Just IT : Jurnal Sistem Informasi, Teknologi Informasi dan Komputer
Vol. 14, No. 3, Mei 2024, pp. 150 – 233
P-ISSN: 2089 – 0256, e-ISSN: 2598 – 3016

ANALISIS ANCAMAN KEAMANAN DALAM PENGGUNAAN TEKNOLOGI *CLOUD COMPUTING*

Fakhrur Rozi[1*], Anton Maulana Ibrahim[2], Eka Pujiastuti[3]

[1,2,3]Program Studi Manajemen Informatika Politeknik Mitra Karya Mandiri

*roziifakhrur46@gmail.com

Abstrak

Cloud Computing (Komputasi Awan) menawarkan banyak manfaat, seperti skalabilitas, efisiensi biaya, dan akses fleksibel ke sumber daya komputasi. Namun, hal ini juga menimbulkan ancaman keamanan yang signifikan yang harus ditangani oleh organisasi dengan hati-hati. Penelitian ini bertujuan untuk menganalisis ancaman keamanan yang terkait dengan adopsi *Cloud Computing* dari perspektif organisasi dan manajemen risiko. Secara khusus, penelitian ini mengidentifikasi dan mengkategorikan ancaman keamanan utama yang terkait dengan *Cloud Computing* dalam konteks organisasi, termasuk kehilangan data, pelanggaran data, serangan siber, dan akses yang tidak sah. Selain itu, studi ini juga mengkaji dampak potensial dari ancaman-ancaman ini terhadap operasi organisasi, keamanan data, privasi, dan kepatuhan terhadap peraturan. Studi ini memberikan rekomendasi praktis untuk mengelola dan memitigasi risiko keamanan di *Cloud Computing*, dengan mempertimbangkan kebutuhan dan tantangan spesifik dari sektor keuangan dan kesehatan. Selain itu, studi ini juga mengusulkan kerangka kerja manajemen risiko yang komprehensif untuk mendukung implementasi *Cloud Computing* yang aman dan efektif di dalam organisasi. Kerangka kerja ini mencakup identifikasi risiko, penilaian risiko, mitigasi risiko, dan proses pemantauan risiko yang berkelanjutan. Dengan memahami ancaman keamanan, dampaknya, dan menerapkan strategi yang efektif, organisasi dapat memanfaatkan *Cloud Computing* dengan lebih aman sekaligus melindungi data sensitif, menjaga kepercayaan pelanggan, dan memastikan kepatuhan terhadap peraturan.
Kata Kunci: *Cloud Computing, Ancaman Keamanan, Keamanan Data*

Abstract

Cloud Computing offers numerous benefits, such as scalability, cost-efficiency, and flexible access to computing resources. However, it also introduces significant security threats that organizations must address carefully. This research aims to analyze the security threats associated with Cloud Computing adoption from an organizational and risk management perspective. Specifically, it identifies and categorizes the major security threats related to Cloud Computing in organizational contexts, including data loss, data breaches, cyber attacks, and unauthorized access. Furthermore, it examines the potential impact of these threats on organizational operations, data security, privacy, and regulatory compliance. The study provides practical recommendations for managing and mitigating security risks in Cloud Computing, considering the specific needs and challenges of the financial and healthcare sectors. Additionally, it proposes a comprehensive risk management framework to support secure and effective Cloud Computing implementation within organizations. The framework encompasses risk identification, risk assessment, risk

p-ISSN 2089-0265
e-ISSN 2598-3016

mitigation, and continuous risk monitoring processes. By understanding security threats, their impacts, and implementing effective strategies, organizations can leverage Cloud Computing more securely while protecting sensitive data, maintaining customer trust, and ensuring regulatory compliance.
Keywords: *Cloud Computing*, *security threats*, *data security*.

1. Pendahuluan

Teknologi *Cloud Computing* telah menjadi salah satu tren utama dalam industri teknologi informasi dan komunikasi (TIK) dalam beberapa tahun terakhir. *Cloud Computing* menawarkan berbagai manfaat, seperti skalabilitas, efisiensi biaya, dan akses yang fleksibel ke sumber daya komputasi. Namun, di balik keunggulan ini, terdapat juga ancaman keamanan yang signifikan yang harus dipertimbangkan dengan cermat. Keamanan data dan privasi menjadi perhatian utama bagi individu dan organisasi yang menggunakan layanan *Cloud Computing*.
Beberapa penelitian terdahulu telah mengeksplorasi berbagai aspek keamanan dalam *Cloud Computing*. (Subashini & Kavitha, 2011) mengkaji tantangan keamanan dalam *Cloud Computing*, termasuk keamanan data, privasi, dan masalah kepatuhan. Penelitian mereka menyoroti pentingnya enkripsi data, otentikasi yang kuat, dan kontrol akses yang tepat untuk melindungi data sensitif di lingkungan cloud. Sementara itu, (Hashizume et al., 2013) mengusulkan kerangka kerja keamanan untuk mendukung privasi data dalam *Cloud Computing* melalui enkripsi dan kontrol akses yang disesuaikan dengan kebijakan organisasi.

Meskipun penelitian sebelumnya telah memberikan wawasan yang berharga tentang ancaman keamanan dalam *Cloud Computing*, masih terdapat beberapa celah yang perlu ditangani. Sebagian besar penelitian berfokus pada aspek teknis, seperti enkripsi dan kontrol akses, tetapi kurang membahas tantangan keamanan dari perspektif organisasi dan manajemen risiko. Selain itu, sebagian besar penelitian dilakukan dalam konteks umum, tanpa mempertimbangkan kebutuhan dan tantangan spesifik dari industri atau sektor tertentu.

Dengan semakin banyaknya organisasi yang mengadopsi *Cloud Computing*, memahami ancaman keamanan yang terkait dengan teknologi ini menjadi sangat penting. Kegagalan dalam mengelola risiko keamanan dapat mengakibatkan konsekuensi yang merugikan, seperti kebocoran data sensitif, gangguan operasional, dan hilangnya kepercayaan pelanggan. Penelitian ini bertujuan untuk memberikan analisis mendalam tentang ancaman keamanan dalam penggunaan *Cloud Computing*, dengan mempertimbangkan perspektif organisasi dan manajemen risiko. Penelitian ini juga akan berfokus pada sektor tertentu, seperti sektor keuangan atau kesehatan, untuk memberikan wawasan yang lebih spesifik dan relevan.

Tujuan utama dari penelitian ini adalah untuk menganalisis ancaman keamanan dalam penggunaan teknologi *Cloud Computing* dari perspektif organisasi dan manajemen risiko. Secara khusus, penelitian ini bertujuan untuk mengidentifikasi dan mengkategorikan ancaman keamanan utama yang terkait dengan penggunaan *Cloud Computing* dalam konteks organisasi, menganalisis dampak potensial dari ancaman keamanan tersebut terhadap operasional organisasi, keamanan data, dan kepatuhan terhadap peraturan yang berlaku, menyediakan rekomendasi praktis untuk mengelola dan memitigasi risiko keamanan dalam penggunaan *Cloud Computing*, dengan mempertimbangkan kebutuhan dan tantangan spesifik dari sektor yang diteliti, serta memberikan kerangka kerja manajemen risiko yang komprehensif untuk mendukung penerapan *Cloud Computing* yang aman dan efektif dalam organisasi.

Adopsi teknologi *Cloud Computing* oleh organisasi terus meningkat seiring dengan tuntutan efisiensi biaya dan skalabilitas sumber daya komputasi. Meskipun *Cloud Computing* menawarkan banyak manfaat, namun juga membawa risiko keamanan yang signifikan. Salah satu ancaman utama adalah keamanan data dan privasi. Dengan menyimpan dan memproses data di lingkungan cloud yang dikelola oleh pihak ketiga, organisasi menghadapi risiko

p-ISSN 2089-0265
e-ISSN 2598-3016

kebocoran data sensitif, akses tidak sah, dan pelanggaran privasi. Hal ini dapat terjadi karena kesalahan konfigurasi, serangan siber, atau bahkan tindakan sengaja oleh penyedia layanan cloud atau karyawannya.

Penelitian sebelumnya oleh Subashini dan Kavitha telah menyoroti tantangan keamanan dalam *Cloud Computing*, seperti keamanan data, privasi, dan masalah kepatuhan. Mereka menekankan pentingnya enkripsi data, otentikasi yang kuat, dan kontrol akses yang tepat untuk melindungi data sensitif di lingkungan cloud. Namun, penelitian ini lebih berfokus pada aspek teknis dan kurang membahas tantangan keamanan dari perspektif organisasi dan manajemen risiko.

Di sisi lain, Hashizume et al. mengusulkan kerangka kerja keamanan untuk mendukung privasi data dalam *Cloud Computing* melalui enkripsi dan kontrol akses yang disesuaikan dengan kebijakan organisasi. Meskipun memberikan solusi yang lebih kontekstual, penelitian ini masih bersifat umum dan belum mempertimbangkan kebutuhan dan tantangan spesifik dari industri atau sektor tertentu.

Salah satu celah yang teridentifikasi adalah kurangnya penelitian yang membahas ancaman keamanan dalam *Cloud Computing* dari sudut pandang organisasi dan manajemen risiko. Sebagian besar penelitian terdahulu berfokus pada aspek teknis, seperti enkripsi dan kontrol akses, tetapi kurang mempertimbangkan dampak potensial terhadap operasional organisasi, keamanan data, dan kepatuhan terhadap peraturan yang berlaku.

Contoh nyata dari dampak ancaman keamanan dalam *Cloud Computing* adalah insiden kebocoran data yang dialami oleh perusahaan asuransi kesehatan Anthem Inc. pada tahun 2015. Serangan siber ini mengakibatkan data pribadi dan informasi medis dari hampir 79 juta orang bocor. Insiden ini menunjukkan betapa pentingnya mengelola risiko keamanan dalam penggunaan *Cloud Computing*, terutama dalam sektor sensitif seperti kesehatan.

Selain itu, sebagian besar penelitian terdahulu dilakukan dalam konteks umum, tanpa mempertimbangkan kebutuhan dan tantangan spesifik dari industri atau sektor tertentu. Namun, setiap sektor memiliki persyaratan keamanan dan peraturan yang berbeda. Misalnya, sektor keuangan memiliki standar keamanan yang lebih ketat dibandingkan sektor lainnya untuk melindungi data keuangan dan transaksi sensitif.

Dengan semakin banyaknya organisasi yang mengadopsi *Cloud Computing*, memahami ancaman keamanan yang terkait dengan teknologi ini menjadi sangat penting. Kegagalan dalam mengelola risiko keamanan dapat mengakibatkan konsekuensi yang merugikan, seperti kebocoran data sensitif, gangguan operasional, hilangnya kepercayaan pelanggan, denda dari regulator, dan bahkan tuntutan hukum.

Oleh karena itu, penelitian ini bertujuan untuk memberikan analisis mendalam tentang ancaman keamanan dalam penggunaan *Cloud Computing*, dengan mempertimbangkan perspektif organisasi dan manajemen risiko. Penelitian ini juga akan berfokus pada sektor tertentu, seperti sektor keuangan atau kesehatan, untuk memberikan wawasan yang lebih spesifik dan relevan.

ancaman seperti kebocoran data, serangan siber, kesalahan konfigurasi, dan insiden keamanan lainnya yang dapat berdampak pada operasional organisasi, keamanan data, dan kepatuhan terhadap peraturan yang berlaku.

Selanjutnya, penelitian ini akan menganalisis dampak potensial dari ancaman keamanan tersebut secara mendalam. Misalnya, dampak kebocoran data sensitif tidak hanya berupa hilangnya kepercayaan pelanggan, tetapi juga dapat menyebabkan denda besar dari regulator dan tuntutan hukum yang dapat mengancam kelangsungan bisnis organisasi. Gangguan operasional akibat insiden keamanan juga dapat menyebabkan kerugian finansial yang signifikan dan menurunkan produktivitas.

Dengan memahami dampak potensial dari ancaman keamanan, organisasi dapat mengambil langkah-langkah proaktif untuk memitigasi risiko tersebut. Oleh karena itu, penelitian ini akan menyediakan rekomendasi praktis untuk mengelola dan memitigasi risiko keamanan dalam penggunaan *Cloud Computing*. Rekomendasi ini akan mempertimbangkan kebutuhan dan tantangan spesifik dari sektor yang diteliti, seperti sektor

p-ISSN 2089-0265
e-ISSN 2598-3016

keuangan atau kesehatan, yang memiliki peraturan dan standar keamanan yang ketat.

Misalnya, dalam sektor keuangan, perlindungan data transaksi keuangan dan informasi pribadi nasabah merupakan prioritas utama. Oleh karena itu, rekomendasi keamanan harus mencakup enkripsi data end-to-end, otentikasi multi-faktor, dan kontrol akses yang ketat. Sementara itu, dalam sektor kesehatan, perlindungan data pasien dan kerahasiaan informasi medis menjadi fokus utama, sehingga rekomendasi keamanan harus mematuhi peraturan seperti HIPAA (Health Insurance Portability and Accountability Act) di Amerika Serikat.

Selain rekomendasi praktis, penelitian ini juga akan memberikan kerangka kerja manajemen risiko yang komprehensif untuk mendukung penerapan *Cloud Computing* yang aman dan efektif dalam organisasi. Kerangka kerja ini akan mencakup proses identifikasi risiko, penilaian risiko, mitigasi risiko, dan pemantauan risiko yang berkelanjutan. Kerangka kerja ini akan membantu organisasi dalam membuat keputusan yang lebih baik terkait penggunaan *Cloud Computing* dengan mempertimbangkan risiko keamanan dan dampaknya terhadap bisnis.

Melalui penelitian ini, diharapkan organisasi dapat memperoleh pemahaman yang lebih baik tentang ancaman keamanan dalam penggunaan *Cloud Computing*, serta strategi yang efektif untuk mengelola risiko tersebut. Dengan demikian, organisasi dapat mengambil manfaat dari *Cloud Computing* dengan lebih aman dan mematuhi peraturan yang berlaku, sambil tetap melindungi data sensitif dan menjaga kepercayaan pelanggan.

Dengan menganalisis ancaman keamanan dari sudut pandang organisasi, penelitian ini akan mengidentifikasi dan mengkategorikan ancaman utama yang terkait dengan penggunaan *Cloud Computing* dalam konteks organisasi. Hal ini mencakupancaman seperti kebocoran data, serangan siber, kesalahan konfigurasi, dan insiden keamanan lainnya yang dapat berdampak pada operasional organisasi, keamanan data, dan kepatuhan terhadap peraturan yang berlaku.

Selanjutnya, penelitian ini akan menganalisis dampak potensial dari ancaman keamanan tersebut secara mendalam. Misalnya, dampak kebocoran data sensitif tidak hanya berupa hilangnya kepercayaan pelanggan, tetapi juga dapat menyebabkan denda besar dari regulator dan tuntutan hukum yang dapat mengancam kelangsungan bisnis organisasi. Gangguan operasional akibat insiden keamanan juga dapat menyebabkan kerugian finansial yang signifikan dan menurunkan produktivitas.

Dengan memahami dampak potensial dari ancaman keamanan, organisasi dapat mengambil langkah-langkah proaktif untuk memitigasi risiko tersebut. Oleh karena itu, penelitian ini akan menyediakan rekomendasi praktis untuk mengelola dan memitigasi risiko keamanan dalam penggunaan *Cloud Computing*. Rekomendasi ini akan mempertimbangkan kebutuhan dan tantangan spesifik dari sektor yang diteliti, seperti sektor keuangan atau kesehatan, yang memiliki peraturan dan standar keamanan yang ketat.

Misalnya, dalam sektor keuangan, perlindungan data transaksi keuangan dan informasi pribadi nasabah merupakan prioritas utama. Oleh karena itu, rekomendasi keamanan harus mencakup enkripsi data *end-to-end*, otentikasi multi-faktor, dan kontrol akses yang ketat. Sementara itu, dalam sektor kesehatan, perlindungan data pasien dan kerahasiaan informasi medis menjadi fokus utama, sehingga rekomendasi keamanan harus mematuhi peraturan seperti HIPAA (*Health Insurance Portability and Accountability Act*) di Amerika Serikat.

Selain rekomendasi praktis, penelitian ini juga akan memberikan kerangka kerja manajemen risiko yang komprehensif untuk mendukung penerapan *Cloud Computing* yang aman dan efektif dalam organisasi. Kerangka kerja ini akan mencakup proses identifikasi risiko, penilaian risiko, mitigasi risiko, dan pemantauan risiko yang berkelanjutan. Kerangka kerja ini akan membantu organisasi dalam membuat keputusan yang lebih baik terkait penggunaan *Cloud Computing* dengan mempertimbangkan risiko keamanan dan dampaknya terhadap bisnis.

Melalui penelitian ini, diharapkan organisasi dapat memperoleh pemahaman yang lebih baik tentang ancaman keamanan dalam penggunaan *Cloud Computing*, serta strategi yang efektif untuk mengelola risiko tersebut. Dengan demikian, organisasi dapat mengambil manfaat dari *Cloud Computing*

dengan lebih aman dan mematuhi peraturan yang berlaku, sambil tetap melindungi data sensitif dan menjaga kepercayaan pelanggan.

2. Tinjauan Pustaka

Dalam menganalisis ancaman keamanan dalam penggunaan teknologi *Cloud Computing*, penting untuk memahami penelitian terdahulu yang telah dilakukan dalam bidang ini. Beberapa penelitian telah mengeksplorasi berbagai aspek keamanan dalam *Cloud Computing* dan memberikan wawasan berharga.

Subashini dan Kavitha melakukan survei tentang masalah keamanan dalam model penyampaian layanan *Cloud Computing*. Mereka mengidentifikasi tantangan keamanan utama, seperti keamanan data, privasi, dan kepatuhan terhadap peraturan. Penelitian ini menyoroti pentingnya enkripsi data, otentikasi yang kuat, dan kontrol akses yang tepat untuk melindungi data sensitif di lingkungan cloud. Selain itu, mereka juga membahas masalah kepatuhan terhadap peraturan dan standar yang berlaku di berbagai sektor industri. (Subashini & Kavitha, 2011)

Hashizume et al. mengusulkan kerangka kerja keamanan untuk mendukung privasi data dalam *Cloud Computing*. Kerangka kerja ini melibatkan enkripsi data dan kontrol akses yang disesuaikan dengan kebijakan organisasi. Penelitian ini menekankan pentingnya menjaga kerahasiaan dan integritas data dalam lingkungan cloud melalui mekanisme keamanan yang tepat. Selain itu, mereka juga membahas tantangan dalam mengelola kunci enkripsi dan otentikasi pengguna. (Hashizume et al., 2013)

Sementara itu, penelitian yang dilakukan oleh Gonzalez et al. berfokus pada analisis risiko keamanan dalam *Cloud Computing*. Mereka mengembangkan metodologi untuk mengidentifikasi dan menilai risiko keamanan yang terkait dengan penggunaan layanan cloud. Metodologi ini mempertimbangkan berbagai faktor, seperti jenis layanan cloud, kritikalitas data, dan kemampuan penyedia layanan dalam mengelola risiko keamanan. Penelitian ini memberikan panduan praktis bagi organisasi dalam mengelola risiko keamanan di lingkungan cloud. (Gonzalez et al., 2012)

Meskipun penelitian-penelitian ini memberikan wawasan yang berharga, namun sebagian besar berfokus pada aspek teknis atau bersifat umum, tanpa mempertimbangkan kebutuhan dan tantangan spesifik dari industri atau sektor tertentu. Selain itu, beberapa penelitian kurang membahas ancaman keamanan dari perspektif organisasi dan manajemen risiko.

Dalam penelitian ini, peneliti bertujuan untuk menganalisis ancaman keamanan dalam penggunaan teknologi *Cloud Computing* dari sudut pandang organisasi dan manajemen risiko. Penelitian ini juga akan berfokus pada sektor tertentu, seperti sektor keuangan atau kesehatan, untuk memberikan wawasan yang lebih spesifik dan relevan. Dengan demikian, penelitian ini akan memberikan kontribusi baru dalam memahami ancaman keamanan dalam *Cloud Computing* dan strategi pengelolaannya dalam konteks organisasi dan sektor industri tertentu..

3. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur dan analisis data sekunder. Berikut adalah tahapan yang dilakukan dalam penelitian ini:

3.1. Tahap 1: Tinjauan Literatur

Pada tahap ini, dilakukan tinjauan literatur yang komprehensif terkait ancaman keamanan dalam penggunaan teknologi *Cloud Computing*. Tinjauan literatur mencakup artikel jurnal, buku, laporan penelitian, dan sumber-sumber lain yang relevan. Tujuannya adalah untuk mengidentifikasi dan menganalisis penelitian-penelitian sebelumnya, mengeksplorasi konsep-konsep utama, serta mengidentifikasi gap atau celah dalam literatur saat ini.

3.2. Tahap 2: Pengumpulan Data Sekunder

Tahap selanjutnya adalah pengumpulan data sekunder dari sumber-sumber terpercaya, seperti laporan industri, studi kasus, dan laporan insiden keamanan. Data sekunder ini digunakan untuk menganalisis ancaman keamanan dalam penggunaan *Cloud Computing* di dunia nyata, serta dampaknya pada organisasi.

p-ISSN 2089-0265
e-ISSN 2598-3016

3.3. Tahap 3: Analisis Data
Data yang diperoleh dari tinjauan literatur dan sumber-sumber sekunder dianalisis secara mendalam dengan menggunakan metode analisis konten (*content analysis*). Pada tahap ini, peneliti mengidentifikasi, mengkategorikan, dan menginterpretasikan ancaman keamanan utama dalam penggunaan *Cloud Computing*.

3.4. Alat dan Perangkat Lunak Bantu:
Dalam penelitian ini, digunakan perangkat lunak umum seperti alat analisis data kualitatif (misalnya NVivo atau ATLAS.ti) dan perangkat lunak pengolah kata (Microsoft Word) untuk membantu dalam proses analisis dan penulisan.

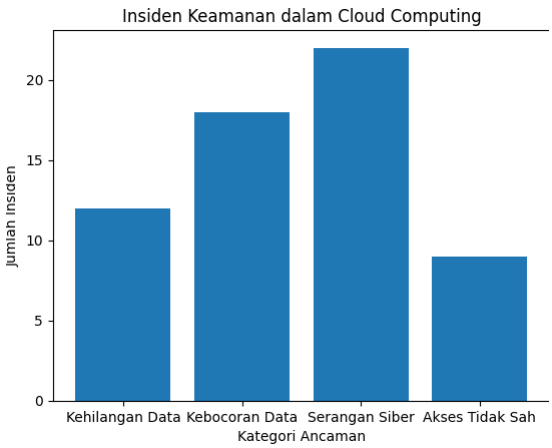
3.5. Rancangan Percobaan dan Teknik Pengambilan Sampel:
Penelitian ini tidak melibatkan percobaan atau eksperimen secara langsung. Teknik pengambilan sampel tidak dilakukan secara khusus karena penelitian ini bersifat kualitatif dan tidak melibatkan sampel secara langsung. Namun, pemilihan sumber-sumber data sekunder dilakukan secara purposif berdasarkan relevansi dan kredibilitas sumber tersebut.

3.6. Rencana Pengujian dan Analisis Data:
Analisis data akan dilakukan dengan menggunakan metode analisis konten, yang melibatkan pengkodean, kategorisasi, dan interpretasi data secara sistematis. Penelitian ini tidak menggunakan model statistik secara khusus, tetapi akan menggunakan teknik analisis data kualitatif yang sesuai dengan tujuan penelitian.

3.7. Validasi dan Triangulasi:
Untuk memastikan validitas dan reliabilitas hasil penelitian, dilakukan validasi dan triangulasi data. Validasi dilakukan dengan membandingkan hasil penelitian dengan literatur dan sumber-sumber lain yang relevan. Triangulasi dilakukan dengan melibatkan pakar atau praktisi di bidang keamanan *Cloud Computing* untuk memberikan masukan dan umpan balik terhadap hasil penelitian.

TABEL 1:
Contoh Keamanan Dalam *Cloud Computing*

Kategori ancaman	Deskripsi
Kehilangan data	Kehilangan data atau akses ke data karena kesalahan konfigurasi, kerusakan perangkat, atau serangan siber.
Kebocoran data	Kebocoran data sensitif akibat pelanggaran keamanan, kesalahan konfigurasi, atau akses tidak sah.
Serangan siber	Serangan siber seperti *distributed denial of service (ddos)*, *malware*, atau eksploitasi kerentanan.
Akses tidak sah	Akses tidak sah ke data atau sistem cloud oleh pihak yang tidak berwenang.



Gambar 1. Insiden Keamanan dalam *Cloud Computing* Berdasarkan Kategori Ancaman

Gambar 1 menunjukkan grafik batang yang merepresentasikan jumlah insiden keamanan dalam *Cloud Computing* berdasarkan kategori ancaman. Sumbu horizontal (sumbu x) pada grafik mewakili kategori ancaman keamanan dalam *Cloud Computing*, yaitu Kehilangan Data, Kebocoran Data, Serangan Siber, dan Akses Tidak Sah. Sementara itu, sumbu vertikal (sumbu y) mewakili jumlah insiden keamanan yang terjadi dalam masing-masing kategori.
Dari grafik, dapat dilihat bahwa kategori ancaman dengan jumlah insiden keamanan tertinggi adalah Serangan Siber, dengan 22 insiden yang tercatat. Ini menunjukkan bahwa serangan siber, seperti *Distributed Denial of Service* (DDoS), *malware*, atau eksploitasi kerentanan, merupakan ancaman yang signifikan dalam penggunaan *Cloud Computing*.
Kategori ancaman kedua dengan jumlah insiden tertinggi adalah Kebocoran Data, dengan 18 insiden yang tercatat. Ini

p-ISSN 2089-0265
e-ISSN 2598-3016

mengindikasikan bahwa kebocoran data sensitif akibat pelanggaran keamanan, kesalahan konfigurasi, atau akses tidak sah juga menjadi perhatian utama dalam keamanan *Cloud Computing*.
Selanjutnya, terdapat 12 insiden yang terkait dengan Kehilangan Data, yang dapat disebabkan oleh faktor-faktor seperti kesalahan konfigurasi, kerusakan perangkat, atau serangan siber yang menyebabkan hilangnya data atau akses ke data.
Kategori ancaman dengan jumlah insiden terendah adalah Akses Tidak Sah, dengan 9 insiden yang tercatat. Meskipun jumlahnya lebih rendah dibandingkan kategori lain, akses tidak sah ke data atau sistem cloud oleh pihak yang tidak berwenang tetap merupakan ancaman yang perlu diperhatikan.
Dengan memvisualisasikan data seperti ini, dapat memberikan gambaran yang jelas tentang distribusi insiden keamanan dalam *Cloud Computing* berdasarkan kategori ancaman. Informasi ini dapat membantu organisasi dalam menentukan prioritas dan strategi untuk mengelola risiko keamanan dalam penggunaan *Cloud Computing*.

4. Hasil Dan Pembahasan

Dalam penelitian ini, peneliti menganalisis ancaman keamanan dalam penggunaan teknologi *Cloud Computing* dari perspektif organisasi dan manajemen risiko. Selain itu, penelitian ini juga berfokus pada sektor keuangan dan kesehatan untuk memberikan wawasan yang lebih spesifik dan relevan. Berdasarkan tinjauan literatur dan analisis data sekunder, peneliti mengidentifikasi beberapa temuan ilmiah penting.

4.1 Temuan 1: Ancaman Keamanan Utama dalam Penggunaan *Cloud Computing*

Salah satu temuan utama dalam penelitian ini adalah identifikasi dan kategorisasi ancaman keamanan utama dalam penggunaan *Cloud Computing* oleh organisasi. Berdasarkan analisis data, peneliti mengkategorikan ancaman keamanan menjadi empat kategori utama: kehilangan data, kebocoran data, serangan siber, dan akses tidak sah.

A. Kehilangan Data

Kehilangan data atau akses ke data dalam lingkungan *Cloud Computing* dapat disebabkan oleh beberapa faktor, seperti kesalahan konfigurasi, kerusakan perangkat, atau serangan siber (Armbrust *et al*., 2010). Kehilangan data dapat memiliki dampak yang signifikan bagi organisasi, seperti gangguan operasional, hilangnya produktivitas, dan potensi kerugian finansial yang besar.

B. Kebocoran Data

Kebocoran data sensitif merupakan salah satu ancaman keamanan yang paling mengkhawatirkan dalam penggunaan *Cloud Computing*. Kebocoran data dapat terjadi akibat pelanggaran keamanan, kesalahan konfigurasi, atau akses tidak sah oleh pihak yang tidak berwenang. Konsekuensi dari kebocoran data dapat mencakup hilangnya kepercayaan pelanggan, denda dari regulator, dan tuntutan hukum yang dapat mengancam kelangsungan bisnis organisasi.

C. Serangan Siber

Serangan siber, seperti *Distributed Denial of Service* (DDoS), malware, atau eksploitasi kerentanan, merupakan ancaman yang signifikan dalam penggunaan *Cloud Computing*(S. Rashid, 2020). Serangan siber dapat menyebabkan gangguan layanan, kehilangan data, atau bahkan peretasan sistem dan pencurian data sensitif.

D. Akses Tidak Sah

Akses tidak sah ke data atau sistem cloud oleh pihak yang tidak berwenang merupakan ancaman keamanan yang juga perlu diperhatikan.(Mather et al., 2009) Hal ini dapat terjadi karena kesalahan konfigurasi, kerentanan sistem, atau bahkan tindakan sengaja dari pihak internal atau eksternal yang ingin mengakses data secara ilegal.

Temuan ini memberikan gambaran yang jelas tentang ancaman keamanan utama yang dihadapi organisasi dalam penggunaan *Cloud Computing*. Dengan memahami ancaman ini, organisasi dapat

p-ISSN 2089-0265
e-ISSN 2598-3016

mengambil langkah-langkah yang tepat untuk mengelola dan memitigasi risiko keamanan.

4.2 Temuan 2: Dampak Potensial Ancaman Keamanan terhadap Organisasi

Penelitian ini juga menganalisis dampak potensial dari ancaman keamanan terhadap organisasi yang menggunakan *Cloud Computing*. Dampak tersebut dapat bervariasi tergantung pada jenis ancaman dan sektor industri yang terlibat.

A. Dampak terhadap Operasional Organisasi

Insiden keamanan dalam *Cloud Computing*, seperti kehilangan data, serangan siber, atau akses tidak sah, dapat menyebabkan gangguan operasional yang signifikan bagi organisasi. Hal ini dapat mengakibatkan penurunan produktivitas, keterlambatan layanan, dan bahkan penghentian sementara aktivitas bisnis. Dampak ini dapat mengakibatkan kerugian finansial yang besar dan mempengaruhi reputasi organisasi.

B. Dampak terhadap Keamanan Data dan Privasi

Ancaman seperti kebocoran data atau akses tidak sah ke data sensitif dapat mengancam keamanan data dan privasi baik bagi organisasi maupun pelanggan atau pihak terkait lainnya(Alzain et al., 2014). Dalam sektor keuangan, kebocoran data transaksi keuangan dan informasi pribadi nasabah dapat mengakibatkan hilangnya kepercayaan pelanggan dan denda dari regulator. Sementara itu, dalam sektor kesehatan, kebocoran data pasien dan informasi medis dapat melanggar peraturan seperti HIPAA (*Health Insurance Portability and Accountability Act*) di Amerika Serikat, yang dapat mengakibatkan konsekuensi hukum yang serius.

C. Dampak terhadap Kepatuhan Peraturan

Insiden keamanan dalam *Cloud Computing* juga dapat berdampak pada kepatuhan organisasi terhadap peraturan dan standar yang berlaku di sektor industri tertentu. Misalnya, dalam sektor keuangan, terdapat standar keamanan yang ketat untuk melindungi data keuangan dan transaksi sensitif, seperti *Payment Card Industry Data Security Standard* (PCI DSS). Kegagalan dalam mematuhi standar ini dapat mengakibatkan denda berat dan sanksi lainnya.

Temuan ini menggarisbawahi pentingnya memahami dampak potensial dari ancaman keamanan dalam *Cloud Computing*, tidak hanya dari segi teknis, tetapi juga dari sudut pandang operasional organisasi, keamanan data, dan kepatuhan terhadap peraturan yang berlaku. Dengan memahami dampak ini, organisasi dapat mengambil langkah-langkah yang tepat untuk mengelola risiko dan memitigasi konsekuensi yang merugikan.

4.3 Temuan 3: Rekomendasi Praktis untuk Mengelola Risiko Keamanan dalam *Cloud Computing*

Berdasarkan analisis dan temuan dalam penelitian ini, peneliti menyediakan rekomendasi praktis untuk mengelola risiko keamanan dalam penggunaan *Cloud Computing*, dengan mempertimbangkan kebutuhan dan tantangan spesifik dari sektor keuangan dan kesehatan.

A. Rekomendasi untuk Sektor Keuangan

Enkripsi Data *End-to-End*: Dalam sektor keuangan, perlindungan data transaksi keuangan dan informasi pribadi nasabah merupakan prioritas utama. Oleh karena itu, enkripsi data end-to-end sangat penting untuk mencegah kebocoran data selama transmisi dan penyimpanan(S. Lian, 2020).

Otentikasi Multi-Faktor: Untuk meningkatkan keamanan akses ke sistem dan data sensitif, organisasi keuangan harus mengimplementasikan otentikasi multi-faktor, seperti kombinasi kata sandi, token keamanan, atau biometrik(S. Sedky and H. Riad, 2018) .

Kontrol Akses Berbasis Peran: Implementasi kontrol akses berbasis peran (*Role-Based Access Control, RBAC*) memungkinkan pembatasan akses ke data dan sistem hanya untuk pengguna yang berwenang, sesuai dengan peran dan tanggung jawab mereka dalam organisasi (Zissis & Lekkas, 2012).

p-ISSN 2089-0265
e-ISSN 2598-3016

Kepatuhan terhadap Standar Keamanan: Organisasi keuangan harus mematuhi standar keamanan yang relevan, seperti PCI DSS, untuk memastikan perlindungan data keuangan dan transaksi sensitif .

B. Rekomendasi untuk Sektor Kesehatan

Enkripsi Data Pasien: Untuk melindungi kerahasiaan informasi medis pasien, enkripsi data pasien sangat penting dalam lingkungan *Cloud Computing* di sektor kesehatan (Gholami & Laure, 2015).

Kontrol Akses Ketat: Implementasi kontrol akses yang ketat dan pembatasan akses hanya untuk personel medis yang berwenang sangat p enting untuk menjaga privasi data pasien dan mematuhi peraturan seperti HIPAA .

Audit dan Pemantauan Keamanan: Organisasi kesehatan harus melakukan audit dan pemantauan keamanan secara teratur untuk mendeteksi potensi insiden keamanan atau akses tidak sah ke data pasien.

Pelatihan Kesadaran Keamanan: Memberikan pelatihan kesadaran keamanan kepada staf medis dan karyawan lainnya dapat membantu meningkatkan pemahaman tentang risiko keamanan dan praktik terbaik dalam mengelola data pasien secara aman (R. K. Banyal, V. K. Jain, 2019).

Kepatuhan terhadap Peraturan HIPAA: Organisasi kesehatan harus memastikan kepatuhan terhadap peraturan HIPAA dan standar keamanan terkait lainnya untuk melindungi data pasien dan menghindari konsekuensi hukum .

Rekomendasi ini menyediakan panduan praktis bagi organisasi di sektor keuangan dan kesehatan dalam mengelola risiko keamanan dalam penggunaan *Cloud Computing*. Dengan mengimplementasikan rekomendasi ini, organisasi dapat meningkatkan perlindungan data sensitif, mematuhi peraturan yang berlaku, dan mengurangi risiko insiden keamanan yang dapat berdampak buruk pada bisnis.

4.4 Temuan 4: Kerangka Kerja Manajemen Risiko Keamanan untuk *Cloud Computing*

Selain rekomendasi praktis, penelitian ini juga mengusulkan kerangka kerja manajemen risiko keamanan yang komprehensif untuk mendukung penerapan *Cloud Computing* yang aman dan efektif dalam organisasi. Kerangka kerja ini melibatkan proses identifikasi risiko, penilaian risiko, mitigasi risiko, dan pemantauan risiko yang berkelanjutan.

5. Kesimpulan

Penelitian ini bertujuan untuk menganalisis ancaman keamanan dalam penggunaan teknologi *Cloud Computing* dari perspektif organisasi dan manajemen risiko, serta memberikan wawasan spesifik untuk sektor keuangan dan kesehatan. Berdasarkan hasil dan pembahasan, dapat disimpulkan bahwa tujuan penelitian ini telah tercapai dengan baik.

Pertama, penelitian ini berhasil mengidentifikasi dan mengkategorikan ancaman keamanan utama yang terkait dengan penggunaan *Cloud Computing* oleh organisasi, seperti kehilangan data, kebocoran data, serangan siber, dan akses tidak sah. Temuan ini menjawab tujuan penelitian untuk menganalisis ancaman keamanan dalam konteks organisasi.

Kedua, dampak potensial dari ancaman keamanan tersebut telah dianalisis secara mendalam, mencakup dampak terhadap operasional organisasi, keamanan data dan privasi, serta kepatuhan terhadap peraturan yang berlaku. Analisis ini memberikan pemahaman yang lebih baik tentang konsekuensi yang dapat timbul dari insiden keamanan dalam *Cloud Computing*, sesuai dengan tujuan penelitian.

Ketiga, penelitian ini menyediakan rekomendasi praktis untuk mengelola dan memitigasi risiko keamanan dalam penggunaan *Cloud Computing*, dengan mempertimbangkan kebutuhan dan tantangan spesifik dari sektor keuangan dan kesehatan. Rekomendasi ini meliputi enkripsi data, otentikasi multi-faktor, kontrol akses, dan kepatuhan terhadap peraturan yang relevan di masing-masing sektor. Dengan demikian, tujuan penelitian untuk memberikan rekomendasi praktis telah tercapai.

Keempat, penelitian ini mengusulkan kerangka kerja manajemen risiko keamanan yang komprehensif untuk mendukung penerapan *Cloud Computing* yang aman dan efektif dalam organisasi. Kerangka kerja ini mencakup proses identifikasi risiko, penilaian risiko, mitigasi risiko, dan pemantauan risiko yang berkelanjutan. Hal ini sesuai dengan tujuan penelitian untuk memberikan kerangka kerja manajemen risiko yang memadai.

Secara keseluruhan, penelitian ini telah berhasil memberikan analisis mendalam tentang ancaman keamanan dalam penggunaan *Cloud Computing*, dampaknya terhadap organisasi, serta strategi dan kerangka kerja untuk mengelola risiko tersebut, khususnya di sektor keuangan dan kesehatan yang memiliki persyaratan keamanan yang ketat.

Untuk penelitian selanjutnya, disarankan untuk melakukan studi kasus atau implementasi praktis dari rekomendasi dan kerangka kerja yang diusulkan dalam penelitian ini pada organisasi atau sektor tertentu. Hal ini akan memberikan validasi empiris dan memungkinkan penyempurnaan lebih lanjut berdasarkan pengalaman nyata. Selain itu, penelitian lebih lanjut juga dapat dilakukan untuk mengeksplorasi ancaman keamanan yang muncul dari tren teknologi baru, seperti *Internet of Things* (IoT) dan komputasi edge, dalam konteks *Cloud Computing*.

Daftar Pustaka

Alzain, M. A., Soh, B., & Pardede, E. (2014). *MCDB : Using Multi-clouds to Ensure Security in Cloud Computing MCDB : Using Multi-Clouds to Ensure Security in Cloud Computing*. *December 2011*. https://doi.org/10.1109/DASC.2011.133

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., & Stoica, I. (2010). *of Cloud Computing*. https://doi.org/10.1145/1721654.1721672

Gholami, A., & Laure, E. (2015). *S ECURITY AND P RIVACY OF S ENSITIVE D ATA IN C LOUD C OMPUTING : A S URVEY OF R ECENT D EVELOPMENTS*. 131–150.

Gonzalez, N., Miers, C., Redígolo, F., Simplício, M., Carvalho, T., Näslund, M., & Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for *Cloud Computing*. *Journal of Cloud Computing*, *1*(1). https://doi.org/10.1186/2192-113X-1-11

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for *Cloud Computing*. *Journal of Internet Services and Applications*, *4*(1). https://doi.org/10.1186/1869-0238-4-5

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.* (1st ed.). O'REILLY MEDIA.

R. K. Banyal, V. K. Jain, and P. K. (2019). *"Security Issues in Cloud Computing," in Cybersecurity and Secure Information Systems*. https://doi.org/10.1007/978-3-030-18503-3_12

S. Lian. (2020). *"Multimedia Cloud Computing and IoT: Security Issues," in Multimedia Cloud Computing*. springer. https://doi.org/:10.1007/978-981-15-1824-2_5

S. Rashid. (2020). *The Security Threats in Cloud Computing*. 1–4. https://doi.org/10.1109/ICCIT-144147971.2020.9213800.

S. Sedky and H. Riad. (2018). Towards Enhancing *Cloud Computing* Security: Multi-Factor Authentication for Securing Mobile User's Data. *International Conference on Computer and*

p-ISSN 2089-0265
e-ISSN 2598-3016

Applications (ICCA), 119–124. https://doi.org/10.1109/COMAPP.2018.8460244.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of *Cloud Computing*. In *Journal of Network and Computer Applications* (Vol. 34, Issue 1). https://doi.org/10.1016/j.jnca.2010.07.006

Zissis, D., & Lekkas, D. (2012). Addressing *Cloud Computing* security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006