SKFNA TEKNOLOGI
JURNAL ILMIAH SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 1 Febuary 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

STRATEGI KEAMANAN DALAM CLOUD COMPUTING ANALISIS ANCAMAN DAN SOLUSI MITIGASI

[1] Awan
(afiliasi) [1]Universitas IBBI
[1]Email one.awan@gmail.com
*Penulis Korespondensi

Abstrak: Cloud computing telah menjadi salah satu teknologi utama yang digunakan oleh berbagai organisasi untuk meningkatkan efesiensi operasional dan skalabilitas. Adopsi cloud computing juga membawa tantangan signifikan dalam hal keamanan data dan infrastruktur. Penelitian ini bertujuan untuk menganalisis ancaman utama yang sering terjadi dalam lingkungan cloud computing seperti serangan siber, kehilangan data dan akses tidak sah. Metode penelitian mencakup kajian literatur yang mendalam dan analisi studi kasus terkait insiden keamanan pada penyedia layanan cloud, dengan metode mitigasi seperti enkripsi, sistem deteksi dan respon ancaman. Studi kasus dan simulasi keamanan menggunakan AWS.

Kata Kunci: Cloud Computing, serangan siber, keamanan data, akses tidak sah, Amazon Web Services (AWS).

Abstrak: Cloud computing has become one of the main technologies used by various organizations to improve operational efficiency and scalability. The adoption of cloud computing also brings significant challenges in terms of data and infrastructure security. This study aims to analyze the main threats that often occur in cloud computing environments such as cyber attacks, data loss and unauthorized access. The research method includes an in-depth literature review and case study analysis related to security incidents at cloud service providers, with mitigation methods such as encryption, threat detection and response systems. Case studies and security simulations use Amazon Web Services (AWS).

Keyword: Cloud Computing, cyber attacks, data security, unauthorized access, Amazon Web Services (AWS).

1. PENDAHULUAN

Cloud computing telah menjadi salah satu teknologi utama yang digunakan oleh berbagai organisasi untuk meningkatkan efisiensi operasional dan skalabilitas. Namun, adopsi cloud computing juga membawa tantangan signifikan dalam hal keamanan data dan infrastruktur. Penelitian ini bertujuan untuk menganalisis ancaman utama yang sering terjadi dalam lingkungan cloud computing, termasuk serangan siber, kehilangan data, dan akses tidak sah. Metodologi penelitian mencakup kajian literatur yang mendalam dan analisis studi kasus terkait insiden keamanan pada penyedia layanan cloud.

Hasil penelitian ini mengidentifikasi beberapa ancaman utama, seperti serangan Distributed Denial of Service (DDoS), eksploitasi kerentanan aplikasi, dan risiko insider threat. Selain itu, solusi mitigasi yang efektif, termasuk penerapan model Zero Trust Architecture (ZTA), enkripsi data end-to-end, manajemen identitas dan akses (IAM), serta audit keamanan secara berkala.

SKFNA TEKNOLOGI
JURNAL ILMIAH SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 1 Febuary 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

Dengan penelitian ini dapat disimpulkan bahwa kombinasi strategi teknis, kebijakan organisasi, dan edukasi pengguna merupakan pendekatan optimal untuk mengurangi risiko keamanan di lingkungan cloud.

2. METODE PENELITIAN

Metode penelitian yang dilakukan adalah dengan menganalisa studi kasus keamanan cloud computing yang telah terjadi dengan pendekatan simulasi. Adapun data yang diperoleh dari laporan insiden dan dokumen yang dapat diakses oleh publik. Eksperimen dilakukan dilingkungan cloud simulasi dirancang menggunakan produk dari Amazon Web Services (AWS) untuk menguji solusi mitigasi tertentu, seperti akses ilegal dan serangan Distributed Denial of Service (DDoS).

2.1. Cloud Computing

Konsep cloud computing berakar dari era mainframe computing pada 1960-an, di mana sumber daya komputasi dibagikan melalui jaringan terminal. Namun, implementasi modern cloud computing mulai berkembang pesat pada awal 2000-an dengan hadirnya layanan seperti Amazon Web Services (AWS) pada 2006, diikuti oleh Google Cloud Platform (GCP) dan Microsoft Azure.

Transformasi cloud computing juga dipengaruhi oleh tren teknologi seperti:

1. Virtualisasi, memungkinkan efisiensi penggunaan server dan alokasi sumber daya secara dinamis.
2. Edge Computing & IoT, meningkatkan kebutuhan akan integrasi cloud untuk pengolahan data dari perangkat pintar.
3. Artificial Intelligence & Big Data, Cloud menjadi platform utama untuk pemrosesan data dalam skala besar.
4. Hybrid & Multi-Cloud, Kombinasi antara cloud publik, privat, dan on-premise untuk fleksibilitas dan keamanan lebih baik.

Dengan meningkatnya ketergantungan pada cloud computing, tantangan keamanan pun semakin kompleks, mencakup data breaches, insider threats, dan serangan DDoS, yang menuntut strategi mitigasi efektif untuk melindungi infrastruktur cloud.

Model layanan cloud adalah kategori utama dalam cloud computing yang menawarkan layanan dengan skala berbeda kepada pengguna, baik individu maupun organisasi. Ada tiga model utama layanan cloud, yaitu IaaS, PaaS, dan SaaS, serta beberapa model tambahan seperti FaaS dan DaaS. Berikut adalah penjelasan detailnya:

- Infrastructure as a Service (IaaS)
  IaaS menyediakan infrastruktur komputasi dasar seperti server, jaringan, penyimpanan, dan virtualisasi. Pengguna memiliki kontrol penuh terhadap sistem operasi, aplikasi, dan data yang diinstal.
  Contoh: Amazon EC2, Google Compute Engine, Microsoft Azure.
- Platform as a Service (PaaS)
  PaaS menyediakan platform bagi developer untuk membangun, menguji, dan menyebarkan aplikasi tanpa perlu mengelola infrastruktur dasar.
  Contoh: Google App Engine, Heroku, Microsoft Azure App Services.
- Software as a Service (SaaS)

E- ISSN: 3058-1570
Volume 2 No 1 Febuary 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

SaaS menawarkan aplikasi lengkap yang berjalan di cloud dan dapat diakses melalui internet.
Contoh: Google Workspace, Microsoft 365, Dropbox, Salesforce.

- Function as a Service (FaaS)
  FaaS dikenal juga sebagai serverless computing. Pengguna dapat menjalankan kode tanpa harus mengelola server.
  Contoh: AWS Lambda, Google Cloud Functions, Microsoft Azure Functions.
- Desktop as a Service (DaaS)
  DaaS menyediakan desktop virtual yang di-host di cloud dan dapat diakses dari berbagai perangkat.
  Contoh: Citrix Virtual Apps and Desktops, Amazon WorkSpaces.

2.2. Ancaman Cloud Computing

Cloud computing memberikan berbagai keuntungan, namun juga menghadirkan ancaman keamanan yang perlu diantisipasi. Berikut adalah ancaman utama yang sering terjadi dalam cloud computing:

- Data Breach (Pelanggaran Data)
  Akses tidak sah ke data sensitif yang disimpan di cloud, seperti informasi pelanggan, data finansial, atau data perusahaan. Penyebab dapat ditimbulkan seperti konfigurasi keamanan yang salah, serangan phishing atau brute force yang dilakukan oleh hacker, kerentanan dalam aplikasi pihak ketiga. Sehingga dampak yang dapat ditimbulkan sangat besar seperti kehilangan reputasi maupun kerugian finansial.
- Loss of Data (Kehilangan Data)
  Kehilangan permanen data akibat penghapusan yang tidak disengaja, serangan malware, atau kegagalan sistem. Kenyataan ini timbul dapat disebabkan tidak ada backup yang memadai, kesalahan atau kelalaian pengguna dan serangan ransomware. Atas ketidakmampuan untuk memulihkan, maka mengakibatkan hilangnya informasi penting.
- Denial of Service (DoS) dan Distributed DoS (DDoS)
  Serangan yang bertujuan membuat layanan cloud tidak tersedia dengan membanjiri server dengan trafik palsu. Sehingga menimbulkan Botnet yang digunakan untuk menyerang server ataupun mengakibatkan kerentanan pada sistem jaringan dengan dampak downtime layanan sampai hilangnya kepercayaan pengguna.
- Application Programming Interface (API) yang Tidak Aman
  API yang digunakan untuk mengelola layanan cloud memiliki celah keamanan yang dapat dimanfaatkan oleh penyerang, disebabkan API tidak terenkripsi atau tidak menggunakan autentikasi yang kuat.
  Konfigurasi yang salah pada endpoint API dapat mengakibatkan akses tidak sah ke sistem cloud dan manipulasi data atau sistem.
- Pembajakan Akun
  Penyerang mengambil alih akun pengguna cloud untuk mendapatkan akses ke data atau layanan dengan cara Phishing atau rekayasa sosial. Ini dapat terjadi dikarenakan kata sandi yang lemah atau tidak terenkripsi.

E- ISSN: 3058-1570
Volume 2 No 1 Febuary 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

Dampak yang ditimbulkan adalah eksploitasi data sensitif, sampai kerugian operasional.

- Insider Threat (Ancaman Orang Dalam)
  Ancaman yang berasal dari karyawan, mitra, atau pihak internal lainnya yang memiliki akses ke cloud yang disebabkan kesalahan manusia, maupun motif balas dendam atau insentif finansial. Dampak yang ditimbulkan pelanggaran data maupun kehilangan kontrol terhadap infrastruktur cloud.
- Misconfigured Cloud Services (Konfigurasi yang Salah)
  Kesalahan dalam pengaturan keamanan, seperti penyimpanan data yang tidak dienkripsi atau bucket penyimpanan yang bersifat publik. Penyebab kurangnya pemahaman tentang pengaturan cloud, kesalahan manusia saat mengonfigurasi layanan. Sehingga berdampak pada data dapat diakses oleh pihak tidak berwenang dan risiko pelanggaran privasi.
- Malware Injection
  Penyerang menyisipkan malware ke dalam aplikasi cloud untuk mendapatkan akses atau mengendalikan layanan. File yang diunggah mengandung malware. Kerentanan pada sistem cloud. Kerusakan pada aplikasi atau data dan gangguan operasional.
- Compliance Violation (Pelanggaran Kepatuhan)
  Pengguna gagal mematuhi regulasi atau standar keamanan yang diwajibkan, sehingga berdampak pada kesalahan dalam pengelolaan data maupun tidak ada proses audit reguler. Sehingga menimbulkan denda besar termasuk kehilangan kepercayaan pelanggan.
- Vendor Lock-In
  Ketergantungan pada satu penyedia cloud yang membuat migrasi ke platform lain sulit dan mahal. Penyebab tidak adanya interoperabilitas antar platform, format data eksklusif. Akan berdampak keterbatasan inovasi, risiko jika vendor mengalami gangguan layanan.

2.3. Analisis Risiko

Analisis risiko pada cloud computing adalah proses sistematis untuk mengidentifikasi, mengevaluasi, dan memitigasi risiko yang dapat memengaruhi keamanan, ketersediaan, dan integritas sistem cloud. Proses ini sangat penting dalam memastikan layanan cloud tetap andal, aman, dan sesuai dengan kebutuhan bisnis.

Risiko seperti bencana alam, gangguan sistem, atau serangan siber dapat mengganggu operasi bisnis. Analisis risiko membantu organisasi seperti menyusun rencana pemulihan bencana (disaster recovery plan), memastikan bahwa waktu henti layanan (downtime) dapat diminimalkan dan menentukan prioritas sistem yang perlu dipulihkan terlebih dahulu.

Proses Analisis Risiko pada Cloud Computing dapat dilakukan dengan identifikasi Risiko dengan cara mengidentifikasi potensi ancaman terhadap sistem cloud. Evaluasi Risiko dengan menilai kemungkinan dan dampak dari

E- ISSN: 3058-1570
Volume 2 No 1 Febuary 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

risiko tersebut. Melakukan Mitigasi Risiko dapat mengembangkan langkah-langkah pencegahan, seperti kontrol akses, enkripsi, atau firewall. Pemantauan Risiko secara berkala dengan memantau efektivitas strategi yang diterapkan dan memperbaruinya sesuai dengan ancaman baru.

Analisis risiko pada cloud computing sangat penting karena membantu organisasi dalam melindungi data sensitif dan menjaga privasi, mematuhi regulasi dan standar industri, menghindari gangguan operasional dan kerugian finansial serta membangun kepercayaan dengan pelanggan dan mitra bisnis. Melakukan analisis risiko secara berkala adalah langkah proaktif untuk menjaga keamanan dan kelangsungan bisnis di era digital.

2.4. Strategi Mitigasi Terhadap Ancaman

Strategi mitigasi ini bertujuan melindungi data, memastikan layanan tetap berjalan, mematuhi regulasi, dan mengurangi dampak dari ancaman pada cloud computing. Implementasi langkah-langkah ini sangat penting untuk keamanan dan kelangsungan operasional.

Adapun strategi yang dapat diterapkan untuk menghindari ancaman dengan mitigasi dapat dilakukan dengan cara :

1. Enkripsi Data (Data Encryption)
2. Autentikasi Multi-Faktor (Multi-Factor Authentication, MFA)
3. Backup Data Secara Rutin
4. Audit Keamanan Berkala
5. Pelatihan Keamanan untuk Pengguna dan Karyawan
6. Menerapkan Keamanan API (API Security)
7. Pemantauan dan Logging (Monitoring and Logging)
8. Pengelolaan Akses (Access Management)
9. Penilaian Keamanan Vendor (Vendor Security Assessment)
10. Rencana Pemulihan Bencana (Disaster Recovery Plan)

3. HASIL DAN PEMBAHASAN

Pendekatan ini berfokus pada analisis mendalam terhadap kasus-kasus nyata yang melibatkan ancaman keamanan cloud computing, baik pada perusahaan global maupun lokal.

3.1.Perancangan dengan Eksperimen Cloud Computing

Berikut ini layanan yang diperlukan dalam pengujian yang dibutuhkan pada eksperimen cloud computing produk AWS :

1. Layanan Compute AWS EC2 untuk pengujian aplikasi, AWS Lambda untuk eksperimen serverless.
2. Storage: S3 untuk penyimpanan data uji, EBS untuk penyimpanan blok.
3. Database: Amazon RDS atau MySQL untuk pengelolaan data.
4. Networking: Amazon VPC untuk pengaturan jaringan virtual yang aman.
5. Monitoring: CloudWatch untuk pemantauan kinerja dan log.

SKENA TEKNOLOGI
JURNAL ILMIAH SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 1 Febuary 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

3.2. Simulasi Penyerangan Layanan AWS oleh DDoS

Berikut ini detail tentang bagaimana serangan DdoS yang terjadi pada layanan AWS disertai dengan skema alur serangan yang melibatkan pengiriman lalu lintas dalam jumlah besar secara bersamaan dari berbagai sumber ke target, seperti aplikasi atau server, untuk membanjiri sumber daya sehingga layanan menjadi tidak responsif. Pada AWS target serangan DdoS meliputi :

- Elastic Load Balancer (ELB): Mengelola distribusi lalu lintas.
- Amazon EC2 Instances: Server aplikasi atau basis data.
- API Gateway: Mengelola lalu lintas API untuk aplikasi serverless.

Scenario Serangan DDoS diarahkan ke aplikasi web yang dihosting di AWS. Penyerang memanfaatkan botnet untuk menghasilkan permintaan HTTP palsu secara masif. Lalu lintas diarahkan ke Elastic Load Balancer (ELB). ELB mencoba mendistribusikan lalu lintas ke beberapa EC2 instances. Namun, beban yang berlebihan menyebabkan aplikasi menjadi tidak responsif. Jika tidak ada perlindungan, pengguna sah tidak dapat mengakses layanan.

Berikut adalah skema visual:

Botnet --> Lalu Lintas Berlebih --> Elastic Load Balancer --> EC2 Instance --> Kegagalan Layanan

Botnet --> Permintaan API Palsu --> API Gateway --> Lambda/Database --> Konsumsi Sumber Daya

Gambar 3.1 Serangan DdoS pada layanan AWS

Dengan demikian gunakan AWS WAF (Web Aplication Firewall) untuk memblokir permintaan mencurigakan, dapat juga memperkuat dengan konfigurasi rate limitting pada layanan yang diberikan akses. Terapkan throtting untuk mengindari lonjakan trafik.

SKENA TEKNOLOGI
JURNAL ILMIAH SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 1 Febuary 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

3.3. Serangan Pada layanan API

Serangan terhadap API pada cloud computing, seperti yang ada pada AWS (Amazon Web Services), sering kali menargetkan celah keamanan dalam pengelolaan API untuk mencuri data, mengambil alih akun, atau melakukan sabotase. Berikut adalah penjelasan tentang beberapa jenis serangan ke API pada cloud computing dan contoh kasusnya.

Serangan Credential Stuffing adalah contoh lain dari serangan ini memanfaatkan kredensial pengguna yang bocor dari sumber lain. Penyerang mencoba menggunakan kredensial tersebut pada API cloud (AWS API Gateway, misalnya) untuk mendapatkan akses tidak sah.

Pada contoh kasus ini penyerang mendapatkan pasangan API key dan secret key pengguna AWS dari kebocoran data sebelumnya. Dengan kredensial tersebut, penyerang mengakses layanan AWS seperti S3 untuk membaca atau menghapus data. Jika tidak ada pembatasan atau rotasi kunci yang baik, serangan ini dapat menyebabkan kehilangan data yang signifikan.

Gambar 3.2. Serangan pada API AWS Credential Stuffing

Untuk melakukan mitigasi atas serangan ini dapat dilakukan dengan gunakan MFA (Multi-Factor Authentication) untuk menambahkan lapisan keamanan ekstra selain password. Implementasi Rate Limiting agar membatasi jumlah permintaan ke API dalam jangka waktu tertentu. Pemantauan Aktivitas API dengan menggunakan AWS CloudTrail atau AWS GuardDuty untuk mendeteksi aktivitas mencurigakan. Kebijakan Kata Sandi Kuat untuk mendorong pengguna untuk menggunakan kata sandi unik dan kuat. Menggunakan token berbasis OAuth2 untuk autentikasi API.

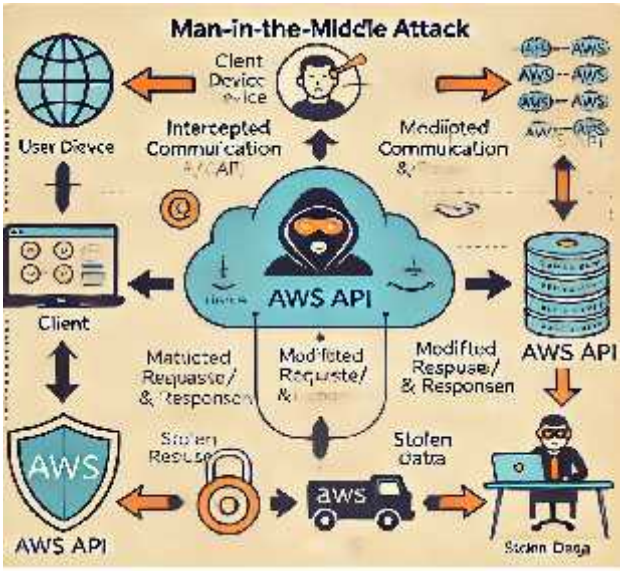
SKENA TEKNOLOGI
JURNAL ILMIAH SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 1 Febuary 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

Serangan lainnya yang juga sangat berbahaya adalah Man-in-the-Middle (MITM) adalah serangan di mana penyerang menyadap, memantau, atau bahkan memodifikasi komunikasi antara klien (misalnya aplikasi pengguna) dan server (API AWS) tanpa sepengetahuan kedua pihak. Serangan ini sering terjadi ketika koneksi tidak aman atau enkripsi tidak diimplementasikan dengan baik.

Cara Kerja Serangan MITM pada API AWS adalah Intercept Koneksi dimana penyerang menggunakan teknik seperti spoofing DNS, ARP spoofing, atau dengan menjadi proxy (Wi-Fi publik berbahaya) untuk menyadap komunikasi antara klien dan server API AWS. Jika koneksi tidak menggunakan protokol yang aman (seperti HTTPS), data seperti API key, token, atau informasi pengguna dapat dibaca secara langsung. Manipulasi Data dapat dilakukan oleh penyerang dapat mengubah data dalam perjalanan, seperti memodifikasi permintaan atau tanggapan API, menyebabkan kerusakan atau kebocoran data. Penyerang melakukan Eksploitasi setelah mendapatkan akses ke data sensitif, penyerang dapat melakukan berbagai tindakan berbahaya, termasuk mencuri kredensial atau mengambil alih sumber daya AWS. Contoh Kasus yang dapat terajdi adalah Klien menggunakan koneksi Wi-Fi publik tanpa VPN untuk mengakses API AWS. Penyerang menyadap token API yang dikirimkan dalam permintaan HTTP, lalu menggunakan token tersebut untuk mengakses sumber daya AWS seperti bucket S3 atau database DynamoDB.

Guna mencegah Serangan MITM pada API AWS dapat menggunakan HTTPS, pastikan semua koneksi menggunakan TLS/SSL untuk mengenkripsi komunikasi. Validasi Sertifikat dengan konfigurasi klien untuk memverifikasi sertifikat server agar menghindari serangan sertifikat palsu. Implementasikan OAuth2 token sementara yang memiliki izin terbatas dan jangka waktu singkat. Pemakaian VPN: Hindari koneksi Wi-Fi publik tanpa proteksi VPN. Monitoring gunakan AWS CloudTrail dan AWS GuardDuty untuk mendeteksi aktivitas mencurigakan.

SKENA TEKNOLOGI
JURNAL ILMIAH SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 1 Febuary 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index



Gambar 3.3. serangan Man-in-the-Middle (MITM) pada API AWS

4. KESIMPULAN

Cloud computing memang telah menjadi salah satu teknologi utama yang sangat berperan di organisasi manapun di dunia. Sehingga banyak di adopsi baik oelh organisasi nirlaba sampai dengan perusahaan nasional sampai dengan multi nasional.

Nanum seiring dengan popularitasnya yang sangat luas, membuat para penyerang juga memiliki keinginan, motovasi dan dengan keilmuannya untuk membuktikan dapat menembus dari celah keamanan yang tidak terlihat. Adapun metode yang saat ini sedang tren dari penyerang memakai metodologi seperti mendapatkan akses secara ilegal, membuat layanan yang disediakan cloud mengalami botnet hingga downtime dengan cara DDoS, melakukan penyerangan pada API dengan untuk mengambil data secara ilegal.

Sehingga perlu dilakukan mitigasi segera dari ancaman tersebut dengan melakukan analisis resiko, serta pengetahuan dari studi kasus yang pernah terjadi, untuk dapat melakukan pencegah dengan teknik yang telah berhasil dibuktikan. Perlunya pelatihan kepada karyawan, memilih mitra atau pihak luar untuk mempelajari lebih lanjut atas serangan baru yang mungkin belum ditemukan cara pencegahaannya.

E- ISSN: 3058-1570
Volume 2 No 1 Febuary 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

5. REFERENSI

Eyal Estrin, 2022, "Cloud Security Handbook: Strategies for Architecting, Designing, and Managing Secure Cloud Services".

Ronald L. Krutz dan Russell Dean Vines. 2020. “Cloud Security: A Comprehensive Guide to Secure Cloud Computing”.

John R. Vacca. 2020. “Cloud Security: A Comprehensive Guide to Secure Cloud Computing”.

Tim Rains. 2020. “Cybersecurity Threats, Malware Trends, and Strategies”.

Tim Mather, Subra Kumaraswamy, dan Shahed Latif , 2020. “Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance”.