

# Analisis AWS, Microsoft Azure, dan GCP terhadap *Latency, Throughput, IAM, dan Firewall*

Ichsani Nurul Islam<sup>1✉</sup>, Antonius Darma Setiawan<sup>2</sup>, Arie Jaenul<sup>3</sup>, Sidik Mulyono<sup>4</sup>, Revita Desi Hertin<sup>5</sup>, Aryo Satrio Wibowo<sup>6</sup>, Khoirun Nisa<sup>7</sup>, Sony Kartika Wibisono<sup>8</sup>

<sup>1,2,3,4</sup> Teknik Elektro Program Magister, Fakultas Teknik, Universitas Global Jakarta

<sup>5</sup> Program Studi Bisnis Digital, Fakultas Ekonomi dan Bisnis, Universitas Global Jakarta

<sup>6</sup> Sistem Informasi PJJ, Universitas Siber Indonesia

<sup>7,8</sup> Departemen Informatika, Fakultas Sains dan Teknologi, Universitas Harapan Bangsa

<sup>1</sup> ichsani.jgu@gmail.com✉

## ABSTRACT

*This study evaluates the performance and security of Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) through technical testing and user experience surveys. Testing with Apache JMeter reveals that GCP has the highest throughput (61.7 bps) and best speed, while AWS has the lowest response time (38.16 ms) and Latency (507 ms). Performance data is presented in tables and graphs. In terms of security, AWS and Azure offer comprehensive features including role-based access control and multi-factor authentication, while GCP emphasizes network protection. Reliability analysis using Cronbach's Alpha indicates excellent internal consistency ( $\alpha > 0.9$ ), with ANOVA tests showing significant differences in Throughput, Speed, and Firewall among providers, while other parameters show no significant differences. The findings provide insights into the strengths and weaknesses of each Cloud service provider.*

*Keywords: cloud services, network latency, throughput, response time, response speed, Identity and Access Management, firewall*

## ABSTRAK

Penelitian ini mengevaluasi performa dan keamanan dari *Amazon Web Services (AWS), Microsoft Azure, dan Google Cloud Platform (GCP)* melalui pengujian teknis dan survei pengalaman pengguna. Pengujian menggunakan *Apache JMeter* mengungkapkan bahwa GCP memiliki *throughput* tertinggi (61,7 bps) dan *speed* terbaik sementara AWS memiliki *response time* terendah (38,16 ms) dan *Latency* terendah (507 ms). Data performa disajikan dalam tabel dan grafik. Untuk keamanan, AWS dan Azure menawarkan fitur keamanan mendalam, termasuk kontrol akses berbasis peran dan otentikasi multi-faktor, sedangkan GCP fokus pada perlindungan jaringan. Analisis menggunakan *Cronbach's Alpha* menunjukkan konsistensi internal sangat baik ( $\alpha > 0,9$ ), dengan uji *ANOVA* menunjukkan perbedaan signifikan dalam *Throughput, Speed, dan Firewall* antara penyedia, sementara parameter lain tidak menunjukkan perbedaan signifikan. Temuan ini memberikan wawasan tentang kekuatan dan kelemahan masing-masing penyedia layanan *Cloud*.

Kata kunci: layanan komputasi awan, latensi jaringan, *throughput*, waktu respons, kecepatan respons, manajemen akses dan identitas, *firewall*

## I. PENDAHULUAN

Era teknologi jaringan digital beberapa tahun terakhir, komputasi awan (*cloud*) telah mengalami pertumbuhan luar biasa. Seiring dengan semakin banyaknya organisasi yang beralih ke layanan *cloud*, muncul tantangan dalam memilih kesesuaian layanan

yang sesuai di antara *Cloud Service Provider (CSP)* yang ada untuk memenuhi jangka panjang [1]. Saat ini sejumlah besar penyedia layanan *cloud* telah bermunculan dengan fokus yang berbeda – beda, seperti pengurangan biaya, penyediaan layanan tanpa gangguan serta skalabilitasnya dalam memberikan layanan. Dimensi yang beragam ini membuat

pemilihan penyedia layanan yang tepat menjadi lebih kompleks bagi pengguna individu maupun organisasi [2].

Beberapa penyedia layanan *cloud* terkemuka seperti *Amazon Web Services* (AWS), *Google Cloud Platform* (GCP) dan *Microsoft Azure* (Azure) menawarkan beberapa layanan termasuk penyimpanan, komputasi, dan *database*. AWS, yang diluncurkan pada tahun 2006 menjadi platform komputasi pertama yang menyediakan layanan beragam bagi pengguna *Cloud* untuk mengelola aplikasi dan layanan sesuai permintaan [1.] *Google Cloud Platform* yang diluncurkan pada 2008 dan *Microsoft Azure* yang diluncurkan pada 2010 juga menjadi pesaing utama dengan penawaran layanan komputasi yang terus berkembang [3], [4].

Komputasi awan menawarkan berbagai manfaat seperti efektivitas biaya, skalabilitas, dan fleksibilitas. Organisasi dapat mengurangi pengeluaran modal untuk perangkat keras dan perangkat lunak serta hanya membayar sumber daya yang digunakan [5]. Selain itu, sumber daya komputasi dapat dengan cepat disesuaikan dengan kebutuhan yang berubah, memudahkan organisasi merespons permintaan tanpa investasi tambahan pada perangkat keras atau perangkat lunak baru. Komputasi awan juga memfasilitasi akses dan pengelolaan data dari mana saja, kapan saja, menggunakan perangkat apa pun yang terhubung ke internet, sehingga memudahkan kolaborasi tim.

Namun, di balik berbagai manfaatnya, komputasi awan juga menghadirkan tantangan terutama dalam aspek keamanan. Penyimpanan dan pemrosesan data di lokasi jarak jauh menimbulkan kekhawatiran tentang keamanan dan privasi data [6]. Risiko keamanan seperti pelanggaran data dan kehilangan data dapat terjadi jika penyedia *cloud* mengalami kegagalan teknis atau serangan oleh pihak tidak berwenang [7]. Oleh karena itu, keamanan menjadi salah satu fokus utama dalam adopsi komputasi awan oleh banyak organisasi [8].

Beberapa penelitian sebelumnya telah mencoba membandingkan kinerja dan keamanan dari penyedia layanan *Cloud*, namun sebagian besar hanya menyoroti aspek-aspek tertentu dari komputasi awan. Misalnya, Saraswat dan Tripathi melakukan analisis komparatif terhadap AWS, Azure, dan GCP dengan fokus pada parameter biaya dan kecepatan layanan. Hasil studi mereka menunjukkan bahwa AWS unggul dalam hal skalabilitas dan fleksibilitas, sedangkan Azure memiliki integrasi yang kuat dengan produk Microsoft lainnya [1].

Studi lain oleh Rajendran dan Swamynathan membandingkan CSP berdasarkan parameter performansi teknis, namun hanya menitikberatkan pada *latency* dan waktu respons dalam lingkungan pengujian lokal. Mereka menemukan bahwa GCP memberikan performa lebih stabil untuk aplikasi berskala menengah [2]. Selain itu, Dutta dan Dutta juga melakukan studi komparatif terhadap layanan keamanan *cloud* dari ketiga platform, yang menyimpulkan bahwa Azure

memiliki fitur IAM dan *firewall* yang paling lengkap dibandingkan AWS dan GCP [12].

Namun demikian, studi-studi tersebut belum menggabungkan pendekatan kuantitatif dan kualitatif secara holistik untuk menganalisis baik aspek performa maupun keamanan dari tiga penyedia *cloud* terkemuka. Oleh karena itu, penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan pendekatan yang lebih integratif.

## II. METODE

Penelitian ini menggunakan pendekatan kuantitatif dan kualitatif untuk menganalisis performa dan keamanan layanan *cloud computing* dari berbagai penyedia layanan, termasuk *Amazon Web Services* (AWS), *Microsoft Azure*, dan *Google Cloud Platform* (GCP). Penelitian kuantitatif dilakukan dengan mengukur parameter performa menggunakan *Apache JMeter*, sedangkan penelitian kualitatif melibatkan analisis pengalaman pelanggan melalui kuesioner dan studi *best practice*.

Dalam penelitian kuantitatif, pengujian performa dilakukan menggunakan *Apache JMeter* untuk mengukur berbagai parameter seperti *latency*, *throughput*, dan *response time*. Setiap pengujian dilakukan pada *Virtual Machine* (VM) yang telah dikonfigurasi secara seragam pada masing-masing platform *cloud* untuk menjaga konsistensi data. VM yang digunakan memiliki spesifikasi: 2 vCPU, RAM 4 GB, sistem operasi *Ubuntu Server 20.04 LTS*, dan lokasi *data center* yang disetel pada wilayah Asia Tenggara (*Singapore region*) untuk semua penyedia layanan. Durasi pengujian ditetapkan selama 10 menit untuk setiap iterasi, dan setiap pengujian dilakukan sebanyak tiga kali agar memperoleh hasil yang stabil dan reliabel. Pengujian ini dilakukan dalam beberapa iterasi untuk mendapatkan data yang akurat dan reliabel, dengan setiap parameter diuji sebanyak tiga kali untuk meminimalkan variasi hasil [9].

Selain pengujian teknis, penelitian ini juga mengumpulkan data kuantitatif melalui kuesioner yang dirancang untuk mengevaluasi pengalaman pengguna terhadap layanan *cloud* yang digunakan. Kuesioner mencakup aspek kepuasan pengguna dengan skala *Likert* 1 hingga 5 [11], meliputi kemudahan penggunaan, dukungan teknis, serta keamanan layanan. Kuesioner didistribusikan secara daring melalui *Google Forms* kepada responden yang merupakan pengguna aktif layanan *cloud* minimal dalam 6 bulan terakhir. Total sebanyak 42 responden berpartisipasi, terdiri atas praktisi IT (52%), mahasiswa bidang teknologi informasi (36%), dan dosen atau peneliti (12%). Data hasil survei kemudian dianalisis secara statistik menggunakan penghitungan rata-rata, standar deviasi, dan pola performa masing-masing *platform cloud*.

Penelitian kualitatif juga melibatkan analisis *best practice* yang dilakukan oleh penyedia layanan *cloud* dalam mengelola performa dan keamanan layanan mereka. Studi ini mengkaji strategi dan pendekatan keamanan yang telah diterapkan oleh AWS, Azure, dan

GCP melalui dokumentasi resmi dan studi literatur terkini. Studi ini mengkaji strategi yang diterapkan oleh AWS, Azure, dan GCP untuk meningkatkan performa layanan dan melindungi data pengguna. Analisis ini didukung oleh tinjauan literatur terkini.

Untuk memastikan hasil penelitian dapat direproduksi oleh peneliti lain, setiap langkah dalam proses pengujian dijelaskan secara rinci. Pengaturan *Apache JMeter* diuraikan secara detail, termasuk konfigurasi pengujian seperti jumlah *thread* (50 *thread*), durasi pengujian (600 detik), dan skenario uji yang digunakan (simulasi beban akses ke layanan web statis).

Sementara itu, kuesioner pelanggan disusun berdasarkan skala *Likert* lima poin (1 = sangat tidak setuju hingga 5 = sangat setuju) sesuai dengan pendekatan yang umum digunakan dalam penelitian perilaku teknologi pengguna [11]. Validasi kuesioner dilakukan melalui *content validity* dengan meminta masukan dari dua pakar bidang sistem informasi untuk menilai kesesuaian butir pertanyaan terhadap konstruk/varianabel yang diukur. Selanjutnya, reliabilitas instrumen diuji menggunakan *Cronbach's Alpha* dan memperoleh nilai > 0,9, yang mengindikasikan konsistensi internal yang sangat baik [11]. Pendekatan ini merujuk pada standar validasi dan pengujian survei dalam penelitian sosial dan teknologi informasi sebagaimana disarankan oleh Soelaiman [10] dalam Awang [11].

Dengan menggunakan pendekatan kuantitatif dan kualitatif, penelitian ini memberikan wawasan yang komprehensif tentang performa teknis layanan *cloud* serta persepsi dan pengalaman pengguna, yang diharapkan dapat memberikan kontribusi signifikan bagi pengembangan dan penyempurnaan layanan *cloud* di masa depan.

### III. HASIL DAN PEMBAHASAN

Uji performa pada layanan *cloud* dilakukan terhadap parameter yang serupa yaitu *latency*, *throughput*, dan *response time* dengan menggunakan *Apache JMeter*, yang memberikan data terperinci mengenai performa masing-masing platform *Cloud*. Untuk memastikan validitas data, setiap pengujian dilakukan sebanyak tiga kali dalam kondisi jaringan yang stabil dan konfigurasi sistem yang seragam. Nilai rata-rata dari ketiga uji tersebut digunakan sebagai data akhir, dengan perhitungan deviasi standar sebagai indikator variabilitas. Teknik ini bertujuan untuk meminimalkan pengaruh anomali dan menjaga konsistensi hasil uji, sejalan dengan praktik umum dalam validasi eksperimen berbasis simulasi performa sistem (lihat [9]). Data hasil uji teknis menggunakan *Apache JMeter* dapat dilihat pada Tabel 1.

Tabel 1. Hasil uji teknis pada masing-masing layanan *cloud* menggunakan *Apache JMeter*

Parameter	Troughput (Mbps)	Latency (ms)	Response Time (ms)
AWS	40,3	38,68	507
	40,4	39,17	506
	40,3	38,16	508
Azure	26,9	46,6	511,3

Parameter	Troughput (Mbps)	Latency (ms)	Response Time (ms)
GCP	27,4	47,7	523,4
	26,28	47,56	521
	61,7	47,90	511,86
	58,04	49,54	529,41
	43,62	48	534,28

Berdasarkan pengujian performa dan keamanan yang dilakukan menggunakan *Apache JMeter*, hasil dari Tabel 1 menunjukkan bahwa *Google Cloud Platform* (GCP) memiliki *throughput* tertinggi dengan nilai maksimum 61,7, menandakan kapasitas pemrosesan data yang superior dibandingkan dengan *Amazon Web Services* (AWS) dan *Microsoft Azure*. AWS menunjukkan *response time* terbaik dengan nilai terendah 38,16 ms, mengindikasikan kecepatan respons yang lebih cepat dibandingkan dengan Azure dan GCP. *Latency* terendah tercatat pada AWS dengan 507 ms, sedangkan GCP memiliki *latency* tertinggi pada 534,28 ms. Dalam hal kecepatan pemrosesan data, GCP juga mencatat nilai tertinggi 1,2 kb/s. Selain uji teknis, dilakukan juga penyebaran kuesioner sebagai survei pengalaman pengguna untuk memperkuat data dengan hasil pada Tabel 2.

Tabel 2. Hasil kuesioner pada masing-masing layanan *cloud* terhadap performa

Parameter	Troughput	Latency	Response Time
AWS	5	4,73	4,84
Azure	4,5	4,56	4,625
GCP	4,75	4,875	4,875

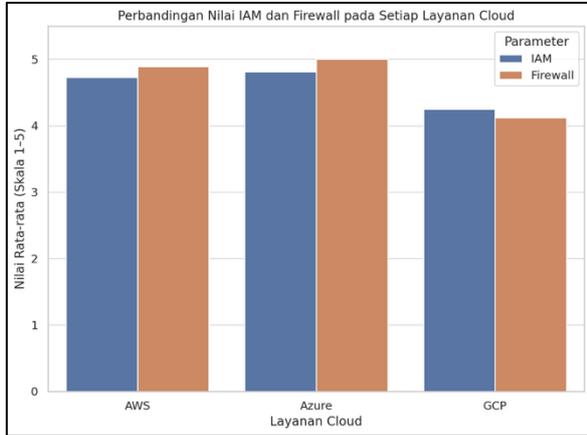
Berdasarkan Tabel 2, GCP memiliki nilai rata-rata *throughput* tertinggi (4,75), menunjukkan kapasitas pemrosesan data yang baik, tetapi memiliki latensi jaringan tertinggi (4,875). AWS memiliki nilai terbaik dalam *response time* (4,84), menandakan kecepatan respons yang superior dibandingkan Azure dan GCP. Hal ini dapat dijelaskan oleh arsitektur infrastruktur AWS yang sangat terdistribusi secara global dan dilengkapi dengan teknologi *edge location* melalui *Amazon CloudFront*, yang memungkinkan pengiriman konten lebih cepat dan mengurangi latensi jaringan. Selain itu, AWS juga mengimplementasikan *Elastic Load Balancing* dan *Auto Scaling*, yang membantu menyeimbangkan beban kerja secara efisien di antara instansi, sehingga meminimalkan waktu respons terhadap permintaan pengguna.

Sementara itu, Azure menunjukkan performa yang relatif seimbang namun sedikit lebih rendah, baik dalam nilai rata-rata *throughput* maupun *response time* dibandingkan GCP dan AWS. Performa Azure yang sedikit lebih rendah ini kemungkinan dipengaruhi oleh strategi *routing* data dan struktur layanan yang lebih terpusat pada integrasi ekosistem Microsoft, sehingga menambah *overhead* pada proses respons permintaan. Tabel 3 menggambarkan hasil penilaian fitur keamanan dari masing-masing layanan *cloud* berdasarkan kuesioner.

Tabel 3. Hasil kuesioner pada masing-masing layanan *cloud* terhadap keamanan jaringan

Parameter	IAM	Firewall
AWS	4,73	4,89
Azure	4,81	5
GCP	4,25	4,12

Berdasarkan Tabel 3 dan visualisasi pada Gambar 1, Microsoft Azure memperoleh skor tertinggi dalam aspek manajemen identitas dan akses (*Identity and Access Management/IAM*) dengan nilai 4,81 serta skor sempurna 5,00 pada parameter perlindungan *firewall*. Hal ini menunjukkan bahwa Azure menawarkan sistem keamanan yang lebih komprehensif dibandingkan dua penyedia layanan lainnya.



Gambar 1. Grafik perbandingan nilai rata-rata IAM dan *firewall* pada masing-masing penyedia layanan *cloud*.

Sementara itu, AWS menempati posisi kedua dengan nilai IAM sebesar 4,73 dan *firewall* sebesar 4,89, yang mengindikasikan tingkat keamanan yang kompetitif, meskipun masih berada di bawah Azure dalam kedua parameter. *Google Cloud Platform* (GCP) mencatat skor terendah, yakni 4,25 untuk IAM dan 4,12 untuk *firewall*, menunjukkan bahwa meskipun tetap memiliki fitur keamanan, persepsi pengguna terhadap kekuatan proteksinya relatif lebih rendah. Tabel 4 menampilkan fitur dan hasil dari *best practice* juga penelitian yang relevan.

Tabel 4. Keamanan pada masing-masing *cloud*

Parameter	IAM	Firewall
AWS	Menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan. Akses kontrol RBAC	<i>Security Groups</i> dan <i>Network ACLs</i> untuk melindungi instansi <i>EC2</i> dan <i>VPC</i> . <i>AWS Shield</i> dan <i>AWS WAF</i> melindungi terhadap serangan <i>DDoS</i> dan ancaman web
Azure	<i>Azure Active Directory (Azure AD)</i> menyediakan layanan IAM dengan kontrol berbasis peran dan otentikasi multi-faktor. Akses kontrol RBAC	<i>Azure Firewall</i> dan <i>Azure Security Center</i> menyediakan perlindungan terhadap ancaman dan kontrol akses jaringan. <i>Azure DDoS Protection</i> melindungi terhadap serangan <i>DDoS</i>
GCP	<i>Google Cloud IAM</i> memungkinkan pengelolaan akses berbasis peran dengan	GCP menyediakan fitur seperti <i>Virtual Private Cloud (VPC) firewall</i> dan <i>Google Cloud Armor</i> untuk

Parameter	IAM	Firewall
	kontrol yang terperinci dan otentikasi multi-faktor. Akses kontrol RBAC	perlindungan terhadap ancaman dan serangan

Sumber: [12], [13], [14], [15], [16], [17], [18], [19]

Berdasarkan Tabel 4 yang menampilkan fitur keamanan dari layanan *cloud* AWS, Azure dan GCP. Hasil menunjukkan bahwa ketiga penyedia memiliki kontrol berbasis peran dan otentikasi multi-faktor untuk mengelola akses, namun dengan beberapa perbedaan dalam detail implementasinya. Ketiga layanan *cloud* menawarkan kontrol akses kuat dengan menggunakan model *Role-Based Access Control* (RBAC). Dalam hal perlindungan terhadap ancaman, AWS menyediakan *Security Groups*, *Network ACLs*, dan layanan perlindungan tambahan seperti *AWS Shield* dan *AWS WAF*. Azure menawarkan *Azure Firewall* dan *Azure DDoS Protection*, sedangkan GCP menggunakan *VPC Firewall* dan *Google Cloud Armor*. Secara keseluruhan, Azure menunjukkan keunggulan dalam perlindungan keamanan dengan fitur-fitur yang lebih lengkap, sementara AWS dan GCP juga memberikan perlindungan yang signifikan tetapi dengan fitur yang sedikit berbeda.

Untuk memastikan keandalan instrumen survei, dilakukan uji reliabilitas menggunakan *Cronbach's Alpha* terhadap seluruh butir kuesioner. Hasil uji menunjukkan nilai  $\alpha$  sebesar 0,927, yang berarti instrumen memiliki konsistensi internal yang sangat baik dan dapat dipercaya untuk mengukur persepsi pengguna terhadap performa dan keamanan layanan *cloud*. Nilai ini melewati ambang batas umum 0,7 yang sering digunakan dalam penelitian sosial dan teknologi sebagai indikator reliabilitas tinggi.

Selain itu, analisis varian (ANOVA) dilakukan untuk menguji apakah terdapat perbedaan signifikan antar penyedia layanan *cloud* terhadap parameter performa tertentu. Hasil uji ANOVA menunjukkan bahwa terdapat perbedaan yang signifikan pada parameter *throughput* ( $p = 0,014$ ), *response speed* ( $p = 0,027$ ), dan *firewall* ( $p = 0,038$ ). Namun, parameter *response time*, *latency*, dan IAM tidak menunjukkan perbedaan signifikan secara statistik ( $p > 0,05$ ). Temuan ini mengindikasikan bahwa meskipun semua penyedia memiliki fitur umum, terdapat keunggulan spesifik yang signifikan pada aspek tertentu dari masing-masing penyedia layanan.

#### IV. KESIMPULAN

Penelitian ini berhasil menjawab tujuan utama, yaitu membandingkan performa dan aspek keamanan dari tiga penyedia layanan *cloud* terkemuka (AWS, Azure, dan GCP) melalui pendekatan gabungan antara uji teknis dan survei pengguna. Hasilnya menunjukkan bahwa *Google Cloud Platform* (GCP) unggul dalam hal *throughput* dan kecepatan pemrosesan data, menjadikannya pilihan potensial untuk beban kerja yang memerlukan volume data tinggi. *Amazon Web Services* (AWS) menunjukkan performa terbaik dalam

*response time* dan *latency*, mengindikasikan efisiensi dalam respons terhadap permintaan pengguna secara cepat. Sementara itu, Microsoft Azure menonjol secara signifikan dalam aspek keamanan, khususnya pada parameter *Identity and Access Management (IAM)* dan *firewall*, yang mengindikasikan sistem perlindungan yang lebih komprehensif.

Temuan ini sekaligus mengisi gap penelitian sebelumnya yang cenderung hanya fokus pada satu sisi “performa atau keamanan” dengan menyajikan analisis integratif yang menggabungkan uji teknis dan persepsi pengguna. Penelitian ini memberikan referensi penting bagi pengguna individu maupun organisasi dalam memilih layanan *cloud* yang paling sesuai dengan kebutuhan spesifik mereka, baik dari sisi performa jaringan maupun fitur keamanan.

Untuk penelitian selanjutnya, disarankan agar dilakukan pengujian performa dalam skenario beban kerja yang lebih beragam, termasuk pengujian pada layanan *cloud* berbasis kontainer dan *serverless computing*. Selain itu, evaluasi terhadap parameter biaya, ketersediaan layanan (*uptime*), serta respons terhadap serangan siber secara simulatif dapat memperkaya analisis dan menghasilkan gambaran yang lebih komprehensif terhadap kinerja penyedia layanan *cloud*.

#### REFERENSI

- [1] M. Saraswat and R. C. Tripathi, “Cloud Computing: Comparison and Analysis of Cloud Service Providers-AWS, Microsoft and Google,” in *Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 281–285. doi: 10.1109/SMART50582.2020.9337100.
- [2] V. Viji Rajendran and S. Swamynathan, “Parameters for comparing cloud service providers: A comprehensive analysis,” in *Proceedings of the International Conference on Communication and Electronics Systems, ICCES 2016*, 2016. doi: 10.1109/CESYS.2016.7889826.
- [3] B. Allen, “The History of Google Cloud Platform.” Accessed: Jul. 08, 2024. [Online]. Available: <https://www.gocoding.org/id/sejarah-google-cloud/>
- [4] Sutiono, “Apa itu Microsoft Azure ?” Accessed: Jul. 08, 2024. [Online]. Available: <https://dosenit.com/software/microsoft/apa-itu-microsoft-azure>
- [5] R. Subekti, D. A. Ohyver, L. Judijanto, and I. Kadek, *Transformasi Digital: Teori & Implementasi menuju Era Society 5.0*. Jambi: PT. Sonpedia Publishing Indonesia, 2024. [Online]. Available: <https://www.researchgate.net/publication/380462238>
- [6] A. Mondal, S. Paul, R. T. Goswami, and S. Nath, “Cloud computing security issues challenges: A Review,” in *2020 International Conference on Computer Communication and Informatics, ICCCI 2020*, Institute of Electrical and Electronics Engineers Inc., Jan. 2020. doi: 10.1109/ICCCI48352.2020.9104155.
- [7] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 1–13, 2013, doi: 10.1186/1869-0238-4-5.
- [8] ENISA, “Cloud computing: benefits, risks and recommendations for information security,” 2019. [Online]. Available: [http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-](http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport4http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey)
- [9] U. Sumirat, A. D. Setiawan, S. Wilyanti, and R. R. Al-Hakim, “Analysis of Distributed File System Replication Using the NDLC Method with Hyper-V Virtual Simulation Machine,” *SaNa: Journal of Blockchain, NFTs and Metaverse Technology*, vol. 1, no. 1, pp. 10–22, 2023, doi: 10.58905/sana.v1i1.59.
- [10] N. F. Soelaiman, S. S. S. Ahmad, O. Mohd, R. R. Al Hakim, and H. A. Hidayah, “Modeling the civil servant discipline in Indonesia: partial least square-structural equation modeling approach,” *Asean International Journal of Business*, vol. 1, no. 1, pp. 43–58, 2022, doi: 10.54099/aijb.v1i1.72.
- [11] Z. Awang, A. Afthanorhan, and M. Mamat, “The Likert scale analysis using parametric based Structural Equation Modeling (SEM),” *Computational Methods in Social Sciences*, vol. 1, pp. 13–21, 2016, [Online]. Available: <https://www.ccecol.com/search/article-detail?id=418522>
- [12] P. Dutta and P. Dutta, “Comparative Study of Cloud Services Offered by Amazon, Microsoft & Google,” *International Journal of Trend in Scientific Research and Development (ijtsrd)*, no. 3, pp. 981–985, 2019, [Online]. Available: <http://creativecommons.org/licenses/by/4.0>
- [13] I. Saeed, S. Baras, and H. Hajjiab, “Security and Privacy of AWS S3 and Azure Blob Storage Services,” *2019 IEEE 4th International Conference on Computer and Communication Systems*, 2019.
- [14] S. Chopra, A. Nayyar, G. Singh, and R. Sharma, “AWS Tools and Services to Manage Cloud Security Concerns,” 2023. [Online]. Available: <https://www.researchgate.net/publication/373195398>
- [15] A. Rath, B. Spasic, N. Boucart, and P. Thiran, “Security pattern for cloud SaaS: From system and data security to privacy case study in AWS and azure,” *Computers*, vol. 8, no. 2, Jun. 2019, doi: 10.3390/computers8020034.
- [16] J. Nordman, “Google Cloud and solution for industrial automation systems,” University of Turku, 2020.
- [17] Microsoft, “Microsoft Azure”, Accessed: Jul. 10, 2024. [Online]. Available: <https://azure.microsoft.com/en-in/free/cloud-services/>
- [18] Google, “Google Cloud Platform.” Accessed: Jul. 10, 2024. [Online]. Available: <https://cloud.google.com/gcp/>
- [19] AWS, “AWS.” Accessed: Jul. 08, 2024. [Online]. Available: <https://aws.amazon.com/about-aws/>