Sanskara Manajemen dan Bisnis
Vol. 02, No. 02, Maret, pp. 67-78
ISSN: 2963-024X, DOI: 10.58812/smb.v2i02

Downtime Data Center: Memahami Penyebab, Dampak, dan Solusi Efektif

Syarifah Fahira Sulaiman[1], Adhitia Hadi Priambodo[2]
[1] Universitas Gadjah Mada, syarifahfahirasulaiman@mail.ugm.ac.id
[2] Universitas Gadjah Mada, adhitiahadipriambodo@mail.ugm.ac.id

Info Artikel

Article history:

Received Dec, 2023
Revised Mar, 2024
Accepted Mar, 2024

Kata Kunci:

Data Center, *Downtime*, Ensure, Impact

Keywords:

Data Center, *Downtime*, Ensure, Impact

ABSTRAK

Penelitian ini fokus pada pengelolaan risiko *downtime* di *Data Center*, khususnya dari perspektif penyedia layanan. Dengan memanfaatkan metode *systematic literature review*, penelitian ini menyelidiki dampak *downtime* yang kecil tetapi signifikan di *Data Center*, serta strategi yang digunakan penyedia layanan untuk mengatasi masalah tersebut. Temuan utama menunjukkan bahwa *downtime*, meskipun singkat, dapat menyebabkan kerugian finansial yang besar dan gangguan operasional. Strategi pencegahan dan pemulihan *downtime* dieksplorasi, termasuk optimasi *multi-server*, deteksi risiko dini, dan manajemen efisien sumber daya. Penelitian ini memberikan wawasan penting untuk penyedia *Data Center* di Indonesia dalam meningkatkan layanan dan keamanan, serta membantu mereka bersaing di pasar global.

ABSTRACT

This research focuses on the management of downtime risks in Data Centers from a service provider perspective. Utilizing the systematic literature review method, it investigates the impacts of small yet significant downtimes in Data Centers, along with the strategies employed by service providers to address these issues. Key findings highlight that even brief downtimes can lead to substantial financial losses and operational disruptions. Strategies for downtime prevention and recovery are explored, including multi-server optimization, early risk detection, and efficient resource management. This study offers crucial insights for Indonesian Data Center providers to enhance their services and security, aiding them in competing in the global market.

Corresponding Author:

Name: Syarifah Fahira Sulaiman
Institution: Universitas Gadjah Mada, Bulaksumur, Caturtunggal, Kec. Depok, Kabupaten Sleman Daerah Istimewa Yogyakarta 55281
Email: syarifahfahirasulaiman@mail.ugm.ac.id

1. PENDAHULUAN

Besarnya penggunaan tempat penyimpanan data yang besar dan banyak oleh organisasi di era digital saat ini (Taylor, 2022) menyebabkan *Data Center* juga semakin banyak digunakan. *Data Center* merupakan sebuah *database* yang digunakan untuk penyimpanan data, pemrosesan data, pengelolaan data, dan lain sebagainya yang disimpan di ruangan fisik. (Hernandez et al., 2018; Taylor, 2022). Penelitian-penelitian terdahulu banyak memberikan bukti empiris mengenai

bagaimana organisasi pengguna *Data Center* mengatasi risiko *downtime* pada *Data Center*nya, tetapi tidak melihat dari perspektif penyedia *Data Center*-nya. Seperti penelitian yang dilakukan oleh Nagashree et al., (2018) yang merekomendasikan penerapan manajemen deteksi agar dapat meningkatkan keamanan *Data Center* saat terjadi *downtime* (Anwar & Malik, 2014) dan juga dapat meminimalkan waktu terjadinya *downtime* (Frolov, 2020). Sedangkan menurut survei yang dilakukan oleh Uptime Institute, sebuah badan penelitian industri, *Data Center* memiliki tingkatan dari *Tier* I hingga *Tier* IV, di mana pada *Tier* IV menawarkan jaminan *uptime* sebesar 99,995%. Dengan adanya celah sebesar 0,005%, dapat mengakibatkan terhentinya suatu operasi organisasi atau yang disebut sebagai *downtime* jika hal tersebut terjadi pada saat organisasi sedang membutuhkan data secara cepat. Karena sedikitnya bukti empiris yang membahas jaminan dari perspektif penyedia *Data Center*, penelitian ini bertujuan untuk memberikan sebuah gambaran bagaimana dampak dari adanya *downtime* tersebut dan bagaimana penyedia *Data Center* mengatasi dampak tersebut. Oleh karena itu, penelitian ini penting untuk dilakukan karena dengan berfokus pada penyedia *Data Center*, penelitian ini dapat memberikan informasi mengenai dampak dari celah yang terjadi dan juga memberikan gambaran apa saja yang akan dilakukan oleh penyedia *Data Center* untuk mengatasi hal tersebut.

Literature sebelumnya menunjukkan bahwa celah dari *Data Center* tersebut bisa mengakibatkan *Data Center downtime* yang terjadi karena adanya masalah jaringan karena tekanan dari sistem (Hao et al., 2019) dan juga serangan siber seperti *ransomware* atau DDoS (Anwar & Malik, 2014; Santalo et al., 2022). Hal tersebut dapat mengakibatkan gangguan kontrol *Data Center* karena serangan-serangan tersebut dapat menyebabkan panasnya perangkat sehingga menyebabkan memperpanjang waktu migrasi dan *downtime* (Hao et al., 2019). Hal ini terbukti berdasarkan survei yang dilakukan oleh Uptime Institute yang menjelaskan bahwa sebanyak 56% organisasi yang menggunakan *Data Center* pihak ketiga mengalami gangguan layanan TI yang disebabkan oleh penyedianya. Salah satu kasus besar yang pernah terjadi adalah serangan siber yang dilancarkan pada salah satu penyedia *Data Center* terbesar di dunia, yaitu Equinix. Berdasarkan *website* resminya, serangan ini mulai terjadi pada 9 September 2020 dan berakhir pada 28 Oktober 2020 (Equinix, 2023). Oleh karena itu, kami berasumsi bahwa meskipun keamanan menjadi kepentingan utama bagi penyedia *Data Center* seperti Equinix, organisasi tetap dapat menjadi korban dari serangan siber seperti *ransomware*.

Untuk menyelidiki dampak dari celah 0,005% *Data Center* serta bagaimana mereka mengatasi hal tersebut, kami memusatkan perhatian pada pengumpulan artikel-artikel melalui sumber utama Scopus dengan kata kunci utama "*Data Center*". Akan tetapi, kami juga menggunakan kata kunci yang serupa, misalnya "*Cloud*", "*Database* Pihak Ketiga", dan lain sebagainya. Alasan kami menggunakan Scopus karena merupakan sumber data penelitian terkemuka dan memberikan akses ke banyak artikel dan konferensi ilmiah dengan tingkat kualitas yang tinggi. Secara khusus, kami juga memfokuskan lagi untuk menggunakan artikel yang terindeks di peringkat Q1 hingga Q3 untuk menekankan kredibilitas dan kontribusi substansial terhadap penelitian kami. Melalui proses *screening* yang teliti, kami menyaring artikel sehingga hanya memasukkan yang paling relevan dan berpotensi memberikan wawasan mendalam terkait dengan pusat data. Terakhir, kami me*review* artikel-artikel pilihan kami untuk menunjukkan temuan dari penelitian ini.

Kami menemukan bahwa celah 0,005% pada *Data Center Tier* IV merupakan *downtime* selama 30 menit per tahunnya, di mana hal ini dapat diakibatkan banyak hal seperti panasnya sistem hingga serangan siber dari luar (Anwar & Malik, 2014; Hao et al., 2019; Santalo et al., 2022). Sedangkan dampak yang diberikan adalah munculnya biaya yang harus dibayarkan karena *downtime* hingga dapat menyebabkan terhentinya operasional organisasi (Santos et al., 2017; Wiboonrat, 2009). Akan tetapi, kami berpendapat bahwa dengan terjadinya *downtime*, dapat menyebabkan sistem organisasi akan lebih rentan menjadi korban dari serangan siber. Oleh karena itu, dengan berfokus pada penyedia *Data Center*, hasil kami dapat menjadi kontribusi yang baik untuk menangani risiko-risiko tersebut bagi penyedia *Data Center* yang ada.

Penelitian ini berkontribusi untuk memberikan gambaran bagi penyedia *Data Center* yang berada di Indonesia untuk melakukan hal yang sama, guna meningkatkan pelayanan mereka dan keamanan bagi pelanggannya. Selain itu, dengan meningkatnya pelayanan yang diberikan, tingkatan penyedia *Data Center* Indonesia juga dapat meningkat ke *Tier* III, bahkan hingga *Tier* IV. Oleh karena itu, penyedia *Data Center* Indonesia juga dapat bersaing dengan penyedia *Data Center* secara global atas layanan yang diberikan. Selain itu, penelitian ini juga dapat memberikan wawasan yang berharga dalam meningkatkan pemahaman kita tentang pengelolaan *Data Center* dan menginspirasi upaya perbaikan yang lebih efektif di masa depan, di mana dengan menyajikan artikel-acuan terkait, penelitian ini dapat menjadi landasan untuk penelitian mendatang yang mengeksplorasi celah-celah yang ada dalam pengelolaan *Data Center*, khususnya dalam penanganan kegagalan yang diakibatkan oleh *downtime*. Penelitian ini berfokus pada penyedia layanan *Data Center*. Dengan demikian, penelitian ini diharapkan dapat memberikan pandangan holistik tentang tantangan dan solusi yang dapat diterapkan dalam meminimalkan risiko kegagalan yang berpotensi merugikan.

Sisa mini *research* ini dilanjutkan dengan menjelaskan *research background* dengan menjelaskan apa itu *Data Center*, yang kemudian dilanjutkan dengan bagian metodologi penelitian seperti apa yang kami gunakan dalam membuat mini *research* ini. Selanjutnya, kami menjelaskan hasil temuan kami, dan diakhiri dengan pengambilan kesimpulan dari hasil-hasil yang telah ditemukan sebelumnya.

2. TNJAUAN PUSTAKA

2.1 Data Center

Taylor (2022), mendefinisikan *Data Center* sebagai sebuah infrastruktur yang terdiri dari sumber daya komputasi dan penyimpanan yang dapat memungkinkan distribusi aplikasi perangkat lunak dan data secara bersama, serta menjadi krusial dalam mendukung operasional harian perusahaan dan kebutuhan konsumen. Sedangkan menurut Hernandez et al., (2018), *Data Center* biasanya merupakan ruang fisik tempat informasi berada diproses, disimpan, ditransmisikan, dipertukarkan, dan dikelola secara terpusat.

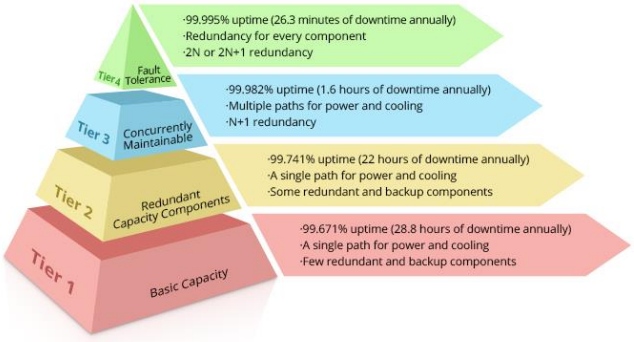
Tujuan dari penggunaan *Data Center* tergantung berdasarkan organisasi atau industri seperti apa yang akan menggunakannya, seperti institusi pendidikan, organisasi berorientasi laba, atau organisasi pemerintahan. Menurut Ayoub et al., (2019) serta Hao et al., (2019) tujuan dari penggunaan *Data Center* yang utama adalah memberikan dukungan operasional kritis dan menyediakan layanan digital dengan menyimpan dan mengelola infrastruktur IT. Selain itu, *Data Center* juga digunakan untuk memaksimalkan penggunaan sumber daya yang tersedia untuk meningkatkan ketangguhan suatu proses bisnis sebuah organisasi (Bari et al., 2014; Shi et al., 2022; Varasteh & Goudarzi, 2015).

2.2 Tier Classification

Menurut Whitehead et al., (2014) memberikan tingkatan sebuah akses berkelanjutan terhadap data pada *Data Center* dapat dilihat dari *Reliability* yang melihat probabilitas beroperasinya suatu *Data Center* tanpa kegagalan pada suatu periode waktu tertentu, *Availability* yang melihat rata-rata waktu *Data Center* beroperasi seperti rencana awal, tanpa waktu tidak aktif, serta *Redundancy* yang melihat topologi infrastruktur pendukung yang memastikan tetap tersedianya *Data Center* saat terjadi kegagalan. Untuk mengukur redundansi dari sebuah *Data Center*, Whitehead et al., (2014) yang didasarkan dari Uptime Institute, memberikan bahasa umum yang dapat digunakan yaitu klasifikasi *Tier*, dari *Tier* I hingga IV. Klasifikasi *Tier* digunakan untuk mengukur kemampuan redundansi suatu *Data Center* untuk tetap menjalankan fungsinya apabila

terjadi masalah. Penjelasan singkat dari klasifikasi *Tier* tersebut dapat dilihat dari Gambar 1.

Gambar 1. Klasifikasi *Tier* redundansi



- *Tier* I : Tingkatan paling dasar yang tidak menawarkan jaminan redundansi untuk sistem kritis apa pun. Pada *Tier* ini, *Data Center* minimal harus dilengkapi dengan fitur seperti UPS, ruang khusus untuk sistem TI, peralatan pendingin, dan juga mesin generator. *Tier* I memiliki kerentanan terhadap berbagai gangguan, baik yang direncanakan maupun tidak, karena hanya menawarkan jaminan *uptime* minimal 99,671%, setara dengan *downtime* maksimal 28,8 jam per tahunnya. Penyedia *Data Center* yang memiliki tingkat redundansi *Tier* I, memiliki harga yang terjangkau, sehingga cocok untuk usaha kecil yang tidak memiliki persyaratan rumit atau operasi sepanjang waktu.

- *Tier* II : Tingkatan yang dibangun berdasarkan persyaratan *Tier* I dengan penambahan beberapa komponen redundansi untuk meningkatkan keandalan. *Tier* ini memberikan jaminan *uptime* sebesar 99,741%, setara dengan *downtime* maksimal 22 jam per tahun. Karena terpacu dengan *Tier* I, *Tier* ini memberikan fitur-fitur yang mirip dengan *Tier* I, namun sedikit lebih tinggi.

- *Tier* III : Tingkatan yang menghadirkan tingkat keandalan yang lebih tinggi dengan menyertakan redundansi N+1 yang berarti arsitektur *Data Center* memiliki kapasitas untuk mendukung beban TI penuh (N) dan menyertakan satu komponen tambahan (+1) sebagai cadangan, sehingga kinerja sistem tidak terpengaruh apabila salah satu komponen mengalami kegagalan. Oleh karena itu, dalam konteks pemeliharaan, hanya akan mematikan salah satu komponen atau jalur distribusi tertentu sehingga tidak mengganggu proses TI secara keseluruhan. *Tier* ini memberikan jaminan *uptime* sebesar 99,982%, setara dengan *downtime* maksimal 1,6 jam per tahun.

- *Tier* IV : Tingkatan tertinggi yang memberikan arsitektur yang sepenuhnya independen dengan duplikasi setiap komponen utama dan menyediakan beberapa jalur distribusi berkapasitas dua kali lipat atau

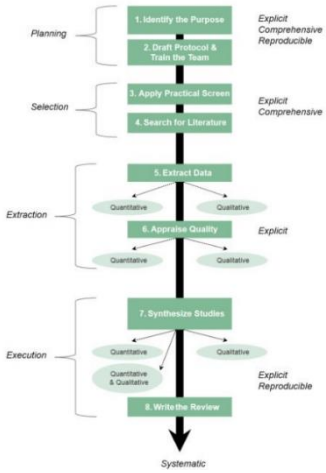
dapat dispesifikasikan 2N atau 2N+1, sehingga *Data Center* akan lebih memiliki toleransi kesalahan yang tinggi terhadap pemeliharaan rutin, pemadaman tak terduga, dan kegagalan peralatan. Ketika terjadi gangguan, sistem redundan secara otomatis mengambil alih untuk menjaga operasi tetap berjalan, memberikan tingkat ketersediaan yang sangat tinggi. *Tier* ini memberikan jaminan *uptime* sebesar 99,995%, setara dengan *downtime* maksimal 30 menit per tahun.

Menurut Edge DC (2023) pada *website*-nya, menjelaskan bahwa *Data Center* memiliki lima jenis utama, yaitu: pertama *Enterprise Data Center*, di mana jenis ini merupakan *Data Center* yang digunakan, disediakan, dioperasikan, dan dirawat secara pribadi oleh organisasi. Jenis ini banyak digunakan oleh organisasi-organisasi besar seperti Google, di mana dijelaskan pada *website* resmi mereka, mereka memberikan fasilitas. Kedua adalah *Cloud Data Center*, di mana penyedia *Data Center* menyediakan layanan sebuah *cloud* yang dapat diakses oleh pengguna menggunakan jaringan internet dari mana saja dan kapan saja. Ketiga *Edge Data Center*, di mana *Data Center* ditempatkan di dekat lokasi pengguna agar akses data lebih cepat. Keempat *Micro Data Center*, di mana organisasi menempatkan *Data Center* di lokasi dengan fasilitas kecil.

Terakhir, jenis *Data Center* yang banyak digunakan oleh Penyedia *Data Center*, yaitu *Colocation Data Center*, di mana penyedia *Data Center* memberikan layanan ruang fisik yang disewakan kepada organisasi untuk menempatkan *Data Center* mereka. Salah satu contoh penyedia *Data Center* yang menggunakan *Colocation Data Center* adalah Equinix. Berdasarkan dari *website* resminya, mereka menyediakan beberapa opsi seperti suite atau kabinet server yang terinterkoneksi secara pribadi, lokal, dan virtual ke *cloud* atau layanan. Mereka memberikan jaminan kabinet server yang aman karena menggunakan ruangan fisik pribadi yang tertutup

3. METODE PENELITIAN

Metodologi penelitian menggambarkan tahapan yang akan dilakukan dalam penelitian. Dalam penelitian ini penulis menerapkan metode *systematic literature review* dengan memanfaatkan model 8 panduan yang telah direkomendasikan oleh Okoli & Schabram (2015). Rincian langkah-langkah dalam melaksanakan proses *review* dapat diidentifikasi melalui ilustrasi yang disajikan dalam gambar.



Gambar 2. Skema Penulisan Literature Review

Langkah 1: *Purpose;* Tujuan dari penelitian ini adalah men-*sithesis* penelitian yang sudah ada untuk mendapatkan pemahaman yang lebih mendalam tentang celah yang memungkinkan *Data Center* untuk gagal dan bagaimana penyedia layanan dapat mengatasi kegagalan tersebut.

Langkah 2: *Protocol*; Langkah ini mengharuskan peninjau agar secara tegas menentukan studi-studi yang akan dimasukkan dalam tinjauan dan studi mana yang akan dikecualikan tanpa perlu pemeriksaan lebih lanjut. Untuk lebih lanjut *protocol* akan dijelaskan pada tabel 1 berikut:

Tabel 1. Kriteria Inklusi dan Eksklusi

Kriteria	**Kriteria Kelayakan**
Inklusi	Peer-*review* dan relevan dengan pertanyaan penelitian Artikel *quartil* 1-3 Tanpa batasan jangka waktu Artikel berbahasa inggris
Eksklusi	Artikel yang bukan berbahasa inggris Artikel di *quartil* 4-5 ataupun tanpa penilaian Artikel *literature review* teks penuh artikel yang tidak bisa diakses

Langkah 3: *Literature Search*, Langkah ini meliputi proses pencarian dan pemilihan awal artikel, seperti kata kunci, basis data yang digunakan, dan kriteria kelayakan. Pencarian literatur dimulai pada tanggal 23 November 2023 dengan basis data utama, yaitu Scopus. Pencarian tidak terbatas dengan tanggal dikarenakan pencarian terus dilakukan karena penulis terus mencari informasi yang terkait dan relevan.. Sementara itu, kata kunci diidentifikasi dari judul, abstrak, dan kata kunci artikel yang relevan. Proses pencarian awal ditemukan sebanyak 72 artikel, namun ditemukan 24 artikel yang tidak dapat diakses, serta 21 artikel yang masuk kategori *quartil*e 4 - *quartil*e 5 dan yang tidak memiliki penilaian. Oleh karena itu, setelah proses pengurangan maka penulis menggunakan 27 artikel seperti yang dijelaskan dalam Tabel 2 berikut ini:

Tabel 2. Proses Pencarian dan Seleksi

Pencarian Kata Kunci	***Database***	**Kriteria Penghapusan**	**Jumlah Artikel**
"*Data Center*" AND "*downtime*" AND "*impact*" "*Data Center*" AND "*downtime*" AND "*ensure*"	Scopus	Tahap Publikasi : Final Tahun Publikasi : Tanpa batasan jangka waktu Tipe dokumen : Jurnal artikel Artikel konferensi Bahasa : Inggris	72
Total			72
Dikurangi artikel yang tidak dapat diakses			-24
Dikurangi artikel yang masuk kategori *Quartil*e 4-5			-21
Total artikel yang diambil(diunduh untuk dibaca)			**27**

Langkah 4: *Pratical Screen;* Langkah selanjutnya melakukan seleksi praktis dengan membaca dengan teliti abstrak, teori, metode, dan hasil penelitian dari setiap artikel yang diperoleh melalui langkah pencarian literatur

Langkah 5: *Quality Screening;* Dalam langkah ini, penulis menyaring dengan hanya menggunakan artikel-artikel yang berada pada rentan kelompok *quartil* 1 sampai dengan *quartil* 3. Sekaligus, mengecualikan penelitian yang hanya menggunakan *literature review* dalam penelitiannya.

Langkah 6: *Data extraction*; Langkah ini dilakukan dengan mengekstrak data dari setiap artikel dalam bentuk *excel* yang digunakan untuk merekam data secara akurat. Proses ekstraksi data dan persiapan data yang dilakukan untuk melakukan identifikasi celah yang terdapat pada *Data Center* dan bagaimana penyedia layanan mengatasinya untuk memberikan hasil yang sedang diteliti.

Langkah 7: *Data synthesis*; Analisis data yang sudah di ekstrak dilakukan dengan mengklasifikasi tema-tema yang berbeda . Sintesis data bertujuan untuk membahas tema luas tentang *Data Center*, seperti tingkatannya, penyebab *downtime*, dampak yang terjadi, dan cara mengatasinya.

Langkah 8: *Writing the review;* Laporan peninjauan dilakukan dengan diskusi yang mendalam antara para penulis, yang kemudian bersama-sama merancang konsepnya dengan sepakat mengenai ide penulisan dan tata letak yang akan digunakan.

4. HASIL DAN PEMBAHASAN

4.1 Cause and Effects of Downtime

Downtime dapat terjadi karena berbagai faktor. Berdasarkan Hao et.al (2019) menunjukkan bahwa tekanan sistem dan masalah jaringan dapat signifikan memperpanjang waktu migrasi dan *downtime*. Dalam penelitian Santalo et.al (2022) menunjukkan bahwa serangan siber, khususnya serangan *ransomware*, dapat menyebabkan *downtime* yang signifikan dalam sistem rumah sakit, terutama mempengaruhi departemen seperti farmasi yang mengandalkan proses otomatis. Berdasarkan Anwar dan Malik (2014), menjelaskan bahwa serangan seperti DDoS dapat mengganggu kontrol *Data Center* karena dapat menyebabkan panasnya perangkat. Adapun, Uptime Institute melakukan studi yang menemukan bahwa 56% organisasi yang menggunakan *Data Center* pihak ketiga pernah mengalami gangguan layanan TI tingkat sedang atau serius dalam tiga tahun terakhir yang disebabkan oleh penyedianya.

Berdasarkan dari *website* resmi Equinix (*www.equinix.com*), di mana sebagai salah satu organisasi penyedia *Data Center* terbesar di dunia, mendeteksi bahwa pada 9 September 2020, organisasi terkena serangan *ransomware* di sejumlah sistem internalnya. Baiknya adalah serangan tersebut tidak berdampak pada kemampuan organisasi untuk memberikan dukungan kepada pelanggannya karena tidak berdampak pada layanan-layanan yang ditawarkan seperti layanan terkelola. Meskipun serangan *ransomware* tersebut dapat teratasi pada 28 Oktober 2020, Equinix juga terancam mengeluarkan tebusan sebesar $4,5 juta supaya data yang terserang tidak bocor ke publik (Adler, 2020). Kasus tersebut menyatakan bahwa, meskipun keamanan menjadi kepentingan utama bagi penyedia *Data Center* seperti Equinix, organisasi tetap dapat menjadi korban dari serangan siber seperti *ransomware*.

Uptime dan *downtime* dari *Data Center* tidak dapat dipisahkan, karena meskipun *Data Center* memiliki layanan dengan tingkatan paling tinggi pun masih memiliki risiko *downtime*. Seperti yang dijelaskan, bahwa *Tier* IV yang merupakan tingkatan paling tinggi, masih ada kemungkinan *downtime* sebesar 0,005%. *Downtime* dapat mengakibatkan organisasi pengguna *Data Center* menjadi kewalahan, terutama jika *downtime* terjadi pada jam-jam sibuk atau saat pengguna sedang sangat bergantung pada data dan layanan yang telah disimpan di *Data Center*.

Berdasarkan survei Information Technology Industry Council (ITIC), bahwa 40% perusahaan mengatakan biaya *downtime* selama satu jam dapat berkisar antara satu hingga lebih dari lima juta dollar, tidak termasuk biaya hukum, denda, dan penalti. Jumlah ini dapat meningkat hingga jutaan per menit jika pemadaman mengganggu transaksi bisnis besar atau terjadi pada jam sibuk. Di mana menurut Wiboonrat (2009) *Data Center* yang mengalami *downtime* dapat merugikan hingga lebih dari satu juta dolar per jam bagi organisasi pengguna terutama di utilitas publik dan/atau rumah sakit yang membutuhkan ketersediaan data selama 24x7 jam. Selain itu, layanan yang berhubungan dengan saling ketergantungan *database* satu dengan yang lain akan sangat

terganggu apabila salah satu *database* sedang mengalami *downtime* (Santos et al., 2017). *Downtime* juga dapat menjadi risiko yang cukup besar, karena menjadi rentan data hilang dan juga dapat menjadi korban serangan *ransomware*. Di mana risiko serangan siber juga dapat terjadi karena pada saat *downtime* menyebabkan layanan terganggu bahkan tidak dapat diakses, sehingga para penyerang dari luar dapat memanfaatkan kelemahan tersebut untuk melancarkan serangan sibernya.

4.2 Downtime Prevention

Downtime dapat terjadi sewaktu-waktu, saat tidak digunakan atau bahkan saat digunakan. Berdasarkan hasil riset sebelumnya, dijelaskan strategi yang digunakan oleh organisasi atau penyedia Pusat Data untuk mencegah masalah saat *downtime* terjadi, bahkan mengupayakan agar dapat dikurangi sebanyak mungkin sebelum terjadi. Salah satu metode untuk mencegah *downtime* adalah dengan mengoptimalkan atau meningkatkan efisiensi penggunaan *multi-server* atau konektivitas. (Matko & Brezovec, 2018; Rauen et al., 2017; Varasteh & Goudarzi, 2015). Karena *downtime* dapat meningkatkan risiko terkenanya serangan siber seperti DDoS (Varasteh & Goudarzi, 2015), penting untuk selalu memantau komponen-komponen infrastruktur yang terintegrasi agar dapat mudah terpantau dan dikelola dari pusatnya, sehingga dapat menelusuri masalah dari sumbernya (Matko & Brezovec, 2018; Rauen et al., 2017). Hal ini sejalan dengan penelitian yang dilakukan oleh Chang (2015) dan Gathecha et al., (2023), di mana menjelaskan pentingnya koordinasi antar pihak pada konfigurasi sistem untuk migrasi data organisasi ke *Data Center*.

Selain itu, organisasi dapat menerapkan manajemen deteksi (Nagashree et al., 2018) untuk meningkatkan keamanan saat terjadi *downtime* (Anwar & Malik, 2014) dan mengurangi waktu terjadinya *downtime* (Frolov, 2020). Dengan penerapan sistem deteksi dan manajemen risiko dini (ERDMS), organisasi mendeteksi potensi risiko (Nagashree et al., 2018) berdasarkan urutan operasi yang dilakukan pada sistem. Ini menguraikan kumpulan log untuk mempelajari aturan deteksi risiko dan merekomendasikan solusi untuk memitigasi atau menghilangkan risiko yang teridentifikasi, yang bertujuan untuk mengurangi waktu terjadinya *downtime* (Frolov, 2020) serta meningkatkan keamanan agar terhindar dari kerusakan fisik pada server dan perangkat keras yang dapat menyebabkan kerusakan *Data Center* (Anwar & Malik, 2014).

Menurut Wiboonrat (2009), menjelaskan bahwa dengan konsep meningkatkan MTTF atau menurunkan MTTR berkontribusi untuk meningkatkan ketersediaan sistem sehingga mengurangi waktu *downtime*. Sejalan dengan penelitian Lima et al., (2020), yang memberikan pendekatan atau model baru dengan memasangkan model cerdas pada setiap *Data Center* dalam rangkaian yang terdistribusi dan membantu administrator memprediksi waktu transfer data yang dibutuhkan sehingga meminimalkan waktu yang digunakan pada ketersediaan sistemnya. Begitu juga dengan Pattanaik, B.C. et, al. (2023), di mana mereka memperkenalkan algoritma komprehensif yang menggabungkan teori pemodelan kesalahan reaktif dan proaktif untuk meningkatkan toleransi kesalahan dengan memprediksi cacat dan mengalokasikan sumber daya secara efisien, sehingga meminimalkan gangguan layanan dan memaksimalkan penggunaan sumber daya. Ini secara efektif mengurangi waktu tidak aktif layanan, memastikan keandalan aplikasi, dan menjaga kinerja optimal melalui migrasi mesin virtual dinamis berdasarkan prediksi cacat, yang membantu dalam alokasi sumber daya yang efisien, penyeimbangan beban, dan meningkatkan ketangguhan sistem.

4.3 Downtime Overcome and Recovery

Dalam menghadapi permasalahan *downtime* yang sudah atau sedang terjadi, penting untuk memiliki strategi yang efektif dalam mengatasi dan memulihkan sistem. Setelah terjadi *downtime*, langkah-langkah tanggap dan solutif diterapkan untuk mengidentifikasi sumber permasalahan, mengisolasi kerusakan, dan memulihkan fungsi sistem dengan secepat mungkin. Dengan adanya strategi *downtime overcome and recovery* yang terintegrasi, perusahaan dapat meminimalkan dampak negatif dari kegagalan dan memastikan ketersediaan layanan *Data Center* yang optimal

Berdasarkan artikel Ayoub et al., (2019) dan Le (2020), tujuan dari migrasi VM adalah meminimalkan *downtime*, memungkinkan administrator sistem untuk melakukan pemeliharaan perangkat keras atau perangkat lunak pada *host* tanpa harus mematikan mesin virtual. Ini dapat meningkatkan keterasediaan sistem.

Untuk mengatasi *downtime* selama migrasi VM di *Data Center*, Najm & Tamarapalli (2022), merumuskan masalah optimasi untuk meminimalkan *Total Cost of Operation* (TCO) penyedia *cloud* serta waktu migrasi. Peneliti mengusulkan algoritma migrasi VM yang efisien yang mempertimbangkan karakteristik VM, *bandwidth*, dan biaya transfer data antar *Data Center* untuk mengurangi TCO dan waktu migrasi, termasuk *downtime*. Hasil eksperimen menunjukkan bahwa algoritma yang diusulkan mengurangi TCO hingga 48% serta mengurangi waktu migrasi, *downtime*, dan jumlah migrasi. Sedangkan Cao et al., (2018) memperkenalkan *Hybrid Multi-Goal Optimization Weight Method* (HMGOWM), mekanisme pengambilan keputusan hibrida untuk otomatisasi migrasi VM, yang dirancang untuk mengurangi *downtime* yang dialami oleh pengguna. HMGOWM mengutamakan keseimbangan antara waktu pemulihan layanan dan pengalaman *downtime* pengguna. Dengan memperluas model biaya kinerja migrasi VM, HMGOWM berhasil mengurangi *downtime* pengguna secara signifikan. Pendekatan ini berfokus pada meminimalkan dampak dari gangguan akses dan mengoptimalkan waktu pemulihan layanan.

Menurut Schiller et al., (2022), pendekatan yang digunakan dengan melakukan migrasi BBU secara langsung untuk mempertahankan kontinuitas jaringan dengan *downtime* yang relatif rendah, yang mengungkapkan bahwa migrasi BBU di jaringan LoRaWAN saat ini dapat dilakukan dengan *downtime* yang rendah. Adapun Bhardwaj & Rama Krishna (2022) mengenalkan teknik LXD/CR, sebuah metode berbasis kontainer untuk mengurangi *downtime* dalam migrasi mesin virtual di pusat data *cloud*. Teknik ini memanfaatkan kontainer yang lebih ringan daripada VM tradisional dan memakai *checkpoint/restore* untuk memindahkan kontainer yang sedang berjalan. Ini menghasilkan pengurangan waktu migrasi, data yang ditransfer, dan *downtime*. LXD/CR meningkatkan efisiensi dan mengurangi beban pada CPU dan memori selama migrasi, sangat bermanfaat dalam kondisi *bandwidth* rendah dan meningkatkan kinerja infrastruktur *cloud*.

5. KESIMPULAN

Berdasarkan hasil yang telah kami temukan sebelumnya, *Data Center* merupakan infrastruktur penting yang kini banyak digunakan oleh organisasi-organisasi kecil maupun besar. Sedangkan penyedia *Data Center* merupakan organisasi yang menyediakan fasilitas *Data Center* berupa ruang fisik, yang bertujuan untuk meminimalisasikan biaya keluaran pengguna akhir terkait dengan pengadaan ruang fisik khusus *Data Center*. Oleh karena itu, mengelola risiko *downtime* di *Data Center* merupakan hal penting yang perlu disoroti.

Salah satu strategi kunci yang disoroti adalah tingkat redundansi, di mana sistem harus memiliki *backup* dalam hal terjadi kesalahan, termasuk redundansi daya, pendinginan, dan

konektivitas jaringan. Selain itu, pemeliharaan preventif rutin juga penting untuk memastikan semua peralatan beroperasi dengan optimal dan mencegah kegagalan yang tak terduga. Pengawasan dan pemantauan 24/7 juga diperlukan untuk mendeteksi dan menangani masalah sebelum mereka berdampak pada operasional. Selain itu, pelatihan karyawan dan prosedur tanggap darurat yang kuat juga menjadi strategi penting. Karyawan harus dilatih untuk mengenali dan merespons cepat terhadap isu yang mungkin menyebabkan *downtime*. *Data Center* juga harus memiliki prosedur tanggap darurat yang terdefinisi dengan baik untuk menangani berbagai skenario, termasuk bencana alam dan serangan siber.

Dijelaskan juga strategi optimasi *multi-server* dan konektivitas untuk peningkatan efisiensi, manajemen deteksi risiko dan sistem deteksi risiko dini (ERDMS) untuk mendeteksi potensi masalah lebih awal, serta peningkatan *Mean Time To Failure* (MTTF) dan pengurangan *Mean Time To Repair* (MTTR) untuk meningkatkan ketersediaan sistem. Selain itu, penggunaan model prediksi dan alokasi sumber daya yang efisien membantu mengurangi *downtime*, serta strategi pemulihan dan migrasi *Virtual Machine* (VM) yang efektif, untuk meminimalkan *Total Cost of Operation* (TCO) dan waktu migrasi setelah *downtime*.

Dalam konteks *Data Center* Indonesia, mereka masih menghadapi masalah terkait redundansi dan ketahanan terhadap gangguan seperti pemadaman listrik atau bencana alam, yang dapat mengakibatkan gangguan layanan dan potensi kehilangan data. Oleh karena itu, penting bagi penyedia *Data Center* di Indonesia untuk mengimplementasikan strategi dan infrastruktur yang meminimalisir risiko *downtime*, serta memiliki rencana pemulihan yang efektif. Ini akan memastikan bahwa *Data Center* di Indonesia dapat memberikan layanan yang andal dan aman, yang penting untuk mendukung pertumbuhan ekonomi digital di negara tersebut. Sehingga penyedia *Data Center* di Indonesia dapat meningkatkan layanan dan keamanan mereka dan memungkinkan mereka dapat berpotensi meningkatkan layanan redundansinya menjadi *Tier* III atau IV, yang menjadikannya mampu bersaing secara global.

Selain itu, penyedia *Data Center* juga dapat memperhatikan kebijakan dan regulasi terkait keamanan data dan privasi, serta tantangan mengenai investasi yang diperlukan untuk membangun dan memelihara *Data Center* canggih, terutama bagi perusahaan kecil dan menengah. Untuk mengatasi tantangan ini, perlu adanya kerja sama antara pemerintah dan pemangku kepentingan guna memastikan keberlanjutan dan keandalan *Data Center* di era digital saat ini serta menjaga infrastruktur yang mendukung pertumbuhan ekonomi dan inovasi di Indonesia.

Dalam penyusunan penelitian ini, kami mengalami beberapa keterbatasan seperti sedikitnya artikel terdahulu yang dapat kami jadikan acuan untuk menyusun penelitian ini. Selain itu, karena terbatasnya waktu dan artikel terdahulu, kami belum dapat memberikan hasil secara spesifik mengenai faktor dan dampak dari *downtime* sehingga kami juga belum dapat memberikan hasil secara spesifik mengenai apa saja yang dapat dilakukan penyedia *Data Center* mengatasi *downtime*.

DAFTAR PUSTAKA

Anwar, Z., & Malik, A. W. (2014). Can a DDoS attack meltdown my data center? A simulation study and defense strategies. *IEEE Communications Letters*, *18*(7), 1175–1178. https://doi.org/10.1109/LCOMM.2014.2328587

Ayoub, O., Huamani, O., Musumeci, F., & Tornatore, M. (2019). Efficient online virtual machines migration for alert-based disaster resilience. *2019 15th International Conference on the Design of Reliable Communication Networks (DRCN)*, 146–153. https://doi.org/10.1109/DRCN.2019.8713760

Bari, M. F., Zhani, M. F., Zhang, Q., Ahmed, R., & Boutaba, R. (2014). CQNCR: Optimal VM migration planning in cloud data centers. *2014 IFIP Networking Conference*, 1–9. https://doi.org/10.1109/IFIPNetworking.2014.6857120

Bhardwaj, A., & Rama Krishna, C. (2022). A container-based technique to improve virtual machine migration in

cloud computing. *IETE Journal of Research*, *68*(1), 401–416. https://doi.org/10.1080/03772063.2019.1605848

Cao, R., Tang, Z., Li, K., & Li, K. (2018). HMGOWM: A hybrid decision mechanism for automating migration of virtual machines. *IEEE Transactions on Services Computing*, *14*(5), 1397–1410. https://doi.org/10.1109/TSC.2018.2873694

Chang, V. (2015). Towards a big data system disaster recovery in a private cloud. *Ad Hoc Networks*, *35*, 65–82. https://doi.org/10.1016/j.adhoc.2015.07.012

Edge DC. (2023). *Pengertian Data Center, Beserta Fungsi dan Jenisnya. A Digital Edge Company*. https://edge.id/id/artikel/pengertian-data-center-beserta-fungsi-dan-jenisnya/

Equinix. (2023). *Cages and Cabinets Interconnection-Ready Colocation Options to House, Power and Protect your IT Infrastructure*. https://www.equinix.com/products/data-center-services/colocation/cages-cabinets

Frolov, V. V. (2020). Analysis Of Approaches Providing Security Of Cloud Sevices. *Radioelectronic and Computer Systems*, *1*, 70–82. https://doi.org/10.32620/reks.2020.1.07

Gathecha, G., Ombiro, O., Shelden, K., Stake, A., Murugami, M., Mungai, E., Odhiambo, G., Maree, E., Muthusamy, R., & Marimuthu, M. (2023). Integrating digital solutions into national health data systems through public–private collaboration: An early experience of the SPICE platform in Kenya. *Digital Health*, *9*, 20552076231203936. https://doi.org/10.1177/20552076231203937

Hao, J., Ye, K., & Xu, C.-Z. (2019). Live migration of virtual machines in OpenStack: A perspective from reliability evaluation. *Cloud Computing–CLOUD 2019: 12th International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings 12*, 99–113. https://doi.org/10.1007/978-3-030-23502-4_8

Hernandez, L., Jimenez, G., & Marchena, P. (2018). Energy Efficiency Metrics of University Data Centers. *Knowl. Eng. Data Sci.*, *1*(2), 64–73. https://doi.org/10.17977/um018v1i22018p64-73

Le, T. (2020). A survey of live virtual machine migration techniques. *Computer Science Review*, *38*, 100304. https://doi.org/10.1016/j.cosrev.2020.100304

Lima, P. A., Neto, A. S. B., & Maciel, P. (2020). Data centers' services restoration based on the decision-making of distributed agents. *Telecommunication Systems*, *74*, 367–378. https://doi.org/10.1007/s11235-020-00660-2

Matko, V., & Brezovec, B. (2018). Improved data center energy efficiency and availability with multilayer node event processing. *Energies*, *11*(9), 2478. https://doi.org/10.3390/en11092478

Nagashree, N., Tejasvi, R., & Swathi, K. C. (2018). An early risk detection and management system for the cloud with log parser. *Computers in Industry*, *97*, 24–33. https://doi.org/10.1016/j.compind.2018.01.018

Najm, M., & Tamarapalli, V. (2022). Towards cost-aware VM migration to maximize the profit in federated clouds. *Future Generation Computer Systems*, *134*, 53–65. https://doi.org/10.1016/j.future.2022.03.020

Okoli, C., & Schabram, K. (2015). *A guide to conducting a systematic literature review of information systems research*. https://doi.org/10.2139/ssrn.1954824

Rauen, Z. I., Kantarci, B., & Mouftah, H. T. (2017). Resiliency versus energy sustainability in optical inter-datacenter networks. *Optical Switching and Networking*, *23*, 144–155. https://doi.org/10.1016/j.osn.2016.06.003

Santalo, O., Perez, G., Lorich, C., Greenberg, M., Hernandez, J. M., Bohorquez, R., & Zhang, B. (2022). Defining key pharmacist and technician roles in response to a hospital downtime or cyberattack. *Journal of the American Pharmacists Association*, *62*(5), 1518–1523. https://doi.org/10.1016/j.japh.2022.03.027

Santos, G. L., Endo, P. T., Gonçalves, G., Rosendo, D., Gomes, D., Kelner, J., Sadok, D., & Mahloo, M. (2017). Analyzing the it subsystem failure impact on availability of cloud services. *2017 IEEE Symposium on Computers and Communications (ISCC)*, 717–723. https://doi.org/10.1109/ISCC.2017.8024612

Schiller, E., Ajayi, J., Weber, S., Braun, T., & Stiller, B. (2022). Toward a live BBU container migration in wireless networks. *IEEE Open Journal of the Communications Society*, *3*, 301–321. https://doi.org/10.1109/OJCOMS.2022.3149965

Shi, B., Shen, H., Dong, B., & Zheng, Q. (2022). Memory/disk operation aware lightweight VM live migration. *IEEE/ACM Transactions on Networking*, *30*(4), 1895–1910. https://doi.org/10.1109/TNET.2022.3155935

Taylor, P. (2022). *Data Centers - Statistics & Facts. Statista*. https://www.statista.com/topics/6165/data-centers/#topicOverview

Varasteh, A., & Goudarzi, M. (2015). Server consolidation techniques in virtualized data centers: A survey. *IEEE Systems Journal*, *11*(2), 772–783. https://doi.org/10.1109/JSYST.2015.2458273

Whitehead, B., Andrews, D., Shah, A., & Maidment, G. (2014). Assessing the environmental impact of data centres part 1: Background, energy use and metrics. *Building and Environment*, *82*, 151–159. https://doi.org/10.1016/j.buildenv.2014.08.021

Wiboonrat, M. (2009). Transformation of system failure life cycle. *International Journal of Management Science and Engineering Management*, *4*(2), 143–152. https://doi.org/10.1080/17509653.2009.10671069