkan prinsip *least privilege*, di mana setiap segmen jaringan hanya diberikan akses minimum yang diperlukan untuk menjalankan fungsinya.

Selain mekanisme *firewall* dan segmentasi jaringan, pengaturan *routing* juga berperan dalam mendukung keamanan jaringan. Pada desain ini digunakan *static routing* karena topologi jaringan bersifat kecil, terkontrol, dan tidak mengalami perubahan jalur komunikasi secara dinamis. Penggunaan *routing protocol* dinamis seperti RIP tidak memberikan manfaat signifikan dalam konteks ini dan berpotensi menambah kompleksitas konfigurasi. Oleh karena itu, *static routing* dipilih untuk menjaga kesederhanaan desain serta kejelasan alur komunikasi antar jaringan.

3.2.3 *Network Address Translation* (NAT)

NAT digunakan untuk menyembunyikan alamat IP internal dari jaringan publik, Layanan publik di DMZ dipublikasikan menggunakan *static* NAT berbasis *port* (*port forwarding*), sehingga hanya *port* layanan tertentu seperti HTTP dan HTTPS yang dapat diakses dari luar jaringan. Penggunaan NAT ini mengurangi *exposure* jaringan internal dan membantu membatasi *attack surface* dari jaringan eksternal.

3.3 Analisis Mekanisme Keamanan Jaringan

3.3.1 Keamanan Data dalam Transmisi (*Data in Transit*)

Untuk melindungi data yang dikirimkan antara klien dan *server* aplikasi, sistem menerapkan protokol HTTPS dengan dukungan SSL/TLS. Penggunaan TLS bertujuan untuk menjamin kerahasiaan dan integritas data, serta mencegah serangan *Man-in-the-Middle* (MitM). Dengan mekanisme ini, informasi sensitif seperti *credentials* pengguna dan data transaksi tidak dapat dibaca atau dimodifikasi oleh pihak yang tidak berwenang selama proses transmisi.

3.3.2 Keamanan Data Tersimpan (*Data at Rest*)

Data sensitif yang disimpan pada *database server* dilindungi menggunakan mekanisme kriptografi simetris dengan algoritma *Advanced Encryption Standard* (AES-256). Enkripsi data bertujuan untuk menjaga kerahasiaan informasi nasabah apabila terjadi akses tidak sah ke media penyimpanan. Pengelolaan kunci enkripsi dilakukan secara terpisah dari data yang dienkripsi untuk mengurangi risiko kebocoran kunci.

3.4 Deteksi Serangan dan Identifikasi Kerentanan

Deteksi serangan dan identifikasi kerentanan pada desain ini dilakukan pada tingkat konseptual dan simulatif. Sistem direkomendasikan untuk menggunakan *Intrusion Detection System* (IDS) berbasis *signature*, seperti Snort, guna mendeteksi pola serangan yang umum terjadi, antara lain *port scanning* dan serangan *Distributed Denial of Service* (DDoS). Pada tahap simulasi menggunakan Cisco Packet Tracer, pengujian dilakukan dengan memverifikasi bahwa trafik yang tidak diizinkan diblokir oleh kebijakan ACL sementara trafik yang sah dapat berjalan sesuai dengan kebutuhan layanan.

3.5 Rekomendasi Pengembangan Keamanan

Berdasarkan hasil analisis, beberapa rekomendasi pengembangan keamanan yang dapat diterapkan pada implementasi nyata antara lain:

1. Penerapan IDS/IPS secara penuh pada lingkungan produksi untuk meningkatkan kemampuan deteksi dan respon terhadap serangan.
2. Penggunaan *Next-Generation Firewall* (NGFW) dengan fitur *deep packet inspection* untuk meningkatkan keamanan aplikasi.

3. Implementasi mekanisme autentikasi yang lebih kuat, seperti *multi-factor authentication* pada sistem manajemen dan administrasi.
4. Penerapan kebijakan keamanan berbasis standar dan regulasi yang berlaku pada sektor keuangan

Dengan penerapan rekomendasi tersebut, sistem FinTech SecureCorp diharapkan mampu menghadapi ancaman keamanan jaringan yang semakin kompleks secara lebih efektif.

BAB 4

IMPLEMENTASI

4.1 Implementasi Topologi Jaringan

Implementasi topologi jaringan pada penelitian ini dilakukan menggunakan aplikasi Cisco Packet Tracer sebagai media simulasi. Topologi yang diimplementasikan mengacu pada desain logis yang telah dibahas pada Bab II, dengan menerapkan pemisahan zona jaringan yang terdiri dari jaringan publik (Internet), zona DMZ, server farm, serta jaringan internal pengguna.

Perangkat utama yang digunakan dalam simulasi meliputi router sebagai firewall perimeter, switch untuk segmentasi VLAN, serta server dan klien sebagai representasi layanan dan pengguna. Setiap segmen jaringan dikonfigurasikan dengan skema pengalamatan IP yang berbeda untuk memastikan isolasi dan pengendalian lalu lintas antar zona. Simulasi ini bertujuan untuk memvalidasi bahwa desain jaringan dapat berjalan secara fungsional sekaligus mendukung kebijakan keamanan yang telah direncanakan.

4.2 Skema Pengalamatan IP

Pengalamatan IP pada jaringan dirancang menggunakan metode Variable Length Subnet Mask (VLSM) untuk mengoptimalkan penggunaan alamat IP dan memisahkan setiap segmen jaringan sesuai kebutuhan fungsional dan tingkat keamanan.

Tabel 4.1. IP Address untuk masing-masing perangkat

Nama Perangkat	Interface	IP Address with Subnet Mask	Keterangan
Web Server	FastEthernet0	10.10.10.10/27	DMZ Network
Mail Server	FastEthernet0	10.10.10.11/27	DMZ Network
Finance-PC	FastEthernet0	10.10.30.10/26	Internal LAN
HR-PC	FastEthernet0	10.10.30.11/26	Internal LAN
Staff-PC	FastEthernet0	10.10.40.10/24	Internal LAN
IT-Administator	FastEthernet0	10.10.99.10/28	Internal LAN
Database Server	FastEthernet0	10.10.20.10/28	Server Farm
App Server	FastEthernet0	10.10.20.11/28	Server Farm
Firewall/Router0	FastEthernet0/0/0	10.10.10.1/27	R0 <-> DMZ
	FastEthernet0/0/1	VLAN 30 : 10.10.30.1/26 VLAN 40 : 10.10.40.1/24 VLAN 99 : 10.10.99.1/28	R0 <-> Internal LAN
	FastEthernet0/0/2	10.10.20.1/28	R0 <-> Server

			Farm
	Gigabit0/1	203.0.113.6/30	R0 <-> ISP Router
ISP Router	Gigabit0/1	203.0.113.5/30	ISP Router <-> R0
	Gigabit0/2	203.0.113.1/30	ISP Router <-> Internet PC
Internet / Outside PC	FastEthernet0	203.0.113.2 /30	Internet User Representative

Skema pengalamatan ini memastikan bahwa setiap segmen jaringan memiliki ruang alamat yang cukup dan tidak saling tumpang tindih.

4.3 Implementasi Keamanan Jaringan

Implementasi keamanan jaringan dilakukan melalui konfigurasi *firewall* berbasis ACL dan NAT pada *router* perimeter. ACL digunakan untuk membatasi akses antar segmen jaringan, khususnya untuk mencegah akses langsung dari jaringan internal pengguna ke *server farm* tanpa melalui mekanisme yang telah ditentukan. Sementara itu, NAT statis berbasis *port* digunakan untuk mempublikasikan layanan *web* pada zona DMZ ke jaringan publik, sehingga hanya port HTTP dan HTTPS yang dapat diakses dari luar jaringan. Pengujian dilakukan dengan mensimulasikan lalu lintas yang diizinkan dan ditolak, serta memverifikasi bahwa kebijakan keamanan berjalan sesuai dengan rancangan. Penerapan TLS difokuskan pada layanan *web* yang diakses oleh klien *eksternal*, karena segmen ini memiliki tingkat risiko tertinggi terhadap penyadapan dan serangan *Man-in-the-Middle*.

4.4 Implementasi Kriptografi Menggunakan AES

Implementasi keamanan data pada sistem ini menggunakan algoritma simetris AES-256-CBC (*Advanced Encryption Standard*) untuk melindungi kerahasiaan data transaksi nasabah. Implementasi ini mencakup modul enkripsi pada level aplikasi (*application layer*) yang memastikan data sudah terenkripsi sebelum disimpan ke dalam basis data.

4.4.1 Arsitektur dan Alur Enkripsi

Sistem dirancang dengan arsitektur *Encryption in Transit and Rest* dimana *web server* bertindak sebagai titik enkripsi/dekripsi. *Database server* hanya menyimpan data dalam format *ciphertext*.

Skema alur data:

1. Finance-PC (*Client*) mengirim data transaksi *plaintext* ke *web server* melalui saluran aman.
2. *Web server* menerima data, men-generate *Initialization Vector* (IV) acak, dan melakukan enkripsi: $C = E_K(P, IV)$ *Dimana* C *adalah Ciphertext,* E *adalah fungsi enkripsi AES-256,* K *adalah Kunci 256-bit, dan* P *adalah Plaintext.*
3. *Web Server* mengirim pasangan $(IV, Ciphertext)$ ke *Database Server*.
4. *Database Server* menyimpan data terenkripsi tersebut.

4.4.2 Implementasi Kode

Modul kriptografi diimplementasikan menggunakan pustaka Python PyCryptodome. Berikut adalah kode inti dari modul DataProtector:

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
import base64


class DataProtector:
    def __init__(self, key):
        self.key = key  # Kunci 256-bit (32 bytes)


    def encrypt_data(self, raw_data):
        # 1. Init Cipher dengan IV acak
        cipher = AES.new(self.key, AES.MODE_CBC)
        # 2. Padding data & Enkripsi
        ct_bytes = cipher.encrypt(pad(raw_data.encode(), AES.block_size))
        # 3. Encode hasil ke Base64
        iv = base64.b64encode(cipher.iv).decode('utf-8')
        ct = base64.b64encode(ct_bytes).decode('utf-8')
        return {'iv': iv, 'ciphertext': ct}


    def decrypt_data(self, enc_dict):
        iv = base64.b64decode(enc_dict['iv'])
        ct = base64.b64decode(enc_dict['ciphertext'])
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        return unpad(cipher.decrypt(ct), AES.block_size).decode('utf-8')
```

4.4.3 Hasil Pengujian Sistem

Simulasi dilakukan dengan skenario transaksi pembayaran vendor dan penggajian (*payroll*) pada jaringan internal Fintech. Berikut ini adalah log dari Web Server yang menunjukkan proses enkripsi berjalan *real-time*:

```
2026-02-06 14:37:44 | WEB-SERVER | INFO | [INCOMING] Payment request from 10.10.30.10
2026-02-06 14:37:44 | WEB-SERVER | INFO | Processing: TRX-20260206143744 | Type:
vendor_payment
2026-02-06 14:37:44 | WEB-SERVER | INFO | Encrypting payload (AES-256-CBC)...
2026-02-06 14:37:44 | WEB-SERVER | INFO | Sending encrypted data to DB Server...
2026-02-06 14:37:46 | WEB-SERVER | INFO | [SUCCESS] Transaction stored securely.
```

4.4.4 Verifikasi Data Tersimpan (*Database*)

Data yang tersimpan pada tabel `transactions` di *database server* terbukti terenkripsi dan tidak dapat dibaca tanpa kunci. Berikut sampel data hasil *dump* dari *database*:

```
Transaction #1
  Tx ID       : TRX-20260206143757
  Created At  : 2026-02-06T14:37:59.095115
  Source IP   : 10.10.30.10
  Key Ref     : MASTER_KEY_001
  IV (Base64) : QsM0JERTKTmXTVif0rsCfA==
  Ciphertext  :
G2CLt3xJes4USzMpDGu6JLOsY2HeO9PnK+sf49C9Oq3D+bEgrFM3hll0LrOJJgmAffNVTWL6ik7AOGCkpwiF7T+tufN
D8O9iLBYnbukCXDMc5dQ+eSd+TNuNRqkr9NyiFz9E8GtMxTjoksQ5BeY7CA/Sr6wDh0hJ+KC8/
TD4Mt0BGqiFL5SfH18nvT20nQDpzd52Ern/dmWoeS8rlQYG7z3dyM+quOvWWxE/FBkk4l8qW5By+byV/
A9ZP0LoFaediMPo95yH6hVkhhhjjvyvLYvuFgzqWOSWLFzv8JtfXTLtQ83pgiwIdUW0JTKfCu3JzmAgT1kSKkVjb4Pi
7Twe34urUUSyw6uKdCr11f9Da6E1M1fyaHCoxT5imMXyAW/
74OUJuvxIWMOTC0aQVVe95MrzyDaE5u1fC+33N0rWm4Wxb9YvewmtfWPNToe0T01nMuRvdwZ6nrHDdkqZ5+J7vL8FeZ
j0QcWcfSq9ciOsuVNJTzBjw0e3UEUdwGg56InS
----------------------------------------
Transaction #2
  Tx ID       : TRX-20260206143750
  Created At  : 2026-02-06T14:37:52.996663
  Source IP   : 10.10.30.10
  Key Ref     : MASTER_KEY_001
  IV (Base64) : qF42+x35pR/Lr6Ilz1wI5g==
  Ciphertext  :
AqzAVPkqqMPLBAr4T8+v/HSExY7UwwxronPer0jyR7JbhKKVkxJ4kR2mhnJHjjENc0U99sKV1hQvhsG4H1uJqvHtVAP
USMBxr0c0pjEi7DaeRMjvHOu6+HVaCNVrHbxLLHU4idAa4XiOzIMxw3X0gmWEI/
XiDaB8I6HXYvqA2yVm0ecxv5gpViYLklvKML/ur3mpy/g/c58raR9hEM5Yqzx3rKv6sUyHk+N4o476kTc3JfKF/
kPr6uUgIGPzPjwYqbmrGQzQErWNh3BJO/
I2qUV7hFl34aekdaq8RRkIKWcowk2k4bXQgSc5bgte1e0jjoHtmyetD8+3jP0Iue8Euez4JDEoiNvNoQBCAMU/
Bs0K0lQhg/99qrVCoxZyiBAGSXY+SrdbmO1Q5BkACiYukJ3OkluFbwzf4BrkAMKwAe/v+oQCb04PT1ujA9tHsgl/
IV7LJyfKJ5+S50yUXfMW2Y49GNf8s2jiWmIJRUJsm+8=
----------------------------------------
Transaction #3
  Tx ID       : TRX-20260206143744
  Created At  : 2026-02-06T14:37:46.856660
  Source IP   : 10.10.30.10
  Key Ref     : MASTER_KEY_001
  IV (Base64) : haHfcPnb+r+61LKKC7aCHw==
  Ciphertext  :
```

```
6YF/KTZy2Okw8FWqJNxj+1DA8TJi1Uq6dX/IOIRSYZuHw8+xoSHvpcwuXoDjlZrr7pjmokLhlWSAJ9gmGqdNpwiU5mh
sCCxxL3Mk8mhbj2yG1BgR6gnbKxHYKvPy4sYpM0dSd+PJcFLLfzlEqdwLmE0OhiuK0kfvwKXJjY818WkzInCRTiA3QP
QRYpqkzB6V6p2mKKIFf6FYorgOt/AyloCmmVfeSEibIcyXU/Jrc4Rksd1r+59/xr6ASCdD5lBNUfl/D/
IWkn8tx6cmKPW/vexkseiZ2sauGp0hDmGZQYkba34S8Js+MIdTI+9W3nP4TA8gK5FGJjMvpx/
Vl+p5Tyr5CnO2jtwuS7UoogMwAGcEg/
4u1VvULwxBpBprWuseuaR2gXzJcD4+JEHGRB3M31dEHL2zWpWZiu6WsgOcG9PTORT1ObGvBDsjV4FPJPSq+gIiZnnOd
WHrwX42czAW/spG+lH4AoGkTSd1RshOUmabNlKBIVn38XtRuB5vemGP
```

Berikut kunci pada tabel ‘encryption_keys’ di *database server* yang digunakan sebagai kunci utama proses transaksi pada modul DataProtector.

```
Item #1
  Key ID      : MASTER_KEY_001
  Key (Hex)   : 5da7de6d73152c9ecb1b42399240be247b4721957f346f99bd53554c68239a81
  Created At  : 2026-02-06T14:22:44.837394
  Status      : active
```

Berikut data pada tabel ‘transaction’ di *database server* yang sudah dilakukan *decryption* menggunkan MASTER_KEY_001.

```
Transaction #1
  PLAINTEXT   :
{
    "transaction_id": "TRX-20260206143757",
    "payment_type": "settlement",
    "from_account": "1300098765432",
    "to_account": "020601002345305",
    "amount": 42500000,
    "currency": "IDR",
    "description": "Settlement Harian Mitra UMKM",
    "beneficiary_name": "Paguyuban Kuliner Nusantara",
    "beneficiary_bank": "BRI",
    "timestamp": "2026-02-06T14:37:57.044701",
    "source_ip": "10.10.30.10"
}
--------------------------------------------------------------------------------
Transaction #2
  PLAINTEXT   :
{
    "transaction_id": "TRX-20260206143750",
    "payment_type": "payroll",
    "from_account": "1300098765432",
    "to_account": "1300012345678",
    "amount": 18500000,
    "currency": "IDR",
    "description": "Gaji Karyawan - Feb 2026 - Staff IT Senior",
    "beneficiary_name": "Budi Santoso",
    "beneficiary_bank": "Mandiri",
    "timestamp": "2026-02-06T14:37:50.944301",
    "source_ip": "10.10.30.10"
}
--------------------------------------------------------------------------------
Transaction #3
  PLAINTEXT   :
{
    "transaction_id": "TRX-20260206143744",
    "payment_type": "vendor_payment",
    "from_account": "1300098765432",
    "to_account": "8210987654",
    "amount": 150000000,
    "currency": "IDR",
    "description": "Pembayaran Server Colocation Q1 2026",
    "beneficiary_name": "PT. Data Center Indonesia",
    "beneficiary_bank": "BCA",
    "timestamp": "2026-02-06T14:37:44.818330",
    "source_ip": "10.10.30.10"
}
```

4.4.5 Kesimpulan Implementasi

Implementasi AES-256 pada sistem ini berhasil memenuhi aspek *Confidentiality*. Dengan memisahkan proses enkripsi di *Web Server* dan penyimpanan di *Database Server*, sistem meminimalkan risiko perparian data jika *database server* berhasil disusupi, karena penyerang hanya akan mendapatkan data acak (*ciphertext*) tanpa kunci dekripsinya.

4.5 Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan bahwa rancangan jaringan dan mekanisme keamanan dapat berjalan sesuai dengan tujuan penelitian. Pengujian yang dilakukan meliputi:

1. Pengujian konektivitas jaringan, bertujuan untuk memastikan setiap segmen jaringan dapat berkomunikasi sesuai kebijakan yang ditetapkan
2. Pengujian kebijakan keamanan, dengan memverifikasi bahwa trafik yang tidak diizinkan diblokir oleh ACL.
3. Pengujian kriptografi, dengan memastikan data yang dienkripsi menggunakan modul AES dapat didekripsi kembali dengan benar.

Hasil pengujian menunjukkan bahwa desain jaringan dan mekanisme keamanan yang diterapkan telah berfungsi sesuai dengan perancangan.

4.6 Dokumentasi Implementasi

Sebagai bagian dari dokumentasi, *project* ini dilengkapi dengan file simulasi jaringan Cisco Packet Tracer, *source code* modul kriptografi, serta rekaman proses pengujian. Dokumentasi ini bertujuan untuk memastikan bahwa hasil penelitian dapat direproduksi dan dipahami dengan baik oleh pihak lain

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, dapat disimpulkan bahwa penelitian ini berhasil merancang sebuah infrastruktur jaringan yang aman dan tersegmentasi untuk mendukung layanan *FinTech*. Desain jaringan yang diusulkan mampu memisahkan zona publik, zona layanan, dan jaringan internal pengguna melalui penerapan konsep DMZ, VLAN, dan *server farm*. Penerapan mekanisme keamanan jaringan berupa *firewall* berbasis ACL dan NAT terbukti mampu membatasi lalu lintas jaringan sesuai dengan kebijakan keamanan yang dirancang. Segmentasi jaringan yang diterapkan juga mendukung prinsip *least privilege* dan *defense in depth*, sehingga potensi dampak serangan dapat diminimalkan.

Pada tingkat aplikasi, penerapan kriptografi menggunakan algoritma AES memberikan perlindungan terhadap data sensitif, khususnya data yang tersimpan dan diproses oleh sistem. Implementasi modul kriptografi ini menunjukkan bahwa keamanan jaringan dan keamanan aplikasi dapat saling melengkapi dalam membangun sistem yang lebih aman secara menyeluruh. Validasi desain melalui simulasi menggunakan Cisco Packet Tracer menunjukkan bahwa rancangan jaringan dapat berfungsi secara operasional dan memenuhi kebutuhan fungsional serta keamanan yang telah ditetapkan. Dengan demikian, tujuan penelitian untuk merancang infrastruktur jaringan dan strategi keamanan TIK yang baik telah tercapai.

5.2 Saran

Berdasarkan hasil penelitian dan keterbatasan yang ada, beberapa saran pengembangan dapat diberikan untuk penelitian atau implementasi selanjutnya, antara lain:

1. Implementasi sistem pada lingkungan nyata dengan menggunakan perangkat jaringan dan sistem keamanan yang lebih lengkap, seperti *firewall* generasi terbaru serta IDS/IPS.

2. Pengembangan mekanisme manajemen kunci kriptografi yang lebih aman dan terintegrasi, misalnya dengan menggunakan *Public Key Infrastructure* (PKI) atau Key yang disimpan pada Security Hardware terpisah.
3. Penerapan standar dan regulasi keamanan informasi yang relevan dengan sektor keuangan untuk meningkatkan tingkat kepatuhan dan keandalan sistem.
4. Pengujian keamanan yang lebih mendalam, seperti *penetration testing* dan *vulnerability assessment*, untuk mengevaluasi ketahanan sistem terhadap serangan siber yang kompleks.

Dengan pengembangan tersebut, sistem yang dirancang diharapkan dapat memberikan tingkat keamanan yang lebih tinggi dan siap diimplementasikan pada skala operasional yang lebih luas.

DAFTAR PUSTAKA

Cisco Systems. (2024). *Network Security Baseline*. Cisco Design Guide.

Cloudflare. (n.d.). *What is SSL/TLS?*. Cloudflare Learning Center. Retrieved June 13, 2025.

NIST. (2001). *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication 197.

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Prentice Hall.

LAMPIRAN

File Simulasi Packet Tracer	: Simulasi Cisco Packet Tracer
File Simulasi DataProtector (Encrypt & Decrypt)	: aol-net-sec
Video Simulasi Cisco Packet Tracer	: Video Simulasi CPT
Video Simulasi DataProtector (Encrypt & Decrypt)	: Video Simulasi DataProtector