

Cloud Computing dan Keamanan Informasi.

Kelompok G:

Edgrant H. S. (2206025016)

Andikha Wisanggeni (2106731503)

Fayza Nirwasita (2106635700)

Fairuz Muhammad (2206814324)

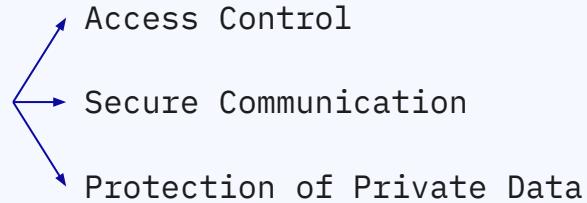
Table of contents

01	Information Security	07	The Security Players	13	Some Suggested Security for Cloud Computing
02	Evolution of Security Considerations	08	Traditional vs. Internet Security Issues	14	Side Channel Security Attacks in the Cloud
03	Security Concerns in Cloud Operating Models	09	Keamanan Menggunakan Kunci Enkripsi	15	An Introduction to Block Chain for Security
04	Identity Authentication	10	Tantangan dalam Menggunakan Algoritma Keamanan Standar	16	Summary
05	Secure Transmissions	11	Variasi dan Kasus Khusus dalam Keamanan Cloud Computing		
06	Secure Storage and Computation	12	Tantangan Utama dalam Cloud Computing dan Virtualisasi		

01

Information Security

Information Security



Access Control

- Memastikan akses yang sah ke sistem atau data.
- Diimplementasikan pada perangkat keras (misalnya, dongle USB) atau perangkat lunak (misalnya, sistem login, cookie).

Secure Communication

- Melindungi transfer informasi di antara para peserta.
- Sangat bergantung pada enkripsi (manajemen kunci sangat penting).

Protection of Private Data

- Melibatkan pengamanan perangkat penyimpanan, unit pemrosesan, dan memori.

Aspek umum: Kerahasiaan, Integritas, Ketersediaan (*CIA* keamanan).

Security Challenges

Weak Points

Ditentukan oleh faktor teknis (panjang kata sandi) dan penerimaan pengguna (autentikasi yang rumit).

Private Data Protection

- Menyeimbangkan ketersediaan dan integritas: Data harus dapat diakses oleh pengguna yang berwenang dengan tetap menjaga keakuratannya.
- Tingkat keamanan bervariasi berdasarkan sensitivitas data (misalnya, membaca iklan vs. aplikasi nuklir).

Cloud Security

Membutuhkan keamanan multi-level karena sumber daya yang digunakan bersama dan beragam aplikasi dengan kebutuhan yang berbeda.

Security Challenges

Environmental Factors Affecting Security

- **Daya komputasi:**

Peningkatan kapasitas mempercepat kemampuan defensif dan ofensif.

- **Kebutuhan yang terus meningkat:**

Semakin banyak industri yang membutuhkan data yang aman, termasuk keuangan dan perawatan kesehatan.

- **Berbagi informasi:**

Penggunaan komputasi awan yang meluas meningkatkan kepentingan keamanan.

02

EVOLUTION OF SECURITY CONSIDERATIONS



Timeline Evolusi

Early Computer Security

- Transisi dari terminal ke PC individual; muncul sistem berbasis ID pengguna dan kata sandi.
- Pengenalan komunikasi melalui saluran telepon dan kontrol akses jarak jauh.

Move to Cloud Computing

- Keamanan fisik adalah metode utama (akses yang besar dan terbatas ke perangkat).
- Perangkat terhubung langsung ke mainframe; kontrol akses masih bersifat dasar (berbasis fisik dan terminal).

Access Control Evolution

- Enkripsi informasi menjadi lebih standar.
- Batas-batas fisik memudar karena pengguna dapat mengakses sumber daya cloud dari mana saja.
- Komputasi awan bertujuan untuk memisahkan penyampaian layanan dari implementasi yang mendasarinya.

Security Challenges

in Cloud Computing

Denial-of-Services (DoS)

Pengguna yang tidak sah dapat membebani layanan secara berlebihan, sehingga menyebabkan kerusakan (misalnya, permintaan web yang berlebihan)

Privacy Concerns

Informasi akses harus dilindungi dari pengungkapan atau penyalahgunaan yang tidak sah.

Security Trade-offs

- Biaya kinerja tinggi untuk enkripsi data penuh, penting untuk data sensitif di Awan Publik.
- Kontrol akses dan kata sandi mungkin cukup untuk perangkat pengguna tunggal.
- Teknik seperti VPN dan pengecekan hash dapat mengamankan koneksi perangkat pribadi ke awan.

Balancing Act

Mempartisi data dan kode sensitif agar dapat berjalan di lingkungan yang aman di dalam Public Cloud untuk menyeimbangkan keamanan dan kinerja.

03

Security Concerns in Cloud Operating Models

Security Concerns in Cloud Operating Models

Varied Security Levels:

Langkah-langkah keamanan bergantung pada tingkat sumber daya pengguna di tingkat Cloud.

Data Security Requirement:

Persyaratan baru memastikan pengguna tidak mengetahui alokasi sumber daya mereka.

Cloud Service Models

Software as a Service (SaaS) :

- Tingkat abstraksi tertinggi, berfokus pada replikasi data di beberapa pengguna.
- Memastikan informasi yang dibagikan terlindungi dengan akses layanan tak terbatas.
- Mengelola kapasitas instance aplikasi melalui sumber daya server host.

Platform as a Service (PaaS) :

- Menargetkan pengembang aplikasi, menyediakan akses layanan yang ditingkatkan.
- Memanfaatkan inti CPU yang dialokasikan ke server host.
- Mendukung akses utilitas dan komponen, memastikan operasi inti yang aman.
- Memungkinkan desain hosting dan tautan untuk penyedia Public Cloud, memfasilitasi analitik skala besar dan kepuasan sistem berbiaya rendah.

04

Identity Authentication



Identity Authentication in Information Security

Traditional Authentication Elements:

What You Know: Passwords, PINs, personal information (e.g., birthday).

What You Have: Item fisik seperti smart card atau token.

What You Are: Biometric data (e.g., fingerprints, facial recognition).

Password Challenges

- Rentan terhadap serangan brute force.
- Meningkatnya kompleksitas menyebabkan praktik pengguna seperti menuliskan kata sandi, sehingga mempertaruhkan keamanan.

Identity Authentication in Information Security

Information Security Functions:

Access Control: User IDs, encryption, secure communication.

Data Protection: Encryption data pada saat diam dan transit, secure logging.

Metadata Management: Menjamin secure access dan handling metadata.

		Access control	Secure communications	Data protection	Monitoring
Software	User application	Some login, usually relies on lower levels [1]	Usually relies on lower levels of implementation	Encrypt or disguise data [5]	Access logs
	Operating system (OS)	Login [1]	In-memory transactions	[1, 5]	Special processes as watchdogs
	Virtual machine layer (VM)	[1, 5]		[1, 5]	[1]
	Hypervisor layer	[1]		[1]	[1]
	Software drivers	From OS	Encryption, security handshake	Encrypt data	
	BIOS/FW-based system management layer	Privileged execution		Privileged access to certain memory locations	Log files

Hardware	CPU	From OS	Port and bus encryption, secure caches	Separate secure registers and memory	
	Memory cache/main RAM	Encrypted busses, hash checking tables	Data encryption	Partitioning and encryption	Interrupt logs
	Memory disk	Hash, checking tables [5–8]	USB data encryption	Encrypt disk storage, removable devices	Error logs [9, 10]
	I/O	Verify access ID, such as Internet IP address	Encrypt transmissions; trust keyboard, mouse, and audio	Security handshake, coding, encryption	Watchdog processes in hardware and software

Pertimbangan keamanan bagi para profesional IoT di lingkungan cloud

Keamanan Konten:

Memastikan perlindungan data dan konten di dalam perangkat IoT dan platform cloud.

Keahlian Profesional:

Pentingnya pengetahuan khusus dalam keamanan IoT dan cloud untuk mengatasi tantangan yang unik.

05

Keamanan Transmisi

Enkripsi Data dan Trade-off Keamanan dan Efisiensi

Pentingnya Keamanan Transmisi

- Seberapa aman pun data di dalam sistem, jika data tersebut harus **dipindahkan** ke sistem lain, data tersebut dapat **terancam keamanannya**.
- Saat data dipindahkan, data berada pada lingkungan publik yang **diluar kontrol sistem; keamanan tidak lagi terjamin**.
- Solusinya adalah dengan **mengenkripsi data**



Trade-off Keamanan dan Efisiensi



Keamanan

Keamanan data tergantung pada enkripsinya. Namun, **bukan berarti kita harus menggunakan enkripsi yang paling kuat**. Enkripsi yang kuat membutuhkan waktu dan **sumber daya yang besar untuk dipecahkan**.



Efisiensi

Keputusan **trade-off** antara keamanan dan efisiensi harus dilakukan dengan mempertimbangkan nilai dan "umur" data.

Contoh Trade-off



Contoh 1

- Pengumuman diplomatik yang akan diumumkan pada **hari berikutnya**.
- Data tersebut memiliki "**umur yang terbatas**", hanya perlu diamankan selama 2 hari.
- Sehingga, enkripsi yang digunakan **tidak perlu terlalu kuat**.



Contoh 2

- Deskripsi investasi jangka panjang yang memiliki nilai **jangka panjang**.
- Data tersebut memiliki "**umur yang panjang**", sehingga **enkripsi** yang digunakan harus sangat **kuat**.

06

Penyimpanan dan Komputasi Aman

Trade-off Keamanan dan Efisiensi



Trade-off Keamanan dan Efisiensi

- Konsep trade-off antara keamanan dan efisiensi juga berlaku untuk penyimpanan dan komputasi.
- Sistem dapat memiliki **enkripsi ringan** dan **cepat** untuk data atau enkripsi yang kuat.
- Jenis enkripsi **tergantung dengan keperluan data**.
- Data harus dienkripsi, terutama jika disimpan di **3rd party storage provider**.



Trade-off Keamanan dan Efisiensi



Keamanan

Data yang memiliki "umur" yang **panjang**, seperti film copyright, memerlukan enkripsi yang **kuat**.



Efisiensi

Data yang memiliki "umur" yang **pendek**, seperti data yang disimpan di memori, dapat menggunakan enkripsi yang ringan, memprioritaskan read-write **speed**.

Trade-off Keamanan dan Efisiensi



- HSMs adalah **perangkat fisik** yang berfungsi sebagai "brankas" untuk menyimpan dan **mengelola kunci digital** untuk dekripsi data.
- HSMs dapat berupa kartu **plug-in** atau **perangkat eksternal** yang terhubung ke server jaringan.
- Data yang paling sensitif dapat disimpan dengan metode **dekripsi yang hanya ada pada HSM**.

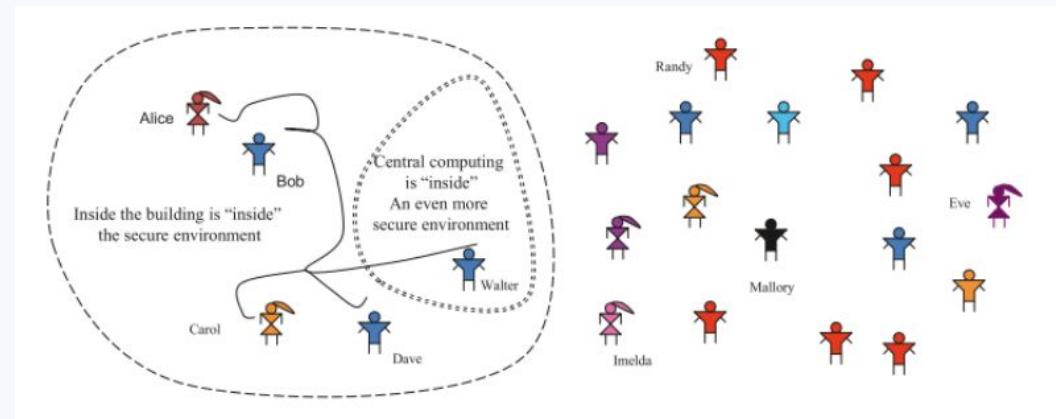
07

Pemain Keamanan

Peran dan Nickname dalam Sistem Keamanan



Pemain Keamanan



- Deskripsi sistem keamanan dan partisipannya dapat membingungkan. Untuk memudahkan, pemain dalam sistem keamanan diberi nickname.
- Nickname adalah sebagai berikut
 - **Alice, Bob, Carol, Dave:** Pengguna dalam sistem (Legitimate Users)
 - **Walter:** Administrator sistem
 - **Eve:** Penyerang eavesdropping (menguping komunikasi)
 - **Mallory:** Penyerang yang mencoba mengubah data (Malicious Attacker)
 - **Randy:** Pengguna atau entitas yang secara tidak sengaja menyebabkan masalah keamanan (Accidental Attacker).
 - **Imelda:** Penyerang yang melakukan serangan Denial-of-Service (DoS) untuk mengganggu layanan sistem.

Tipe Serangan

Lapisan	Jenis Serangan	Perubahan Data atau Program Tidak Sah (Mallory dan Randy [Accidental])	Pengamatan dan Penyalinan Tidak Sah (Eve dan Randy [Accidental])	Serangan Denial-of-Service (DoS) (Imelda dan Randy [Accidental])
Perangkat Lunak	Aplikasi Pengguna	Login palsu, atau akses tidak langsung	Biasanya bergantung pada lapisan implementasi yang lebih rendah	Enkripsi atau penyamaran data
	Sistem Operasi (OS)	Login palsu, instruksi tingkat rendah	Transaksi dalam memori	
	Lapisan Mesin Virtual (VM)	Komunikasi antar-VM	Kebocoran informasi	
	Lapisan Hypervisor			
	Driver Perangkat Lunak	Dari sistem operasi (OS)	Enkripsi, keamanan handshake	Enkripsi data
Perangkat Keras	BIOS/Lapisan manajemen sistem berbasis firmware	Manipulasi stempel waktu dan tanggal	Lokasi memori yang aman	Autentikasi untuk eksekusi
	CPU	Kebocoran informasi	Kebocoran informasi	
	Memori cache/RAM utama	Kebocoran informasi		
	Disk Memori	Hak akses	Hak akses	

08

Pemain Keamanan

Peran dan Nickname dalam Sistem Keamanan



Keamanan Tradisional

- Pendekatan keamanan tradisional bergantung pada **penghalang fisik**.
- **Akses** ke pusat komputasi hanya tersedia untuk **personil terperaya**.
- Aktivitas dan **akses** hardware dan jaringan **terkontrol** dan dipantau.



Keamanan Internet



- Dengan internet, admin sistem memiliki **akses** melalui **channel transmisi yang tidak terkontrol**.
- **Identitas** asli pengguna **tidak diketahui**.
- **Intruder** memiliki **kesempatan tak terbatas** untuk mencoba **akses**.
- Kebijakan **keamanan** yang **ketat** dapat **mengganggu pengguna** yang sah seperti menyebabkan serangan Denial-of-Service (DoS).

09

Keamanan Menggunakan Kunci Enkripsi

Keamanan dalam Cloud



Enkripsi

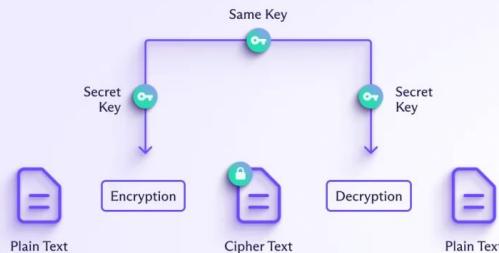
Enkripsi digunakan untuk melindungi data dari akses tidak sah dengan mengonversi informasi menjadi bentuk yang hanya dapat dibaca oleh pihak yang berwenang.



Jenis Enkripsi

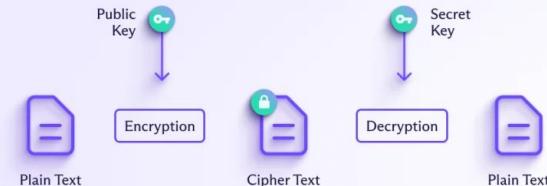
Enkripsi Simetris: Menggunakan satu kunci yang sama untuk enkripsi dan dekripsi (contoh: AES, DES).

Symmetric Encryption



Enkripsi Asimetris: Menggunakan pasangan kunci publik dan privat (contoh: RSA, ECC).

Asymmetric Encryption

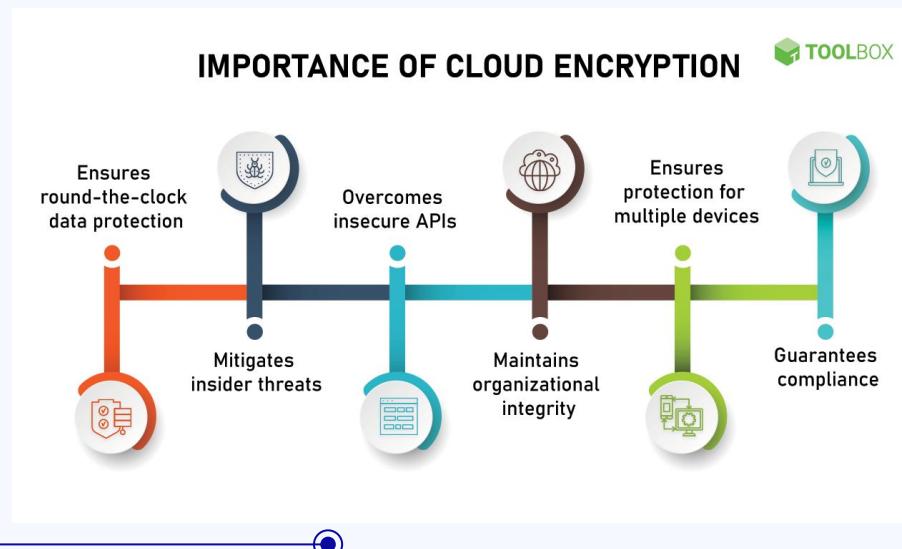


Perbandingan Enkripsi Simetris dan Asimetris

Aspek	Enkripsi Simetris	Enkripsi Asimetris
Kunci yang Digunakan	Satu kunci yang sama untuk enkripsi dan dekripsi	Pasangan kunci publik dan privat
Keamanan	Kurang aman jika kunci bocor	Lebih aman karena kunci privat tidak dibagikan
Kecepatan	Lebih cepat	Lebih lambat karena kompleksitas kriptografi

Penerapan dalam Cloud

- Melindungi data saat transit dan saat disimpan.
- Digunakan dalam layanan seperti TLS/SSL, VPN, dan penyimpanan terenkripsi.



10 Tantangan dalam Menggunakan Algoritma Keamanan Standar

Tantangan yang dihadapi dalam Cloud



Efisiensi, Performa, Tantangan

- Algoritma keamanan yang lebih kuat seringkali membutuhkan sumber daya komputasi yang lebih besar.
- Tantangan utama dalam penyimpanan dan distribusi kunci yang aman.
- Algoritma konvensional seperti RSA dan ECC bisa menjadi rentan jika komputer kuantum berkembang.



11

Variasi dan Kasus Khusus dalam Keamanan Cloud Computing



Kasus Khusus dalam Keamanan Cloud

- **Keamanan Multi-Tenant:** Pengguna berbagi infrastruktur yang sama.
- **Proteksi DDoS:** Serangan dapat mengganggu layanan berbasis cloud.
- **Keamanan API:** API yang lemah dapat membuka celah keamanan.
- **Isolasi Data:** Data harus dipisahkan dengan baik antara pengguna.

12

Tantangan Utama dalam Cloud Computing dan Virtualisasi



Tantangan Utama dalam Cloud Computing dan Virtualisasi

- **Manajemen Identitas:** Verifikasi pengguna dan kontrol akses.
- **Isolasi Sumber Daya:** Memastikan keamanan antar lingkungan virtual.
- **Privasi dan Kepatuhan:** Mematuhi regulasi seperti GDPR dan HIPAA.
- **Ancaman Insider:** Risiko dari pengguna internal yang memiliki akses ke sistem.

13

Some Suggested Security for Cloud Computing

You can enter a subtitle here if you need it

Best Practices

Continuous Monitoring

Pemantauan terus-menerus diperlukan untuk mendeteksi pola penggunaan yang tidak biasa atau perubahan dalam sumber daya cloud.

Attack Surface Management

Mengelola dan membatasi titik akses yang bisa dimanfaatkan oleh pihak tidak berwenang untuk mengakses data penting.

No Residual Footprints

Menghapus jejak digital dari memori atau disk setelah penggunaan cloud, sehingga data yang tersisa tidak dapat dieksplorasi oleh pihak lain.

Strong Access Control

Mengelola kontrol akses dengan baik untuk mencegah serangan melalui titik masuk yang tidak terduga, seperti sistem HVAC yang kurang aman.

Damage Control

Menyusun strategi mitigasi untuk mengurangi dampak jika terjadi serangan, misalnya dengan menonaktifkan akun yang terancam atau mematikan server yang terinfeksi.

Keamanan Cloud

Email	Application
<ul style="list-style-type: none">• Antivirus• Anti-spam• Information Leakage Control• Kemampuan membuat aturan untuk blokir konten• Email Traffic Monitoring	<ul style="list-style-type: none">• Intrusion Detection Tools• Application Firewall• Firewall generasi terbaru• Alat Mitigasi Serangan DDoS• Log Correlation• CDN (Content Delivery Network)

* Persyaratan keamanan ini dapat dimasukkan dalam SLA (Service-Level Agreement) antara penyedia cloud dan penggunanya untuk memastikan tanggung jawab dan alat keamanan yang tersedia.

14

Side Channel Security Attacks in the Cloud

You can enter a subtitle here if you need it



Kategori Side Channel Attack

Cache Side Channel Attack

- Serangan ini menargetkan cache memori yang digunakan oleh berbagai proses dalam sistem berbagi sumber daya.
- Jika dua proses menggunakan cache yang sama, penyerang bisa mengamati pola penggunaan cache untuk menebak informasi dari proses lain.

Timing Attacks

- Penyerang mengukur waktu eksekusi operasi tertentu untuk mendapatkan informasi terkait algoritma atau data yang digunakan.
- Contohnya adalah calculation timing attacks, di mana perbedaan kecepatan operasi tertentu membantu penyerang menebak bagian dari kunci enkripsi.

Power Analysis Attacks

- Serangan ini menggunakan pola konsumsi daya dari prosesor untuk menebak data yang sedang diproses.
- Contohnya, variasi konsumsi daya saat transistor berpindah antara 1 dan 0 bisa memberikan informasi tentang bit dalam sebuah kunci enkripsi.

Serangan Side Channel Lain

Electromagnetic Radiation	Photon Attack	Acoustic Attack
Menganalisis sinyal elektromagnetik yang dipancarkan oleh chip untuk mendapatkan informasi tentang data yang diproses.	Mengamati chip menggunakan teknik optik untuk memahami operasi internalnya.	Menggunakan pola suara yang dihasilkan oleh perangkat keras, seperti getaran dari keyboard atau disk drive.

15

An Introduction to Block Chain for Security

You can enter a subtitle here if you need it

Blockchain

Blockchain adalah basis data terdistribusi yang mencatat semua transaksi digital yang terjadi di dalam jaringan. Teknologi ini bersifat desentralisasi, artinya data tidak tersimpan di satu tempat tetapi didistribusikan ke semua peserta jaringan, sehingga sulit untuk diretas atau dimanipulasi.

Tiga komponen utama:

1. Block → berisi daftar transaksi yang terjadi dalam periode tertentu
2. Chain → blok-blok ini ditandai dengan timestamp dan dihubungkan secara kriptografis, sehingga membentuk rantai yang aman
3. Distributed Ledger → setiap peserta dalam jaringan memiliki salinan data transaksi yang selalu diperbarui

Keuntungan:

1. Menghilangkan perantara dalam transaksi, sehingga lebih cepat dan hemat biaya.
2. Meningkatkan keamanan, karena transaksi dienkripsi dan tidak bisa diubah.
3. Mengurangi risiko kejahatan siber dan penipuan.

Aplikasi Blockchain

Cryptocurrency	Smart Contracts	Trusted Computing
<ul style="list-style-type: none">• Digunakan untuk menyimpan dan mentransfer nilai tanpa otoritas pusat.• Menggunakan enkripsi kuat (misalnya SHA-256) untuk melindungi dari manipulasi data.• Setiap peserta jaringan memiliki salinan transaksi sehingga tidak bisa dipalsukan.	<ul style="list-style-type: none">• Kontrak yang dijalankan secara otomatis tanpa perantara.• Bisa melibatkan dua atau lebih pihak dengan aturan yang telah disepakati.• Memungkinkan pembayaran otomatis setelah syarat terpenuhi.• Menerapkan sanksi jika aturan tidak dipenuhi.	<ul style="list-style-type: none">• Meningkatkan keamanan dalam berbagi sumber daya dan transaksi.• Menggabungkan blockchain, desentralisasi, dan smart contracts untuk menciptakan sistem yang lebih aman.

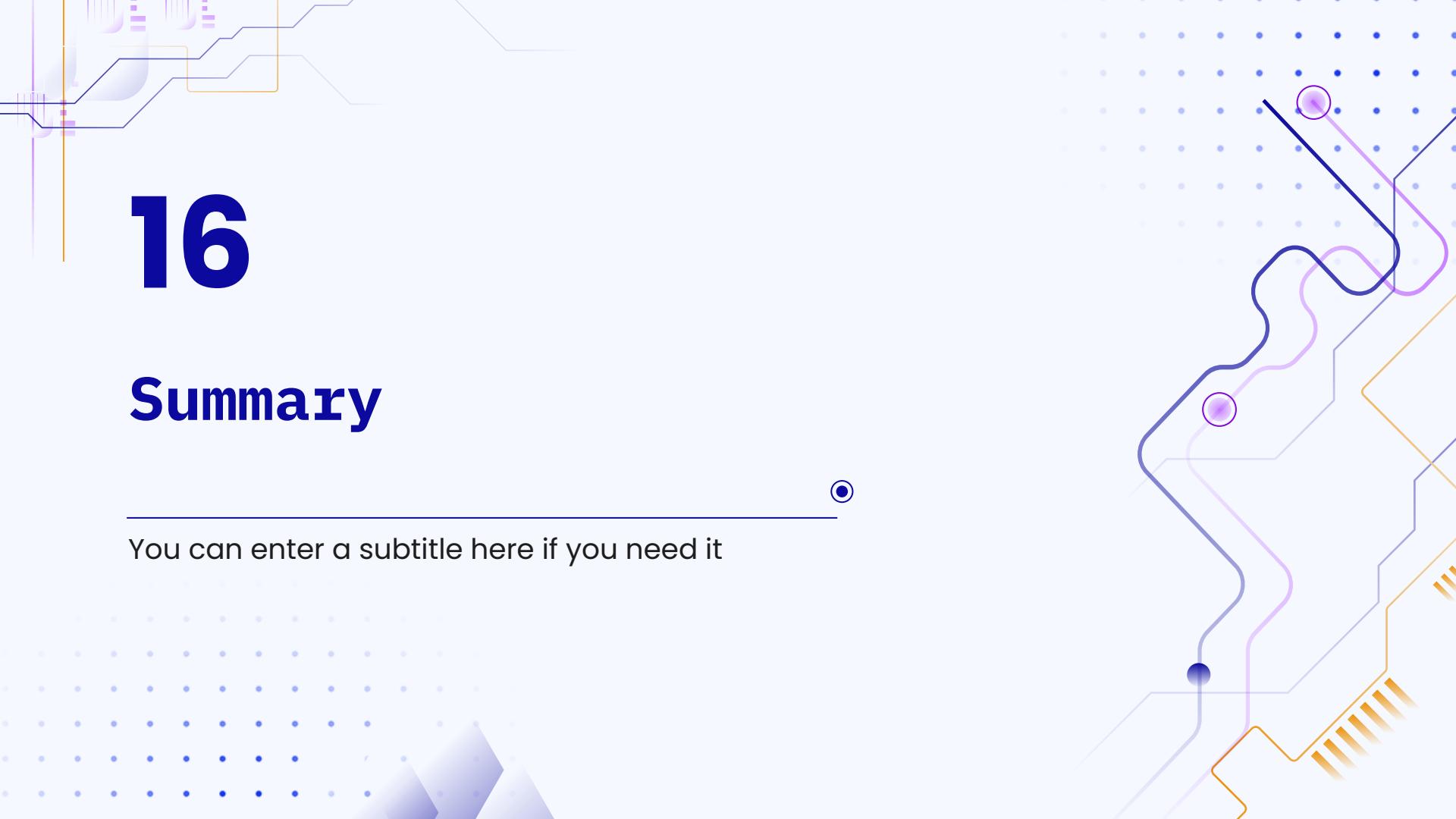
Cara Kerja Transaksi Keuangan

1. Setiap blok memiliki input, amount, dan output
 - Input → Sumber dana yang digunakan dalam transaksi
 - Amount → Jumlah yang ingin dikirimkan
 - Output → Alamat penerima transaksi
2. Transaksi baru dibuat dalam bentuk blok dan dikirim ke jaringan.
3. Setiap node dalam jaringan memperbarui ledger-nya.
4. Konsensus terjadi untuk memvalidasi transaksi baru.
5. Blok baru ditambahkan ke rantai blockchain.

16

Summary

You can enter a subtitle here if you need it





Pertumbuhan Internet meningkatkan risiko keamanan informasi, terutama dengan penerapan Cloud Computing. Bab ini membahas tantangan keamanan spesifik Cloud Computing dan perlunya keseimbangan antara keamanan dan kinerja sistem. Solusi keamanan harus mencakup berbagai lapisan dan fungsi. Pembahasan ini bertujuan mendorong diskusi lebih lanjut mengenai model keamanan Cloud Computing, mencakup ancaman nyata maupun persepsi risiko.

—Summary



Thanks !

Do you have any questions?