YAYASAN MEMAJUKAN ILMU DAN KEBUDAYAAN
UNIVERSITAS SIBER ASIA
Kampus Menara, Jl. RM. Harsono, Ragunan - Jakarta Selatan.Daerah Khusus Ibukota Jakarta 12550. Telp. (+6221) 27806189. asiacyberuni@acu.ac.id. www.unsia.ac.id

**LEMBAR JAWABAN**
**UJIAN AKHIR SEMESTER**
**SEMESTER GANJIL TAHUN AJARAN 2024/2025**

| | |
|---|---|
| Mata Kuliah | : Analisa Berorientasi Objek |
| Kelas | : IF404 |
| Prodi | : PJJ Informatika |
| Nama Mahasiswa | : Muhammad Farhan |
| NIM | : 230401020086 |
| Dosen | : Abdul Azzam Ajhari, S.Kom., M.Kom |

---

**Jawaban Ujian**

**1. Jelaskan bagaimana prinsip Enkapsulasi dan Abstraksi dalam OOP dapat mencegah insiden seperti hardcoded credentials pada studi kasus!**

Pada studi kasus serangan ransomware terhadap Pusat Data Nasional Indonesia, diketahui bahwa salah satu penyebab utama kebocoran adalah penggunaan *hardcoded credentials* di dalam sistem backend. Hal ini dikonfirmasi dalam laporan *Reuters* bahwa:

“The breach exploited hardcoded credentials in the Data Management Portal, which allowed attackers to bypass authentication.”
https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24

Dalam prinsip **Object-Oriented Programming (OOP)**, konsep **enkapsulasi** melindungi data dari akses langsung dengan menyimpannya dalam atribut privat dan hanya mengizinkan akses melalui method yang telah divalidasi. Ini akan mencegah pengembang menyimpan kredensial langsung di dalam kode.

Sedangkan prinsip **abstraksi** menyederhanakan akses ke sistem kompleks seperti autentikasi, dengan mengandalkan interface atau class CredentialManager, yang mengambil kredensial melalui API atau secrets vault, bukan kode keras.

**2. Identifikasi 2 fase kritis SSDLC yang gagal dalam studi kasus! Berikan rekomendasi aktivitas keamanan untuk masing-masing fase.**

Berdasarkan laporan *The Record* dan *Paubox*, diketahui bahwa:

“The attack succeeded due to poor implementation practices, including hardcoded passwords and lack of system review.”
https://therecord.media/indonesia-national-data-centre-hacked

Dua fase **Secure Software Development Life Cycle (SSDLC)** yang gagal dalam kasus ini adalah:

- **Fase Design**
  *Kegagalan:* Tidak dilakukan threat modeling.

*Rekomendasi:* Lakukan *security design review* dan *threat modeling* secara rutin untuk mengidentifikasi celah sejak tahap perancangan.

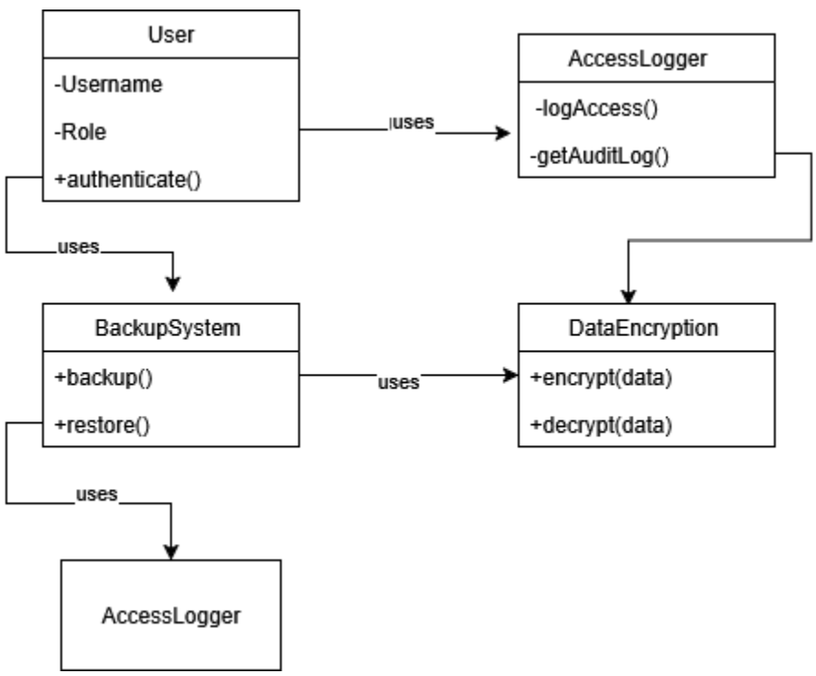
- **Fase Implementation**
  *Kegagalan:* Kredensial ditulis langsung ke dalam kode program (hardcoded).
  *Rekomendasi:* Terapkan praktik *secure coding* dan *automated static code analysis* untuk mendeteksi potensi kesalahan sebelum masuk ke deployment.

**3. Dalam konteks OOP, apa perbedaan antara Use Case dan Misuse Case? Berikan contoh misuse case untuk skenario "Akses Ilegal ke Database PDN".**

**Use Case** adalah skenario penggunaan sistem oleh pengguna sah, sedangkan **Misuse Case** adalah skenario yang menggambarkan penyalahgunaan sistem oleh aktor jahat untuk tujuan yang tidak diinginkan.

“The attacker used Brain Cipher ransomware to illegally access and encrypt Indonesia’s National Data Center systems.”
https://www.paubox.com/news/cyberattack-paralyzes-indonesias-national-data-center

**BAGIAN B: PEMODELAN OBJEK & KEAMANAN**




**1. User**

User merupakan entitas yang akan mengakses sistem. Sebelum dapat menggunakan fitur seperti backup atau restore, user harus terlebih dahulu melalui proses autentikasi melalui method authenticate(). Setiap user memiliki atribut username dan role yang menentukan hak aksesnya.

**2. AccessLogger**

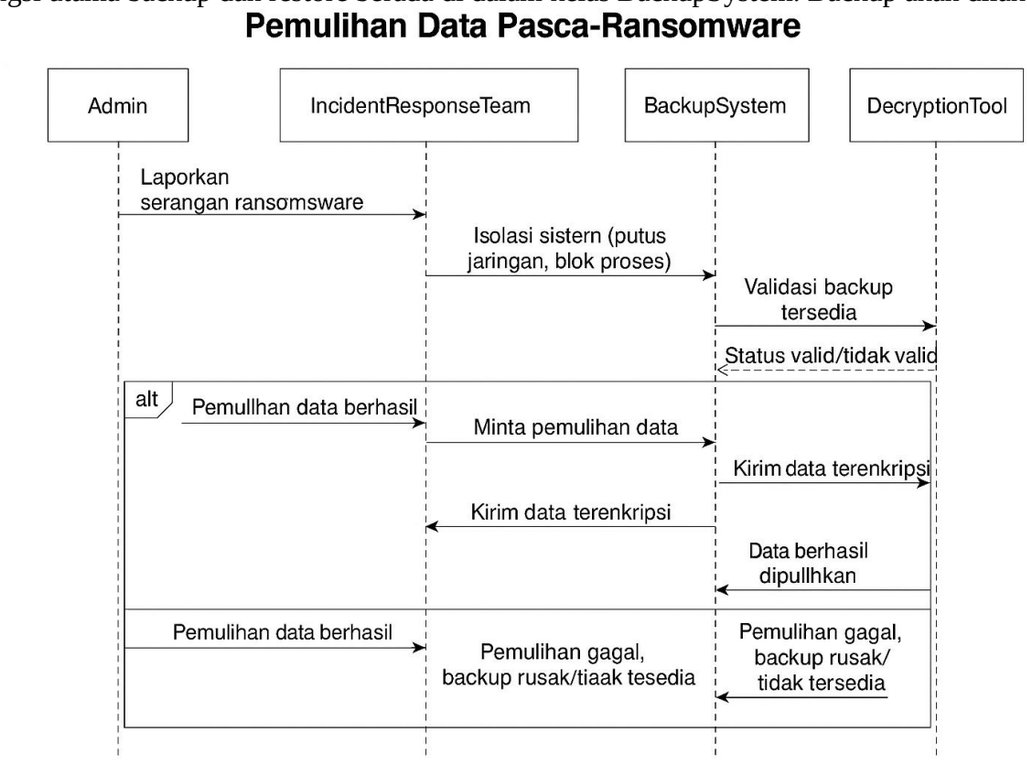
Setiap kali user berhasil mengakses sistem, maka aktivitas tersebut dicatat oleh AccessLogger melalui method logAccess(user, time). Logger ini juga menyediakan method getAuditLog() untuk melihat catatan aktivitas, penting dalam sistem yang menerapkan prinsip Zero Trust untuk menjaga jejak audit dari semua akses.

**3. DataEncryption**

Jika user melakukan tindakan backup atau restore data, maka sistem akan memanggil kelas DataEncryption. Data akan dienkripsi terlebih dahulu melalui method encrypt(data) agar tidak dapat dibaca pihak tidak berwenang. Saat data perlu dikembalikan, method decrypt(data) akan digunakan untuk mengembalikan ke bentuk aslinya.

**4. BackupSystem**

Fungsi utama backup dan restore berada di dalam kelas BackupSystem. Backup akan dilakukan




mengambil data berdasarkan dataId, kemudian mendekripsi dan mengembalikannya kepada user. Semua proses ini juga dicatat melalui AccessLogger.

**Alur Interaksi Antar Objek (Zero Trust Flow)**

1. **User melakukan login** menggunakan authenticate() → diverifikasi terlebih dahulu (tidak ada kepercayaan bawaan).
2. Jika autentikasi berhasil, sistem mencatat aktivitas ke AccessLogger.
3. Jika user melakukan backup:
    - Data dikirim ke BackupSystem.
    - Data terlebih dahulu dienkripsi melalui DataEncryption.
    - Aktivitas dicatat oleh AccessLogger.
4. Jika user melakukan restore:
    - BackupSystem mengambil data berdasarkan dataId.
    - Data didekripsi melalui DataEncryption.
    - Proses restore juga dicatat oleh AccessLogger.

YAYASAN MEMAJUKAN ILMU DAN KEBUDAYAAN
UNIVERSITAS SIBER ASIA
Kampus Menara, Jl. RM. Harsono, Ragunan - Jakarta Selatan.Daerah Khusus Ibukota Jakarta 12550. Telp. (+6221) 27806189. asiacyberuni@acu.ac.id. www.unsia.ac.id

**Alur Pemulihan Data Pasca-Ransomware**

1. **Isolasi Sistem**
   Setelah terdeteksi adanya serangan ransomware, Admin segera mengambil langkah isolasi sistem untuk menghentikan penyebaran malware. Sistem yang terdampak diputus dari jaringan utama dan aksesnya dibatasi hingga dilakukan investigasi lebih lanjut.

2. **Investigasi dan Koordinasi**
   Incident Response Team (IRT) melakukan analisis untuk mengetahui skala serangan, titik awal infeksi, dan perangkat yang terpengaruh. Mereka juga menyusun strategi pemulihan dan menentukan sistem mana yang aman untuk dioperasikan kembali.

3. **Validasi Backup**
   Setelah sistem berhasil diamankan, tim melakukan validasi terhadap data cadangan yang tersimpan di Backup System. Validasi ini mencakup pengecekan integritas data dan memastikan bahwa file backup tidak terinfeksi ransomware.

4. **Dekripsi (Jika Diperlukan)**
   Bila backup tidak tersedia atau tidak mencakup seluruh data penting, tim menggunakan Decryption Tool untuk mencoba memulihkan file yang telah dienkripsi oleh ransomware. Langkah ini dilakukan dengan hati-hati dan sesuai prosedur hukum serta keamanan siber.

5. **Restorasi Data**
   Setelah backup tervalidasi atau file berhasil didekripsi, data kemudian dikembalikan ke sistem bersih yang telah direkonstruksi oleh IRT. Proses restorasi dilakukan secara bertahap untuk memastikan sistem pulih dengan benar tanpa membawa sisa malware.

6. **Monitoring dan Audit**
   Pasca pemulihan, tim melakukan monitoring aktif terhadap sistem untuk memastikan stabilitas dan mendeteksi aktivitas mencurigakan. Laporan audit insiden juga disusun sebagai dokumentasi dan dasar peningkatan keamanan di masa depan.

**Referensi**


- https://www.cisa.gov/news-events/news/isolate-prevent-ransomware
- https://www.ncsc.gov.uk/collection/ransomware-response
- https://www.nist.gov/news-events/news/2020/10/prepare-defend-recover-ransomware-attack
- https://www.nomoreransom.org/
- https://www.acronis.com/en-us/blog/posts/how-restore-backup-after-ransomware-attack
- https://www.cyber.gov.au/acsc/view-all-content/guidance/recovering-ransomware-attack

YAYASAN MEMAJUKAN ILMU DAN KEBUDAYAAN

# UNIVERSITAS SIBER ASIA

Kampus Menara, Jl. RM. Harsono, Ragunan - Jakarta Selatan.Daerah Khusus Ibukota Jakarta 12550. Telp. (+6221) 27806189. asiacyberuni@acu.ac.id. www.unsia.ac.id

| **Nilai** | **Tanda Tangan Dosen Pengampu / Tutor** | **Tanda Tangan Mahasiswa** |
|---|---|---|
| | **(……..)** | **(……..)** |
| Diserahkan pada Tanggal: | | Tanggal Mengumpulkan: |
| | | |